Tivoli Management Framework

Release Notes

Version 4.3.1

GI11-0890-02

Tivoli Management Framework

Release Notes

Version 4.3.1

GI11-0890-02

Tivoli Management Framework Release Notes

Trademarks

IBM, AIX, DB2, OS/2, OS/400, S/390, pSeries, Tivoli,, Tivoli Enterprise, Tivoli Enterprise Console, Tivoli SecureWay, TME, zSeries, and the Tivoli logo are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Lotus and Lotus Notes are a registered trademarks of IBM Corporation and Lotus Development Corporation in the United States, other countries, or both.

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

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

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

Notices

References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to valid intellectual property or other legally protectable right of Tivoli Systems or IBM, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user. Tivoli Systems or IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.

Contents

About this guide v
Conventions used in this guide v
Accessing publications online. v
Ordering publications vi
Contacting software support vi

Chapter 1. About this release 1
Technologies that are no longer supported 1
New features 1
Support for Linux for iSeries, pSeries, zSeries systems 3
Support for Solaris2 on ix86 systems 3
ODBC connection for SQL Server databases . . . 3
Tivoli Firewall Security Toolbox changes 4
Compatibility and interoperability 4
Tivoli Management Framework Compatibility CD 5
Patches included in Version 4.3.1 6
Defects fixed 6

Chapter 2. Installation and upgrade notes 15
Determining operating system patch levels 15
Determining operating system swap space 15
System requirements 16
AIX operating system on pSeries and PowerPC systems. 17
HP-UX operating system on HP 9000 systems . . 18
Linux on Intel systems 18
Linux on PowerPC systems 18
Linux on zSeries systems 18
OS/400 systems 19
Solaris operating environment on Sun SPARC and Intel systems 19
Windows operating system on Intel systems . . 19
Browsers requirements 20
SSL security packages requirements 20
SSL-A package requirements. 20
Upgrade from Tivoli Management Framework 4.1.1 requirements 20

Chapter 3. SSH Requirements. 23

Chapter 4. Web server requirements for Tivoli Web interfaces 25

Chapter 5. Disk space requirements . . 27
Tivoli servers, managed nodes, and gateways . . . 27
Endpoints 27

Chapter 6. RDBMS requirements . . . 29
Supported RDBMS servers 29
Requirements for DB2 clients by server version . . 30
Requirements for Informix clients by server version 31
Requirements for Microsoft SQL Server clients by server version 32
Requirements for Oracle clients by server version . 32
Requirements for Sybase clients by server version 32

Chapter 7. Installation and product notes 35
Installation notes 35
General installation notes. 35
Upgrading to Tivoli Management Framework, Version 4.3.1 37
Upgrading Tivoli Management Framework on AIX operating systems when an Oracle client is installed 37
Upgrading Tivoli Management Framework when Tivoli Security Management is installed 37
Product notes. 38
General product notes 38
Windows 2000 and Windows Server 2003 and 2008 40

Chapter 8. Interpreter type mappings 41

Chapter 9. Software limitations, problems and workarounds. 43
Limitations 43
Known defects and workarounds 44
Endpoint and gateways 44
Endpoint installation 45
Multiplexed Distribution 46
Object dispatcher 46
Product installation. 46

Chapter 10. Internationalization notes 47
Installation and upgrade notes 47
Enabling language support 47
System requirements for Asian environments . . 48
Java requirements 48
Endpoint notes 48
NEC PC98 systems 48
Cantonese Chinese 49
Software limitations, problems, and workarounds . 49

About this guide

These release notes provide important information about Tivoli® Management Framework, Version 4.3.1. These release notes are the most current information for the product. *Review these notes thoroughly before installing or using this product.*

Both Tivoli and TME® 10 are used in our sales, marketing, and product literature. These terms are interchangeable with Tivoli Management Framework.

In addition, a Tivoli endpoint is sometimes called a Tivoli management agent, lcfd, Tivoli Lightweight Client, or endpoint daemon. All these terms refer to the Tivoli process running on the endpoint client.

Conventions used in this guide

This guide uses several typeface conventions for special terms and actions. These conventions have the following meaning:

Bold Commands, keywords, file names, authorization roles, URLs, names of windows and dialogs, other controls, or other information that you must use literally are in **bold**.

Italics Variables and values that you must provide, new terms, and words and phrases that are emphasized are in *italics*.

`Monospace`
Code examples, output, and system messages are in a `monospace` font.

This guide uses the UNIX convention for specifying environment variables and for directory notation:

- When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables and replace each forward slash (**/**) with a backslash (\) in directory paths.
- When using the bash shell on Windows, use the UNIX conventions.

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both. Refer to the readme file on the CD for instructions on how to access the documentation.

The product CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both. To access the publications using a Web browser, open the infocenter.html file. The file is in the appropriate publications directory on the product CD.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:

http://www.ibm.com/software/tivoli/library/

Scroll down and click the **Product manuals** link. In the Tivoli Technical Product Documents Alphabetical Listing window, click the IBM Tivoli Configuration Manager link to access the product library at the Tivoli software information center.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File ″ Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, see the following Web site for a list of telephone numbers:

http://www.ibm.com/software/tivoli/order-lit/

Contacting software support

If you have a problem with any Tivoli product, refer to the following IBM Software Support Web site:

http://www.ibm.com/software/sysmgmt/products/support/

If you want to contact software support, see the *IBM Software Support Guide* at the following Web site:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides information about how to contact IBM Software Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers, depending on the country in which you are located
- Information you must have before contacting IBM Software Support

Chapter 1. About this release

This chapter describes the new features included in Tivoli Management Framework, Version 4.3.1. In addition, this chapter provides information about software technologies that are no longer supported; product compatibility and interoperability; the patches included in this release; and the fixed defects included in this release.

Technologies that are no longer supported

The documentation for Tivoli Management Framework contains references to software technologies that are no longer supported by IBM. For example, references to ADE/ADF should be ignored because the Application Development Environment and Application Development Framework portions of Tivoli Management Framework are no longer supported. References to older Windows platforms released prior to Windows 2000 Server (such as Windows NT, Windows 98, and Windows Me) should also be ignored, because those Windows operating systems are no longer supported.

Additionally, the use of Tivoli Management Framework Release 4.3.1 or any of its components is no longer supported on NetWare, SunOS, or OS/2. References to these systems still exist in the documentation and should be ignored.

New features

This section briefly describes the new features or enhancements of Tivoli Management Framework, Version 4.3.1. The new features are as follows:

Updated platform support for Tivoli Management Framework and Tivoli Firewall Security Toolkit.

For information about supported platforms for Tivoli Firewall Security Toolkit, see the Tivoli Firewall Security Toolkit User's Guide. For a list of operating system platforms that are supported by Tivoli Management Framework, Version 4.3.1, see “System requirements” on page 16. For the latest supported platform list, refer to the following URL: http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivoliManagementFramework.html.

Adaptive Bandwidth Control for Windows and Linux

Adaptive bandwidth control dynamically manages the bandwidth used to perform distributions. When this feature is enabled, The amount of bandwidth used to perform distributions between gateways and endpoints varies, depending on changes in network conditions.

When the network is busy with other traffic, distributions happen more slowly so they do not consume large amounts of bandwidth that might be needed by more critical application.

When the network load is idle or traffic is light, distributions occur quickly because the adaptive bandwidth feature adjusts to consume more bandwidth to speed distributions.

The amount of impact that distributions have on network traffic is configurable by parameter settings that specify whether distributions will be treated as having low, medium, or high priority.

See the **wmdist** command in the Tivoli Management Framework Reference Manual, for adaptive bandwidth configuration parameters.

Login Nearest Gateway
The login nearest gateway feature allows roaming endpoints to migrate to the nearest gateway and receive distributions when their previously assigned gateway is in a different geographic location. See the **wgateway** command option **ep_iprange** for **login_nearest_gateway** in the Tivoli Management Framework Reference Manual.

Post Tivoli Management Framework notices to syslog (UNIX-like systems only)
This feature provides an audit trail of management actions by posting Tivoli Management Framework notices to the UNIX syslog subsystem. See the **wcfgnotif** command in the Tivoli Management Framework Reference Manual.

Keep alive: oserv to oserv communications
A new set_keep_alive= parameter has been added to the **odadmin** command. This can be used to ensure that firewalls do not close idle oserv-to-oserv connections. This increases the stability of critical Tivoli Management Framework daemons and Tivoli Enterprise application daemons when traversing firewalls. See the **odadmin** command in the Tivoli Management Framework Reference Manual.

PAM (Pluggable Authentication Module) support
Allows remote desktop and Java applications to use PAM for authenticated remote logins. This feature is available on Linux, AIX, HP, and Solaris systems. Pluggable Authentication Module support is described in the Tivoli Enterprise Installation Guide, under the discussion of **Starting the Tivoli desktop**. See **Using Pluggable Authentication Modules (PAM) on UNIX-like systems**.

Enhancements for mobile service
A number of enhancements have been added to the mobile Computing console. The installer program has been modified such that if you run the `setup.exe` program to install the mobile console, it is installed and runs using the Windows LocalSystem account, which allows any user, whether in the Administrators group, or not, to accept distributions sent from a Tivoli Administrator, when the mobile endpoint is not connected. A new option for setup.exe (**-noservice**) disables this new behavior. See **Installing the Tivoli® Mobile Computing console** in the Tivoli Management Framework User's Guide

A number of new configuration options have also been added for the mobile computing console. The new parameters are: **clientBootDelay**, **suppressMandatoryPopus**, **disableTimeRemainingColumn**, **showMenu**, **allowCloseMandatory**, **extraStatus**, and **showPauseOnly**. These too are described in **Installing the Tivoli Mobile Computing console** in the Tivoli Management Framework User's Guide.

Support for IBM Tivoli License Compliance Manager
Product signature files have been added to the components in this release to make Tivoli Management Frameworkcomponents (server and client) compliant with IBM Tivoli License Compliance Manager. IBM Tivoli License Compliance Manager is a web-based solution that tracks the use and installation of software products. Now that the Tivoli Management Framework components have the signature files, customers using IBM Tivoli License Compliance Manager can now collect data related to Tivoli

Management Framework installations, including the release and version of the management regions, managed nodes, and endpoints.

Name Registry enhanced
The Name Registry Increases performance of interconnected regions. In previous releases, the name registry was designed to use a “pull” model. The **wupdate** command or ″read-thru″ pulls the information from the foreign Tivoli management regions. When changes occur in the foreign name registries, those changes were not seen until new data was pulled. In this release, there is an addition of a new type, named “push”, to the existing types; this new type updates foreign Tivoli name registries as and when data is updated.

upcall_method_timeout added to wgateway
New get and set options on **wgateway** allow you to set or retrieve the **upcall_method_timeout** interval. This interval specifies the number of seconds that a gateway will wait, after starting an upcall method, for a response from the upcall method.

Improved error messages
More descriptive and complete error messages have been added to upcall, downcall, and mdist2 operations. The new messages includes reporting of critical status data, like the endpoint cache lock, jobs that are pending in the gateway's job queue, and so on.

Endpoint management enhancements
A technical paper (a Field Guide) describing numerous endpoint management enhancements, some of which are not in the standard library of documents for Tivoli Management FrameworkVersion 4.3.1 has been posted to http://www.ibm.com/support/docview.wss?uid=swg27005330 &aid=1. Topics contained include such things as Endpoint Communication Reliability Enhancements; Endpoint Health Checks; and Reporting Endpoint Repair, including automatic self repair and remote repair.

Integrated component and status monitoring
For information see the readme file in $BINDIR/../generic/tmfmon/ README for information about oserv status logging, and using the **odadmin set_keep_alive** feature on endpoint managers and gateways.

Support for Linux for iSeries, pSeries, zSeries systems

This release of Tivoli Management Framework supports Linux for iSeries, pSeries and zSeries systems as server and clients.

Support for Solaris2 on ix86 systems

This release of Tivoli Management Framework supports solaris2 for ix86 systems as server and clients.

ODBC connection for SQL Server databases

In Tivoli Management Framework, Version 4.3.1, the RDBMS interface module (RIM) uses ODBC to connect to a Microsoft SQL Server database rather than using a Microsoft SQL Server client. Therefore, you must create an ODBC data source to enable RIM to connect to a Microsoft SQL Server database. For more information about creating an ODBC data source, see the chapter about using RIM objects in the *Tivoli Enterprise Installation Guide*.

Tivoli Firewall Security Toolbox changes

Tivoli Firewall Security Toolbox, Version 1.3.2 contains the following changes:

New operating system support
The table of supported operating systems, in the *Tivoli Firewall Security Toolbox, Version 1.3.2 User's Guide* has been updated to include the latest versions of RHEL, Solaris, Windows, and HP systems.

Installing Windows event sink
Text has been altered to make the location of the eventsink.exe file more clear.

enable-identity
A new configuration option for endpoint and gateway proxies allows the use of dynamic IP addresses (NAT) with unidirectional clients. This new parameter also changes the behavior of some existing configuration values. These are described in a section that describes how to configure enable-identity.

Setting the endpoint proxy login interval on all platforms
This text has been updated for this release to clarify that the procedure is only performed for recent releases of Tivoli Management Framework.

wproxy examples
Additional examples have been added to illustrate the use of the **wproxy** command.

Providing more detail in the log files and to support
Clarification of the effects of max-size and enabling detailed log levels, and additional tips about what to collect before calling IBM support.

Compatibility and interoperability

This section contains information about the compatibility and interoperability of Tivoli Management Framework.

Note: The compatibility of a Tivoli Enterprise product with Tivoli Management Framework does not indicate that the Tivoli Enterprise product is also compatible with new operating system releases that are supported by Tivoli Management Framework.

The terms *compatibility* and *interoperability* are defined as follows:

Compatibility
Whether different versions of a Tivoli Enterprise product can communicate with different versions of Tivoli Management Framework.

Interoperability
Whether different versions of the same Tivoli Enterprise product can communicate with each other.

Tivoli Management Framework, Version 4.3.1, can interoperate with all supported versions of Tivoli Management Framework. When you upgrade your Tivoli management region server (Tivoli server) to Version 4.3.1, the endpoint manager is upgraded. After upgrading your server, upgrade your gateways. You can upgrade endpoints using the **wepupgrd** command, by using a **login_policy** script, or by using the endpoint automatic upgrade option in the gateway to automatically upgrade endpoints the first time they log in to the upgraded gateway.

Note: Endpoint methods associated with a previous version can be downloaded and run on Version 4.3.1 endpoints when a Tivoli environment has both versions of gateways.

Note: Tivoli Management Framework, Version 4.3.1 is compatible with all supported versions of Tivoli Enterprise products. For a definitive statement about whether a specific Tivoli Enterprise product is compatible with Tivoli Management Framework, Version 4.3.1, refer to the release notes for that product. In some cases, a patch is required for these products to be compatible.

Note: Tivoli Management Framework supports Network Address Translation (NAT). NAT managed nodes cannot communicate with non-NAT managed nodes. However, the following combinations between gateways and endpoints are supported:

- Non-NAT endpoint to non-NAT gateway
- Non-NAT endpoint to NAT gateway
- NAT endpoint to non-NAT gateway
- NAT endpoint to NAT gateway

Because Tivoli Enterprise software supports Kerberos 4.0 and because Kerberos 4.0 depends on static IP addresses, Kerberos and NAT cannot coexist.

Tivoli Management Framework Compatibility CD

Java components, such as Tivoli Java Client Framework and Tivoli Java RDBMS Interface Module, enable Tivoli Management Framework and other Tivoli products to run Java programs. New Java components do not supersede or overwrite old Java components. For example, Tivoli Java Client Framework, Version 4.3.1 does not supersede Tivoli Java Client Framework, Version 4.1.1. It installs separately, and the two can coexist on the same system.

The new Tivoli Compatibility CD contains Java components that you may need to install if you are using an application that requires previous versions of Java components. See the product-specific documentation for more information.

Note: You do not need to install any software from this CD if you are using the most recent versions of Java and Tivoli Management Framework.

The Tivoli Management Framework Compatibility CD supplies the following previous versions of Java components for backwards compatibility:

- JavaHelp for Tivoli, Version 3.7
- Java Client Framework for Tivoli, Version 3.7
- Java Client Framework for Tivoli, Version 3.7.1
- Java Client Framework for Tivoli, Version 4.1
- Java for Tivoli, Version 3.7
- Java for Tivoli, Version 3.7.1
- Tivoli Java RDBMS Interface Module (JRIM), Version 3.7
- Tivoli Java RDBMS Interface Module (JRIM), Version 3.7.1
- Tivoli Java RDBMS Interface Module (JRIM), Version 4.1
- Swing for Tivoli, Version 3.7

Patches included in Version 4.3.1

Tivoli Management Framework, Version 4.3.1, includes all Tivoli server, managed node, and gateway patches through 4.1.1-TMF-0104 and endpoint patches through 4.1.1-LCF-0058.

Defects fixed

The following defects have been fixed in Tivoli Management Framework, Version 4.3.1:

- APAR IY25413: Scheduled software distribution of endpoint which was deleted.
- APAR IY31890: Tivoli desktop gadget value of ″_unchanged_″ not recognized.
- APAR IY34400: Mdist2GUI login windows does not appear.
- APAR IY36652: The select_gateway_policy names is ignored.
- APAR IY39616: Mdist2GUI hangs or crashes.
- APAR IY42343: JRIM does not return error code.
- APAR IY43331: wifconfig does not work with logical interfaces.
- APAR IY44113: w4inslcf script does not work with name format set to path.
- APAR IY44586: Mdist2GUI with auto update crashes.
- APAR IY45053: The files_transfer method can hang.
- APAR IY46386: The WOL on windows endpoint always wakes on port 2304.
- APAR IY46526: Security issue when dragging & dropping a query from a query library.
- APAR IY46529: The start_delay is overwritten when endpoint is upgraded.
- APAR IY46561: When unsubscribing a Profile Manager, all profiles are lost on the target endpoint.
- APAR IY46710: The TME administration notice group contains error message.
- APAR IY47951: The wadminep get_file cores if endpoint label is same as file name.
- APAR IY48151: Large DLL is not downloaded from gateway repository to endpoint.
- APAR IY48401: Oserv crashes if NAT is enabled.
- APAR IY48570: The ″-s″ option of winstlcf registers the wrong absolute path.
- APAR IY48898: Scheduled database backup fails on Linux.
- APAR IY49027: In some situations, the Tivoli Name Registry and Endpoint Manager database may go out of sync.
- APAR IY49044: Only one AEF actions runs when there are multiple unique action
- APAR IY49165: The ″wep set″ command crashes.
- APAR IY49396: Jobs running tasks that write to stdout cause high cpu usage.
- APAR IY49500: The ″wlookup -ar Endpoint″ on the Hub does not show the Spoke’s endpoints.
- APAR IY49594: The action option window is too small in Japanese mobile.
- APAR IY49860: The last modification time reported by wdepot list is not useful.
- APAR IY49863: The wmv CLI is not working correctly
- APAR IY49942: A task that produces a large amount of output may fail.
- APAR IY50030: Add -a and -m to wcrtrim usage statement.
- APAR IY50151: If wmailhost is not set, send_support fails.

- APAR IY50207: Inconsistent behavior is observed in Tivoli FRW (WebServer).
- APAR IY50214: The ″wep <ep>″ does not with one-way inter-connected TMR.
- APAR IY50481: Incorrect ACL defined on some endpoint methods.
- APAR IY50767: HTTP request on port 94 can cause oserv to crash.
- APAR IY50865: A distribution status does not reach 100% completion after expiry time.
- APAR IY50967: Mdist2 fails with error message ″failed to get the file″.
- APAR IY51380: LCFD uses 100% cpu.
- APAR IY51390: The wlsconn CLI reports incorrect value.
- APAR IY51443: The spd_eng.exe fails on an endpoint.
- APAR IY51614: The rpt2.exe crashes frequesntly with unhandled exception.
- APAR IY52000: The documentation for wpatch is incorrect.
- APAR IY52045: The first mobile popup during a distribution is displayed in English.
- APAR IY52184: The framework install completes with ypwhich error.
- APAR IY52302: The widmap <incorrect arg> gives incorrect error.
- APAR IY52450: The AIX gateway process is limited to 256MB process size.
- APAR IY52504: The web_post fails on LCFD if network is unavailable during LCFD start.
- APAR IY52510: No activity is shown in lcfd.log until LCFD is recycled.
- APAR IY52558: The wgateway reports wrong status.
- APAR IY52619: The wrimtest shows old 3.6.1 flags in 4.1.1 version.
- APAR IY52699: Distribution ID does not get generated.
- APAR IY52704: The gateway caused an unhandled exception.
- APAR IY52724: The rim_db2_agent not being cleaned up.
- APAR IY52858: DBCS named task on solaris TMR fails to execute.
- APAR IY52861: The mobile GUI takes too long to start.
- APAR IY52891: The gateway port held open for 10 minutes before a restart.
- APAR IY53025: ITM install fails.
- APAR IY53083: Incorrect error message during endpoint remote control session.
- APAR IY53291: Viewing default.html webpage results in blank page.
- APAR IY53347: A failure to lauch windows desktop on one system may cause failure on others.
- APAR IY53388: Create a tunable gateway parameter for tcp backlog.
- APAR IY53399: Create a tunable gateway parameter to send gateway aliases.
- APAR IY53733: TAP does not generate tokens when the TRAA account does not exist.
- APAR IY53906: TAP can not generate token for user eu\administrator.
- APAR IY54019: Profile manager names can contain invalid names.
- APAR IY54054: Orphaned endpoint can cause gateway to crash.
- APAR IY54135: The mn_rpt_before.sh script fails.
- APAR IY54150: The Tivoli_Admin_Privileges group is not updated correctly when endpoint is created using the ″winstlcf″ command.
- APAR IY54152: The wifconfig cannot differentiate multiple addresses on a single interface.
- APAR IY54155: Incorrect error message ″account expired″ in oservlog.

- APAR IY54204: The t_tmf_ccms_subscribee_subscribee crashes with trans NONE.
- APAR IY54311: The TMR authentication On Linux fails using PAM.
- APAR IY54328: The gateway cores due to mdist2 race condition.
- APAR IY54373: A redirect character can cause a task to fail on windows endpoints.
- APAR IY54395: LCFD can't start if a space is appended to the lcfd_port value in last.cfg.
- APAR IY54512: TAP errors.
- APAR IY54535: desktop for windows login and exit messages on a French Canadian installation.
- APAR IY54559: Huge memory growth of oserv process when running ITM.
- APAR IY54622: A query throws a 'no describe for table' exception.
- APAR IY54653: Unscalable fonts in desktop for windows.
- APAR IY54687: The distmgr takes a long time to refresh its cache.
- APAR IY54698: The spo_core exits with e=11 performing software distribution.
- APAR IY54833: TAP does not pickup active directory nested global group member.
- APAR IY54895: A duplicate tune attributes is created in repeater manager.
- APAR IY54913: The 'sync_gw_epcache' method hangs.
- APAR IY54918: Incorrect message in wbkupdb.
- APAR IY55154: The wep get httpd output loses user ID.
- APAR IY55171: Wrong ACL is defined on some endpoint methods.
- APAR IY55342: The gateway tries to change login mode of mobile endpoint on every normal login.
- APAR IY55406: The RIM fails on temporary table with execute_sql().
- APAR IY55437: The gateway process leaks memory.
- APAR IY55470: The deadline is reached for distribution even before it starts.
- APAR IY55564: The spd_eng.exe generates a spawn_impl error 32.
- APAR IY55627: The pcremote process crashes with signal 11.
- APAR IY55686: The endpoint manager receives lots of isolation and migration login.
- APAR IY55690: After upgrading to TMF 4.1.1 distributions seem to hang.
- APAR IY55691: The results from mdist2 distribution fail to be posted.
- APAR IY55930: The oserv's tmp environment variable is not set correctly on windows 2000.
- APAR IY56180: The 4.1.1 version of wpatch can fail silently.
- APAR IY56221: The mobile console client doesn't work with multiple endpoint installation.
- APAR IY56244: The gatelog is flooded with Mdist error messages.
- APAR IY56346: The mobile popup shows incorrect/confusing information.
- APAR IY56427: The wchkdb fails with errors FRWSL0024E.
- APAR IY56471: The endpoint health check is not responding to gateway within set time.
- APAR IY56474: LCFD throws an execption when shutting down on Windows XP.
- APAR IY56617: The epmgr leaks memory. APAR IY56646: LCFD is not started after upgrade.

- APAR IY57006: The ″wepmgr restart″ command can’t open *.bdb files.
- APAR IY57118: Add gateway parameter to delay start of repeater thread.
- APAR IY57130: The endpoint GUID can’t be changed for inventory.
- APAR IY57362: The oserv crashes in certain condtition.
- APAR IY57416: The ″wep sync_gateways″ failed to sync gateway.
- APAR IY57680: The shift_jis codeset is not deployed into AS2.1 Linux endpoint.
- APAR IY57855: TAP does not allow a TRAA account to be specified using a DNS-style domain name.
- APAR IY58147: The files_transfer method on windows managed node can hang.
- APAR IY58257: The gateway process crashes with signal 11.
- APAR IY58417: The gateway crashes when a user is accessing the gateway’s data.
- APAR IY58418: Russian codeset (1251) is not sent to endpoint.
- APAR IY58476: The wchkdb in TMF411 is slower than the TMF371.
- APAR IY58678: The RPT2 leaks file descriptors.
- APAR IY58812: The windows advert thread dies after lots of distributions.
- APAR IY58848: The software distribution depot handling has problems.
- APAR IY58876: The wepupgd returns incorrect error for users that are not authorized.
- APAR IY58878: The endpoint_callback method passes incorrect endpoint parameters.
- APAR IY58907: The wep -s renaming endpoint to an existing endpoint name gives incorrect error.
- APAR IY59034: The ’wgateway gw set_interface_ignore_list none’ does not work.
- APAR IY59089: The mobile gui fails to start.
- APAR IY59246: The gateway cores when unable to resolve the ep’s hostname.
- APAR IY59523: The tec_dispatch core with sigsegv when SSL is enabled.
- APAR IY59718: The ’wchkdb’ doesn’t complete or gives incorrect message.
- APAR IY59759: The library_skel1 shows memory growth and terminates abnormally.
- APAR IY60017: The cached TEC events are not sent if allow_proxy_upcalls=true.
- APAR IY60446: The gateway crahses when loading a SP if ’repeater_multicast’.
- APAR IY60565: Massive usage of wlssub causes meory leak in gateway proces.
- APAR IY60800: Reexecing the oserv can cause the gateway process to crash.
- APAR IY60842: The gateway process spawns lots of method threads and sometimes hangs.
- APAR IY60920: LCFD process spikes to 40 to 60% of cpu usage.
- APAR IY61281: Distribution interrupted for endpoints logged after retry_ep_cutoff.
- APAR IY61488: LCFD leaks memory when upcall_proxy is enabled.
- APAR IY61726: The ’wruntask’ hangs and repository_skel1 leaks memory.
- APAR IY61731: The ep_mgr cores if allow_nat=true and endpoint hostnames not resolvable.
- APAR IY62005: The endpoint login fails and lcfd hangs.
- APAR IY62059: The gateway crashes during Mdist1 operations.
- APAR IY62172: The oservlog error message needs to provide more information.
- APAR IY62489: The ’wruntask -m staged’ does not accept valid input for -s.

- APAR IY62621: The mobile client startup usablity problems.
- APAR IY62711: The rpt2 debug_level is not affective until process restarts.
- APAR IY62831: Purging mdist depot can cause core.
- APAR IY62833: The ep_lock causes excessive gateway threading.
- APAR IY62895: The wnavpop script has syntax error for adding software package.
- APAR IY62898: The winstlcf fails for windows 2003 endpoints.
- APAR IY62983: The distribution manager does not wake up when database is connected.
- APAR IY63028: The wunstmn script has error in line 1123.
- APAR IY63058: Reinstall endpoint won't re-use the existing guid.
- APAR IY63119: Unix desktop displays password in clear text.
- APAR IY63350: The HTML ouput option in ″wepstatus -f htm″ doen't work.
- APAR IY63396: The jcf.jar needs to drop stale connections from TEC server.
- APAR IY63563: LCFD crashes during upcall processing.
- APAR IY63564: The endpoint manager getting into state where it runs slow.
- APAR IY63972: Memory leak in ntfserver due to inventory flooding notices.
- APAR IY64359: Wrong message in the gatelog is logged.
- APAR IY64417: The 'wupdate -r endpoint <tmr>″ fails randomly.
- APAR IY64539: The 'wgateway <gw> set update_gwalias 0' command does not properly.
- APAR IY64581: The LCF_DATDIR is not exported in the lcfd environment.
- APAR IY64599: The retry_ep_cutoff does not reset when data is successfully.
- APAR IY64729: The wepupgd & winstlcf fails if a bad -l parameter is passed.
- APAR IY65286: The policy region parents attribute is corrupted.
- APAR IY65572: The ″wgettask -f″ creates incorrect keyword.
- APAR IY65631: Two VPN endpoints may get the same name and dispatcher number.
- APAR IY66226: Windows desktop displays garbage characters.
- APAR IY66390: Mdist2 allows invalid value to be set for mem_max.
- APAR IY66571: Can't reserve 2147483647 KB in the depot.
- APAR IY66595: With SBDBT enabled, a bdt channel may still be opened on an incorrect port.
- APAR IY66599: endpoint mdist2 timeout hard coded too short during method.
- APAR IY66641: The wstandalone command does not complete all required steps.
- APAR IY66675: The mobile console does not reflect current status.
- APAR IY66699: The multicast in-progress error during multicast distributions.
- APAR IY66711: The winstlcf fails to install endpoint on WindowsXP SP2.
- APAR IY66812: setup_env.sh-multiple sourcing of this cause problems with grep.
- APAR IY66813: The spider fails to parse environment variables.
- APAR IY66882: Unencrypted password is sent to a java client, in a disconnect request.
- APAR IY67019: The roles for mdist commands are not consistant with documentation.
- APAR IY67148: The collection_prog1 leaks memory.
- APAR IY67182: LCFD crashes when allow_proxy_upcalls is set to ″true″.

- APAR IY67409: The admin_prog1 command leaks memory.
- APAR IY67431: The gateway crashes on endpoint migration.
- APAR IY67620: LCFD on Microsoft cluster fails with wsaprotocol_info error.
- APAR IY67809: An attempt to delete profiles does not delete all copies.
- APAR IY67870: The epproxy leaks memory.
- APAR IY67910: The wtll aborts if implementation is a file.
- APAR IY68031: LCFD logs ″preferenced account is currently locked″.
- APAR IY68160: Jobs results can’t be saved in a file.
- APAR IY68240: After changing mobile gui preferences, GUI may not restart.
- APAR IY68277: The TEC adapter leaks memory when LCFD is stopped.
- APAR IY68346: A negative dispatcher number is displayed in odstat output.
- APAR IY68611: The winstlcf fails to install an Unix endpoint.
- APAR IY68682: Disabled scheduled jobs are purged when next execution time has passed.
- APAR IY68799: The wepstatus -v is causing an coredump on ix86 platforms.
- APAR IY68832: The wdepot exit codes are not consistent.
- APAR IY69028: The wping does not work is NAT is enabled.
- APAR IY69226: LCFD crashes on shutdown if detect_address_change is set.
- APAR IY69510: The TMF scheduler may terminate abnormally.
- APAR IY69511: when ep migrates from one multicast gw to another 2.
- APAR IY69645: The endpoint manager leaks memory.
- APAR IY69758: In correct status reported by ″wep″ command.
- APAR IY69950: An unexpected behaviour using wmdist -n option.
- APAR IY70216: In correct endpoint healthcheck reports error codes 7,8,9.
- APAR IY70252: A distribution does not expire at the requested deadline.
- APAR IY70413: The endpoints mcast_receiver.cfg gets overwritten by gateway.
- APAR IY70649: The wol_direct can’t be set using wgateway command.
- APAR IY71514: The wepstatus -v output is incomplete.
- APAR IY71993: The oserv can terminate when it is passed a bad password.
- APAR IY72659: The repository_skel1 process grows during MQ domain deletions/creations.
- APAR IY72991: The Mdist2 does not handle exceptions correctly.
- APAR IY73005: Incorrect status displayed if a package is canceled through APM.
- APAR IY73491: The gateway proxy is unable to handle improperly formatted data.
- APAR IY73622: The gateway crashes if oserv is unresponsive.
- APAR IY73687: The wformatvalue returns extraneous comma on RH Linux.
- APAR IY73719: The wgetprf fails with an error ″general failure″.
- APAR IY73810: The diag_accts=false is not persistent in last.cfg.
- APAR IY74447: The WOL does not work after applying SP1 on Windows 2003.
- APAR IY74876: The wdepot core dumps with incorrect syntax.
- APAR IY75242: The ’files_transfer’ idlcall fails on Windows target.
- APAR IY75955: The LCFD crashes shortly after start.
- APAR IY75986: The install_info process leaks memory.
- APAR IY76364: The multicast re-dist fails if previous dist not complete.

- APAR IY76776: The installation of Linux endpoints fails.
- APAR IY76840: The wsettask does not on 4.1.1-TMF-0048 patch.
- APAR IY76867: The diag_accts=false does not prevent checking of admin accounts.
- APAR IY77008: The tnr_prog1 process leaks memory when read-thru is enabled.
- APAR IY77089: LCFD upcall can cause HMAC errors.
- APAR IY77095: The wtll causes collection_prog1 to crash.
- APAR IY77127: The wep_post_interval option does not work on LCFD.
- APAR IY77288: LCFD terminates without any errors on windows 2000.
- APAR IY77371: The ″odadmin trace off″ command is not working.
- APAR IY77472: The distribution source host RPT2 can loop under load.
- APAR IY77720: The rpt2 process leaks memory.
- APAR IY77830: Can not find endpoint manager OID when read through is enabled.
- APAR IY77885: Duplicate repeater object is created when gateway is created.
- APAR IY78215: The Tivoli desktop crashes.
- APAR IY78263: A distribution by Mdist2 does not work properly.
- APAR IY78396: The lcs.machine_unique_id is corrupted during endpoint upgrade.
- APAR IY78772: The rim_oracle_agent dumps core.
- APAR IY78855: The TMF scheduler is not working correctly after DTS change.
- APAR IY79438: The wep_set_interfaces is not working on Netware endpoints.
- APAR IY79927: LCFD crahses during restart.
- APAR IY80172: The gateway has performance problem if endpoint health check is enabled.
- APAR IY80238: The wtll exits without error when cpp is not found.
- APAR IY80239: The lcf_env.csh fails on multiple platforms.
- APAR IY80246: The lcs.machine_unique_id can not be set.
- APAR IY80827: Change the syntax of %tmepsswd% in md2gui.bat.
- APAR IY80895: Loading depot during data collection can corrupt MDist2 database.
- APAR IY81833: The custom boot method fails to run.
- APAR IY81876: Windows commands using special characters (″″\″″ ″″|″″) are not working.
- APAR IY81910: Collection_prog1.exe exits with status 6.
- APAR IY83177: The gateway retry function to prevent ″ipc shutdown″ in eplogin thread.
- APAR IY83260: The endpoint manager leaks memory.
- APAR IY83541: The shapshot script doesn’t cover correct tar return codes on Linux.
- APAR IY83703: ″wgetsched can core if ″″-v″″ flag is used and corrupted jobs″.
- APAR IY83820: The status_time label is missing from ″wep ls -i all″ output.
- APAR IY83963: Certain wake-on-lan events fail to wake up the endpoint.
- APAR IY83969: The missing error.htm file can crash the gateway.
- APAR IY84086: The ntconfig is not checking tivoli_admin_privileges group.
- APAR IY84225: The mobile client unusable if login user cannot access mobile.cfg.

- APAR IY84491: Failed to login via desktop for windows.
- APAR IY84611: The tec_dispatch crashes when using SSLA.
- APAR IY85114: The wmdist -la reports incorrect ″completed″ count and percentage.
- APAR IY85120: TAP fails to authenticate on certain domain controllers.
- APAR IY85979: The endpoint GUID is used as LCFD ID.
- APAR IY86193: The wmdist -q reports old endpoint label.
- APAR IY86728: The mdist2 allows consumption of depot space beyond disk_max.
- APAR IY86761: The framework web access cannot download static content.
- APAR IY87069: The get_rpt_format method is not relaseing endpoint cache lock.
- APAR IY87109: Incorrect error message on ″wep <ep> status″ call.
- APAR IY87159: The Linux gateway fails to start. APAR IY87262: LCFD responds to login reply to timed out request.
- APAR IY87678: ″Text file busy″ message during tecad_logfile upgrade.
- APAR IY87696: Unable to manage paused distributions if endpoint isolates.
- APAR IY87989: The RIM replaces accented characters in non-English version of Oracle with the ″?″.
- APAR IY88003: what is the maximum job id and what happens if it is reached?
- APAR IY88162: tivoli desktop doesn’t show the restricted job correctly.
- APAR IY89137: mcast_receiver.exe has encountered a problem and needs to close.
- APAR IY89307: LCFD HTTP interface does not accept the last parm specified.
- APAR IY89601: LCFD crashe may cause endpoint corruption in config files.
- APAR IY89618: LCFD UDP initial login fails.
- APAR IY89733: Error code ora-01003 received when updating the INV RIM database.
- APAR IY89823: Reordering entries in mobile console does not work properly.
- APAR IY89874: The RPT2 process crashes on Linux.
- APAR IY90105: The endpoint manager fails if it is passed a null endpoint address.
- APAR IY90444: The mobile.exe gets visual c++ runtime error.
- APAR IY90450: LCFD crashes on windows 2000.
- APAR IY90622: The orphaned endpoint login fails.
- APAR IY91100: The distributions may become interrupted or fail.
- APAR IY91248: The wlssub doesn’t list profile manager(s).
- APAR IY91488: The wepupgd command can crash the gateway.
- APAR IY91852: The ″winstlcf -j″ command returns ″tivoli endpoint install failed″.
- APAR IY92193: The winstlcf can not install an endpoint.
- APAR IY92369: The wmdist shows garbled output, if a SP distribution fails.
- APAR IY92576: The EPSTATUS data in gatelog has a space.
- APAR IY92587: The tmf_sched leaks memory.
- APAR IY92983: The endpoint manager crashes during login storms.
- APAR IY93460: Display endpoint IP address in HMAC error message in the gatelog.
- APAR IY94068: TEC adapter on 390 z/linux leaks file discripter.

- APAR IY94232: Task execution on Managed Node is different than same task execution on EP.
- APAR IY94400: The ″wep boot_method list <tag> <ep>″ returns garbage.
- APAR IY94649: The GUI patch install diaglog will not open in certain conditions.
- APAR IY95072: wbkupdb fails if disk space in more than 4.5GB.
- APAR IY95083: Solaris gateway cores.
- APAR IY95090: Oserv crashes when running ″gwlist start <bad_gw_oid>″
- APAR IY95617: fw task executing from activity plan reports wrong status to
- APAR IY96219: Lookup accountname failure.
- APAR IY96381: DES encrypttion displays incorrectly and is misleading.
- APAR IY96474: Mobile suppress the pop-up for any state other than ″paused″.
- APAR IY96789: The endpoint stays in ″initializing″ state when system comes out of stand-by mode.
- APAR IY97940: Logging long string to lcfd.log file can crash endpoint.
- APAR IY99595: The TMR install fails if /etc/tivoli/bin or /etc/tivoli/lib exists.
- APAR IZ01257: The scheduler email function makes garbled japanese ″subject″.
- APAR IZ01424: The oserv hangs at startup if TMFMON is enabled.
- APAR IZ02490: add_object marshalling exception.
- APAR IZ02656: The upcall on an endpoint may crash, if the system runs out of file descriptors.
- APAR IZ03492: Installing endpoint on windows vista gets error message.
- APAR IZ03758: Disabled widmap user causes port leak on endpoint.
- APAR IZ04886: The endpoint fails to start when temp_dir is set to ″″.
- APAR IZ06029: The epmgrlog file grows above set limit.
- APAR IZ07314: CLOSE_WAIT's build up on the gateway.
- APAR IZ07491: Two multicast receivers started on SUSE Linux endpoint.
- APAR IZ14274: The wruntask command core dumps.
- APAR IZ14739: Forwarding a notice group message on AIX 5.3 yields ″commas″.
- APAR IZ15686: Endpoint crashes on windows vista APAR IZ18235: heapdump of java apm process.
- APAR IZ20238: wmdist -l loops after setting bind variables.
- APAR IZ22845: The endpoint manager crashes due to internal processing.
- APAR IZ23770: The wbkupdb objsnapshot uses wrong path on LINUX.
- APAR IZ24316: The wtll fails to create task.
- APAR IZ24819: Unable to specify tasks arguments when scheduling a job.
- APAR IZ24823: The gateway shows false endpoint health check messages.
- APAR IZ26786: ″scheduling a job with ″″date=28th″″ + ″″-r '1 month'″″, next date i″.
- APAR IZ28527: The wruntask with the ″-a″ argument of japanese chars fails.

Chapter 2. Installation and upgrade notes

This chapter contains the following information:
- Determining operating system patch levels and swap space
- System, disk space, and database requirements
- Installation and product notes
- Interpreter type mappings

Determining operating system patch levels

Table 1 shows the commands used to display which operating system level or patches are installed on various systems supported by Tivoli Management Framework.

Table 1. Commands for determining operating system level and installed patches by operating system

Operating system	Example
IBM® AIX®	`instfix -a`
HP-UX	`swlist`
IBM OS/400®	To determine the operating system level, use the **dspsfwrsc** command. To determine what patches are installed, use the **dspptf** command.
Sun Solaris	To determine if a patch is installed, look for a directory with that name in `/var/sadm/patch`.
Microsoft® Windows®	Open Windows Explorer and click **About Windows** in the **Help** menu.

Determining operating system swap space

Table 2 shows the commands used to display the amount of swap space and the number of process slots on various systems supported by Tivoli Management Framework.

Table 2. Commands for determining swap space and process slots by operating system

Operating system	Swap space	Process slots
IBM AIX	**/usr/sbin/lsps –a**	**/usr/bin/sar –v**
HP-UX	**/etc/swapinfo**	**/usr/bin/sam**
Sun Solaris	**/usr/sbin/swap –s**	**/usr/bin/sar –v**
Microsoft Windows	In the **System Properties** dialog on the **Control Panel**, select the **Performance** tab, and click **Change**	N/A

Refer to your operating system documentation to increase the amount of swap space or the number of process slots on your system.

System requirements

This section describes the operating system software and hardware requirements for Tivoli Management Framework resources. For information about additional system requirements for Asian languages, see "System requirements for Asian environments" on page 48.

Tivoli Enterprise software has specific software and hardware prerequisites that must be met before it can be installed and considered functional. These requirements include operating systems, hardware platforms, relational and object database management systems, e-mail and Web servers, and support libraries. The prerequisites listed in this document are the recommended environment for Tivoli Enterprise software at the time of publication. Tivoli Enterprise software is supported only when used with prerequisites that are officially supported by the third-party vendor.

Many vendors unilaterally withdraw support for their products on a regular basis. IBM reserves the right to unilaterally withdraw support for its software based on the availability of support from a vendor for any prerequisite software. Contact the vendor of any prerequisite software if you have questions about its current support.

This section contains information about the supported operating system versions for each supported hardware platform. IBM does not distribute or maintain operating system patches from hardware vendors, except for IBM operating systems. Contact your hardware vendor for information about obtaining and installing the most current operating system patches. If you do not know how to contact your hardware vendor, contact your IBM support provider for details on the recommended procedure.

For detailed list of supported operating systems, please refer to the following URL:
`http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivoliManagementFramework.html`

Table 3 lists which Tivoli Management Framework resources (Tivoli server, managed node, gateway, endpoint) are supported on which operating systems.

Table 3. Resource types supported on operating systems

Operating system	Resource type
AIX	Tivoli server Managed node Gateway Endpoint
HP-UX	Tivoli server Managed node Gateway Endpoint
Linux on Intel®	Tivoli server Managed node Gateway Endpoint
Linux on PowerPC®	Tivoli server Managed node Gateway Endpoint

Table 3. Resource types supported on operating systems (continued)

Operating system	Resource type
Linux on zSeries	Tivoli server Managed node Gateway Endpoint
NetWare	Gateway (supported at the Tivoli Management Framework 4.1.1) Endpoint
OS/2®	Gateway (supported at the Tivoli Management Framework 4.1.1) Endpoint
OS/400	Endpoint
OS/390®®	Endpoint
Solaris on SPARC Solaris on Intel	Tivoli server Managed node Gateway Endpoint
Windows 2000 Professional Windows XP Professional Windows Vista Professional	Endpoint
Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition Windows Server 2003, Datacenter Edition Windows Server 2008	Tivoli server Managed node Gateway Endpoint

AIX operating system on pSeries and PowerPC systems

The following Tivoli resources are supported on AIX 5.1, AIX 5.1C, AIX 5.2, AIX 5.2B or AIX 6.1 on pSeries®® and PowerPC systems in 32-bit mode:

- Tivoli server
- Managed node
- Gateway
- Endpoint

For AIX 5.1, you must install maintenance level 5100-01.

Note: Before installing maintenance level 5100-01, you must apply and commit APAR IY19375 using the AIX System Management Interface Tool (SMIT). This fix includes the following filesets:

- bos.mp64 5.1.0.1
- bos.mp 5.1.0.1
- bos.up 5.1.0.1

After installing these filesets, reboot the system, install maintenance level 5100-01, and reboot the system again.

These maintenance levels and fixes can be downloaded from the following site:

http://techsupport.services.ibm.com/rs6000/fixes

RS/6000 systems with the POWER processor are not supported.

HP-UX operating system on HP 9000 systems

The following Tivoli resources are supported on HP 9000/700 or 800 series with the PA RISC 1.1 or PA RISC 2.0 architecture running HP-UX 11i or HP-UX 11.0:

- Tivoli server
- Managed node
- Gateway
- Endpoint

For HP-UX 11i, you must install Quality Pack GOLDQPK11i

For HP-UX 11, you must install Quality Pack QPK1100

The quality pack bundles can be downloaded from the following site:

http://www.software.hp.com/SUPPORT_PLUS/qpk.html

Java™ support can be downloaded from the following site:

http://www.hp.com/products1/unix/java/infolibrary/patches.html

Linux on Intel systems

The following Tivoli resources are supported on Linux on Intel® or Pentium®® systems running Red Hat Advanced Server 3.0, 4.0 or 5.0; SuSE SLES 9.0 or 10.0:

- Tivoli server
- Managed node
- Gateway
- Endpoint

Linux on PowerPC systems

The following Tivoli resource is supported on Linux on PowerPC iSeries or pSeries systems running Red Hat Advanced Server 3.0, RHEL 4 or 5, SuSE Linux SLES 9 or 10:

- Tivoli server
- Managed node
- Gateway
- Endpoint

Note: Multicast is not supported on Linux on PowerPC systems.

Linux on zSeries systems

The following Tivoli resources are supported on IBM S/390® G5, G6, or MP3000 system with the Linux 2.4 kernel running Red Hat Advanced Server 3.0, RHEL 4 or RHEL 5 on zSeries®, SuSE Linux SLES 9 or 10 on zSeries:

- Tivoli server
- Managed node
- Gateway
- Endpoint

Linux on S/390 does not support a native Tivoli desktop. You can install Tivoli Desktop for Windows on another system and connect to a Linux on S/390 managed node.

OS/400 systems

The following Tivoli resource is supported on V5R1, V5R2 and V6R1 of IBM OS/400:

- Endpoint

You must ensure that the following communication protocols are active to transfer files to and from OS/400 endpoints in the Tivoli environment:

- TCP/IP communications
- File Transfer Protocol (FTP) services

Notes:

1. Multicast is not supported on OS/400.
2. You cannot install multiple endpoints to an OS/400 system.

Solaris operating environment on Sun SPARC and Intel systems

The following Tivoli resources are supported on Solaris 8, Solaris 9, or Solaris 10 on Sun SPARC and Solaris 10 on Intel:

- Tivoli server
- Managed node
- Gateway
- Endpoints

For Solaris operating systems, you must install Patch Clusters with a date of January 2002 or later.

Additional information for downloading patches is available from the following site:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

Additional information regarding Java support is available from the following site:

http://java.sun.com/j2se/1.3/install-solaris-patches.html

Windows operating system on Intel systems

The following Tivoli resources are supported on Windows Server 2003, Datacenter Edition; Windows Server 2003, Standard Edition; or Windows Server 2003 Enterprise Edition; Windows Server 2008, Enterprise Edition; :

- Tivoli server
- Managed node
- Gateway
- Endpoint

The following Tivoli resource is supported on Windows 2000 Professional with Service Pack 3 or Service Pack 4 and Windows XP Professional with Service Pack 1; or Windows Vista Professional:

- Endpoint

Note: Tivoli Management Framework does not support multiuser add-ons such as Windows Terminal Server, WinDD, or Citrix Metaframe. When running with a multiuser add-on, Tivoli Management Framework manages this machine as a single entity.

Tivoli Management Framework also does not support the **lcfep** process in the environments where Windows Terminal Servers, Remote Desktop, or Fast User Switching is installed. **lcfep** checks for the presence of these programs when it is started, and if any of them exist in the registry, the program immediately exits. **lcfep.exe** will not show in the list of running processes, and its Task Bar icon will not be displayed. This generally affects any ″server″ edition of Windows (for example, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server) and newer versions of Windows for workstations, such as Windows XP and Windows Vista. Disabling these services does not allow **lcfep** to run; they must be uninstalled before **lcfep** can function.

Browsers requirements

Depending on the operating system, the requirements for browsers differ. Browsers are used to access and display Tivoli Management Framework Web contents.

Note: For any Web browser, ensure that you have the latest security patch installed on your operating system. These patches can be downloaded from the Web site of the vendor.

The supported minimum and maximum versions are as follows:

- For all other operating systems, you must use at least Netscape, Version 4.72. However, some applications do not support Netscape, Version 6.0 or higher; consult the application documentation for more information.
- For all Windows operating systems, you must use at least Internet Explorer, Version 5.5 with service pack 1, but you can use any version of Internet Explorer up to and including Version 6.0. However, some applications do not support Internet Explorer, Version 6.0; consult the application documentation for more information. With any version of Internet Explorer, you must use the version with 128-bit encryption.

SSL security packages requirements

It is mandatory that if you decide to enable SSL in your Tivoli Framework Release 4.3.1 Environment, then the entire environment must be at Tivoli Framework Release 4.3.1. The TMR and the Managed Nodes at Tivoli Framework Release 4.3.1 will not communicate with TMR or Managed Nodes at Tivoli Framework Release 4.1.1 or older.

SSL-A package requirements

SSL encryption using the Tivoli Management Framework SSL-A package is fully supported for single-port bulk data transfers communication channels on all systems that Tivoli Management Framework, Version 4.3.1 supports, with the following exceptions:

- Only available for oserv communication channels, not for BDT, on HP-UX and Linux.
- Not supported by gskit on NetWare.

Upgrade from Tivoli Management Framework 4.1.1 requirements

The steps in upgrading a Framework 4.1.1 environment to Framework 4.3.1 when SSL is used:

- Make a system backup of the installation. A system backup such as a tarball will contain the entire installation (database, binaries, data files) as opposed to wbkupdb which only backs up the database.
- Turn off SSL on all Managed Nodes in the installation.

  ```
  odadmin set_network_security none all
  odadmin shutdown clients
  odadmin reexec 1
  odadmin start clients
  ```
- Upgrade all Managed Nodes to Framework 4.3.1. Upgrading Managed Nodes will distribute new certificates to these Managed Nodes.
- Install SSLA (GSkit 7) on all Managed Nodes in the installation. Restart the oserv for each Managed Node and verify that odadmin reports Network Security = none / SSL capable.
- Turn on SSL on Managed Nodes.

  ```
  odadmin set_network_security SSL all
  odadmin shutdown clients
  odadmin reexec 1
  odadmin start clients
  ```
- Verify that all the managed nodes restarted successfully.
- Use the ″odadmin odinfo″ command to verify that SSL is enabled on all managed nodes. You can now change the network security level of managed nodes to SSL or FORCE_SSL if you need to.

Chapter 3. SSH Requirements

Tivoli Management Framework, Version 4.3.1 supports OpenSSH 3.6.1 and later for secure shell (SSH) connection for remote installations of managed nodes and endpoints as long as all relevant OpenSSH patches are also installed.

Note: You cannot use SSH to perform installations on OS/400, and Windows targets.

If you are going to use Cygwin with SSH, review the Cygwin documentation for any issues that might affect your environment.

Chapter 4. Web server requirements for Tivoli Web interfaces

You can use any Web server that supports the Servlet 2.2 specification with the Tivoli Web interfaces. However, the Tivoli Web interfaces were certified against the following Web servers:

- IBM WebSphere® Application Server, Advanced Single Server Edition, Version 4.0
- IBM WebSphere Application Server, Enterprise Edition, also called the Enterprise Application Server, Version 4.0.2
- IBM WebSphere Application Server — Express, Version 5
- IBM WebSphere Application Server, Version 5
- Jakarta Tomcat 3.2.3

Chapter 5. Disk space requirements

This section describes the disk space requirements for the following:

- Tivoli servers, managed nodes, and gateways
- Endpoints

Do not place files for Tivoli Enterprise products on a remote file system or share Tivoli Management Framework files among systems in a Tivoli environment.

Required disk space for any product can be estimated by checking the size of the installation folder for that product and calculating that the uncompressed value will be 20% to 70% larger. For example, if the JAVA folder is 100 MB, the actual installation size will be between 120 MB and 170 MB.

Tivoli servers, managed nodes, and gateways

The following table lists the estimated disk space required for Tivoli Management Framework. The estimated disk space includes space for the Tivoli libraries, binaries, server database, client database, manual (man) pages, and message catalogs. The binaries include the lcf bundles for all supported releases.

Operating System	Libraries	Binary files	Server database	Client database	Manual pages	Message catalogs
AIX	28 MB	220 MB	30 MB	10 MB	1.3 MB	1 MB
HP-UX	22 MB	220 MB	30 MB	10 MB	1.3 MB	1 MB
Linux	19 MB	220 MB	30 MB	10 MB	1.3 MB	1 MB
Solaris	17 MB	220 MB	30 MB	10 MB	1.3 MB	1 MB
Windows	220 MB in the same location		30 MB	10 MB	N/A	1 MB

The following table presents the minimum memory requirements for Tivoli Management Framework.

Operating System	Tivoli server	Managed node (with Tivoli desktop)	Managed node (without Tivoli desktop)
AIX	128 MB	128 MB	N/A
HP-UX	128 MB	128 MB	N/A
Linux	128 MB	128 MB	N/A
Solaris	128 MB	128 MB	N/A
Windows	128 MB	128 MB	128 MB

As each Tivoli Enterprise product is added to your Tivoli environment, additional disk space is required. Refer to the appropriate documentation for planning information and additional disk space requirements.

Endpoints

The endpoint client uses less than 2 MB of memory. It runs on any system configured to the recommended specifications of the vendor.

Chapter 6. RDBMS requirements

This section provides information about the supported client and server database for each supported operating system, detailed information about each relational database management system (RDBMS), tips for installing and configuring the RDBMS software for use with Tivoli Enterprise products, and troubleshooting information.

This information is intended for database administrators and others responsible for installing and configuring the RDBMS. Refer to the database vendor documentation to understand the implications of these tasks and for complete instructions about performing these tasks.

Consider the following information while configuring and using the RDBMS Interface Module (RIM):

- The database client software must be properly installed and tested on the RIM host for database connectivity.
- When creating a RIM object with the **wcrtrim** command, the password is limited to eight characters unless you use the **–i** option.
- You can configure multiple Tivoli Enterprise products to use a single database instance or combined application schemas. If you choose to use a configuration with a single database instance, consult a qualified database administrator about tuning the database server to ensure the best performance for each application involved. In addition, you should thoroughly test your environment to ensure that it works properly.
- The RIM host requires a 32-bit client for all supported RDBMSes except Oracle. The database server can be either 32-bit or 64-bit. If the RIM host is on the same system as the 64-bit database server, you must install the 32-bit database client in a separate directory and you must configure the RIM object to reference the 32-bit client directory, for example by using the **wcrtrim –H** or **wsetrim –H** command.

Supported RDBMS servers

The following table lists the supported server databases for each operating system.

Operating system	Supported database servers
AIX	• DB2®[1] 8.1, 8.2, 9 • Informix® 9.4 • Oracle[3] 10g, 11g • Sybase 12.5.4
HP-UX	• DB2[1] 8.1, 8.2, 9 • Informix 9.4 • Oracle[3] 10g, 11g • Sybase 12.5.4

Operating system	Supported database servers
Linux on Intel	• DB2[1] 8.1, 8.2, 9 • Informix 9.4 • Oracle[3] 10g, 11g • Sybase 12.5.4
Linux on zSeries	• DB2[1] 8.1
Solaris on Sparc	• DB2[1] 8.1, 8.2, 9 • Informix 9.4 • Oracle[3] 10g, 11g • Sybase 12.5.4
Solaris on Intel	• Oracle[3] 10g
Windows	• DB2[1] 8.1, 8.2, 9 • Informix 9.4 • Microsoft SQL Server 2000 SP4, 2005 SP1, 2008 • Oracle[3] 10g, 11g • Sybase 12.5.4
z/OS	• DB2[2] 7

[1] Support for Enterprise Edition (EE), Enterprise-Extended Edition (EEE), and Workgroup Edition.

[2] Only the DB2® server is supported on z/OS® operating systems.

[3] Support for Enterprise Edition and Standard Edition.

Upgrade note: Because of changes in the supported version of Oracle software, different upgrade scenarios must be used. The following information will help you decide your required upgrade path to maintain a working Tivoli environment.

- Tivoli Management Framework, Version 4.3.1 supports Oracle 10g and Oracle 11g.
- Tivoli Management Framework, Version 4.1.1 supports Oracle 8.1.7 and Oracle 9i (Release 2).
- Tivoli Management Framework, Version 3.7 Revision B, Tivoli Management Framework, Version 3.7.1, and Tivoli Management Framework, Version 4.1 support Oracle 8.1.7.
- Tivoli Management Framework Version 3.7.1 and Tivoli Management Framework, Version 4.1.1 support Oracle 9i (Release 2).

Requirements for DB2 clients by server version

The following table lists the supported DB2 client installations for each supported operating system.

Operating System	DB2 Server	
	DB2 UDB Version 8.x	**DB2 9 for Linux, UNIX, and Windows**
AIX	DB2 8.x Runtime Client	DB2 9.x Runtime Client

Operating System	DB2 Server	
	DB2 UDB Version 8.x	DB2 9 for Linux, UNIX, and Windows
HP-UX	DB2 8.x Runtime Client	DB2 9.x Runtime Client
Linux on Intel	DB2 8.x Runtime Client	DB2 9.x Runtime Client
Linux on zSeries	DB2 8.x Runtime Client	DB2 9.x Runtime Client
Solaris	DB2 8.x Runtime Client	DB2 9.x Runtime Client
Windows	DB2 8.x Runtime Client	DB2 9.x Runtime Client

Requirements for Informix clients by server version

You *must* use unbuffered logging with all Informix databases. Do *not* use American National Standards Institute (ANSI)-mode logging. If you do not switch from ANSI-mode logging to unbuffered logging, you might experience problems with database locks that cause Tivoli programs to hang. To switch to unbuffered logging, you need to back up, delete, and then re-create all of your databases used by Tivoli Enterprise products.

Refer to the Informix documentation for complete instructions about switching to unbuffered logging. The following steps provide a high-level description of the procedure:

1. Create a level 0 archive of the databases to replace.
2. Export existing tables using the **dbexport** command with the **–ss** option.
3. Drop current databases configured with ANSI-mode logging.
4. Create new databases configured with unbuffered logging.
5. Import the exported tables from step 2 into the new databases created in step 4 by using the **dbimport** command.

The following table lists the supported Informix client installations for each supported operating system.

Operating System	Informix Server 9.4
AIX	SDK 2.81
HP-UX	SDK 2.81
Linux on Intel	SDK 2.81
Solaris	SDK 2.81
Windows	SDK 2.81

Notes:

1. Testing has shown that Informix can have concurrency problems in a high-transaction or high-volume Tivoli environment. Under these conditions, tune your Informix server carefully to ensure that you do not have locking problems that result in data loss. Enabling row-level locking can resolve the locking problems with IBM Tivoli Enterprise Console®® in certain environments. You should consult a qualified Informix database administrator to determine the best lock mode for your environment.

   To set lock mode to row-level locking, run the following command on all tables:

```
ALTER TABLE table_name LOCK MODE (ROW);
```

where *table_name* is the name of the table to be set to row-level locking.

Requirements for Microsoft SQL Server clients by server version

In Tivoli Management Framework, Version 4.3.1, the RDBMS interface module (RIM) uses ODBC to connect to a Microsoft SQL Server database rather than using a Microsoft SQL Server client. Therefore, you must create an ODBC data source to enable RIM to connect to a Microsoft SQL Server database. For more information about creating an ODBC data source, see the chapter about using RIM objects in the *Tivoli Enterprise Installation Guide*.

Requirements for Oracle clients by server version

The following table lists the supported Oracle client installations for each supported operating system.

Operating System	Oracle Server 10g	Oracle Server 11g
AIX	10g	11g
HP-UX	10g	11g
Linux on Intel	10g	11g
Linux on PPC	10g	Not supported
Solaris on Sparc	10g	11g
Solaris on Intel	10g	Not Supported
Windows	10g	11g

Notes:

1. On AIX systems, connection problems might persist if the proper boot parameters are not set for the AIX operating system to run with asynchronous I/O. For details on resolving this issue, see "Upgrading Tivoli Management Framework on AIX operating systems when an Oracle client is installed" on page 37.
2. For Japanese, Simplified Chinese, or Korean environments, you must install the Oracle client. If not fully installed on your UNIX® RIM host, you can experience connectivity problems.
3. The TNS_ADMIN and LOCAL environment variables are not supported. If you need to store your `tnsnames.ora` file in a location other than `$ORACLE_HOME/network/admin` directory, create a link or copy the file to that directory.

Requirements for Sybase clients by server version

The following table lists the supported Sybase client installations for each supported operating system.

Operating System	Sybase Server 12.0	Sybase Server 12.5
AIX	SDK 12.0	SDK 12.5
HP-UX	SDK 12.0	SDK 12.5
Linux on Intel	SDK 12.0	SDK 12.5
Solaris	SDK 12.0	SDK 12.5

Operating System	Sybase Server 12.0	Sybase Server 12.5
Windows	SDK 12.0	SDK 12.5

Chapter 7. Installation and product notes

Consider the following important information before installing Tivoli Management Framework or while using the product.

Installation notes

This section contains important information that you should consider when installing Tivoli Management Framework or using its installation mechanisms to install other Tivoli Enterprise software. It contains the following topics:

- "General installation notes"
- "Upgrading to Tivoli Management Framework, Version 4.3.1" on page 37
- "Upgrading Tivoli Management Framework when Tivoli Security Management is installed" on page 37
- "Upgrading Tivoli Management Framework on AIX operating systems when an Oracle client is installed" on page 37

General installation notes

- When you perform a new installation of a Tivoli Management Framework, Version 4.3.1 endpoint and the general globally unique identifier (GUID) does not already exist, Tivoli Management Framework creates a new GUID. However, when you upgrade an endpoint to Tivoli Management Framework, Version 4.3.1 and the GUID does not already exist, the general GUID that Tivoli Management Framework creates matches the lcf.id of the endpoint you are upgrading. Therefore, you might want to upgrade any existing endpoints on which you run inventory scans before installing or upgrading any endpoints on a system; this ensures the GUID matches the ID from previous inventory scans. In addition, in versions prior to Tivoli Management Framework, Version 4.3.1, if your system has multiple endpoints and you have not created the general GUID, you will have multiple entries for that system in the configuration repository. However, if you upgrade or install a Tivoli Management Framework, Version 4.3.1 endpoint on that system, only one entry will be updated in the configuration repository during subsequent inventory scans.
- When installing a Tivoli server for UNIX or Linux, the installation path that you specify cannot contain spaces.
- The default remote connection setting for Version 4.3.1 managed nodes is **version_2**. In versions prior to Version 4.1, installation of managed nodes used **version_1** as the default remote connection setting. To enable remote connections from Java clients using Tivoli Management Framework, Version 3.7.*x* use the odadmin command as follows:

  ```
  odadmin set_allow_rconnect TRUE
  ```

- Before installing a product or patch, verify that all managed nodes in your Tivoli management region (Tivoli region) are quiescent. (Refer to the **wlocktmr** and **lcfd** commands.)

  Do not share binaries between managed nodes or across Tivoli region boundaries. However, if your installation shares its binaries from an NTFS file server, use the file manager on the NTFS server that holds the binaries to clear all remaining network connections that pertain to the Tivoli installation directories. Perform this step before starting the installation.

This prevents errors that can occur during the installation of Tivoli Management Framework that result in files not being updated. This can happen because it is not possible to move or replace files in a directory when NTFS has a read lock that has not expired on the directory.

- Products are sometimes listed by the **wlsinst** command even when they cannot be uninstalled using the **wuninst** command. A common cause is that the product does not provide the uninstall script required by the **wuninst** command. Refer to the product documentation for information about how to uninstall these products.
- Products are sometimes listed by the **wlsinst –p** command even after they have been uninstalled from the Tivoli region. If you suspect this is happening, use the **wlsinst –p –v** command to check whether the product is installed on any systems in the Tivoli region.
- The root shell on UNIX managed nodes should be bash, Bourne, or Korn shell. During installation, shell commands are sent to the managed node. If the root shell on the target system is the C shell (csh) , these commands fail.
- For UNIX operating systems, ensure that you have enough file system space on Network File System (NFS)-mounted file systems to install Tivoli Management Framework and Tivoli Enterprise applications. If the file system lacks sufficient space, the installation hangs without providing an adequate indication of the problem. Contact your operating system provider to report NFS problems.
- Tivoli Management Framework installs the `msvcrt40.dll` file, the C runtime library, in the `%SystemRoot%\system32` directory on supported Windows operating systems for use by Tivoli Enterprise applications. This version of the runtime library is the one that is shipped with Microsoft Visual C++, Version 6.0. If the `%SystemRoot%\system32` directory contains a newer version of this file, Tivoli Management Framework copies the file located in `$BINDIR/mslib/msvcrt40.dll` to the following locations:
  - `%DBDIR%`
  - `$BINDIR/bin`
  - `$BINDIR/tools`

  If a Tivoli Enterprise application has command-line interface (CLI) programs that are not in the `$BINDIR/bin` or `$BINDIR/tools` directory, Tivoli Management Framework copies `$BINDIR/mslib/msvcrt40.dll` to the directories where the CLI programs reside. Complete the following steps if a Tivoli-based application runs a method that changes the current working directory and spawns a program that links with `msvcrt40.dll`. This procedure ensures that no incompatibilities occur between the C runtime library needed by Tivoli Enterprise applications and the one needed by non-Tivoli applications.

  1. Determine the directory where a command might reside by using the **type** command in the bash shell. The following example shows that the **wep** command is in the `$BINDIR/bin` directory:

     ```
     %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
     C:\>sh
     bash$ type wep
     wep is e:/Tivoli/bin/w32-ix86/bin/wep.exe
     bash$ echo $BINDIR/bin
     e:/Tivoli/bin/w32-ix86/bin
     ```

  2. Put a copy of the `$BINDIR/mslib/msvcrt40.dll` file in the new current working directory or the directory where the spawned program resides.

Upgrading to Tivoli Management Framework, Version 4.3.1

This section contains information on which CDs to use to install or upgrade Tivoli Management Framework, Version 4.3.1.

The following table describes which versions of Tivoli Management Framework to install and, where necessary, in which order. For installation information, see the *Tivoli Enterprise Installation Guide*.

If your current version is...	Follows these steps...
Version 3.6.5 Version 3.7, Revision B Version 3.7.1 Version 4.1, Revision 4.1.1	Upgrade to Tivoli Management Framework, Version 4.3.1 using the *Tivoli Management Framework Upgrade to Version 4.3.1 Upgrade* CD.
New installation	Install Tivoli Management Framework, Version 4.3.1 using the *Tivoli Management Framework, Version 4.3.1* (1 of 2) CD.

To enable Tivoli Management Framework for non-English environments, install the appropriate language packages from the *Tivoli Management Framework Language Support* CD after installing or upgrading Tivoli Management Framework.

Upgrading Tivoli Management Framework on AIX operating systems when an Oracle client is installed

To upgrade Tivoli Management Framework on an AIX operating system with an Oracle client, perform the following steps using the System Management Interface Tool (SMIT):

1. To change the characteristics of asynchronous I/O, enter the following command:

   ```
   smith chaio
   ```

2. From the menu, select **State to be configured at system restart**.
3. Change the value of this option from **defined** to **available**.
4. Press Enter.
5. Exit SMIT by pressing F10.
6. Restart the system by entering the following command:

   ```
   shutdown -r
   ```

Upgrading Tivoli Management Framework when Tivoli Security Management is installed

This section contains information related to Tivoli SecureWay®® Security Manager and Tivoli Access Control Facility that you should consider when upgrading Tivoli Management Framework:

- Always start an object dispatcher or endpoint using the full path to the daemon. Start the object dispatcher using **$BINDIR/bin/oserv**. Start the endpoint daemon using **$LCF_BINDIR/lcfd**.

  If you created or customized scripts that start the object dispatcher or endpoint, they must be edited. If you use the **oserv** or **lcfd** command from the command line, specify the full path.

  If you do not specify the full path to the oserv or endpoints, you cannot perform basic Tivoli Access Control Facility related functions, such as populating and distributing security profiles or running tasks.

- When upgrading Tivoli Management Framework on a UNIX Tivoli server or managed node where Tivoli Access Control Facility is installed, or when upgrading endpoints on which Tivoli Access Control Facility is installed, the following steps are required for a successful upgrade:
  1. Define root as a Tivoli Access Control Facility administrator using the **Add/Remove TACF Administrator/Auditor** task in the Tivoli Access Control Facility Tasks task library.
  2. Stop the Tivoli Access Control Facility daemons using the **Stop TACF Servers** task.
  3. Upgrade Tivoli Management Framework on affected systems. For more information about how to do this, see the *Tivoli Enterprise Installation Guide*.
  4. As root, use the **selang –l** utility to explicitly retrust **oserv** (and possibly **task_endpoint**) on a Tivoli server or managed node or to retrust **lcfd** on an endpoint. This is illustrated in the following examples.

     For a Tivoli server or managed node running Tivoli Access Control Facility, Version 3.6.*x*, that *has* been upgraded from Version 3.2:

     ```
     /usr/seos/bin/selang -l
     TACF> cr PROGRAM /path/oserv trust
     TACF> cr PROGRAM /path/task_endpoint trust
     TACF> quit
     ```

     For a Tivoli server or managed node running Tivoli Access Control Facility, Version 3.6.*x*, that *has not* been upgraded from Version 3.2:

     ```
     /usr/seos/bin/selang -l
     TACF> cr PROGRAM /path/oserv trust
     TACF> quit
     ```

     For an endpoint:

     ```
     /usr/seos/bin/selang -l
     TACF> cr PROGRAM /path/lcfd trust
     TACF> quit
     ```

     Note: You can create a task to perform the retrust on all the UNIX systems on which programs must be retrusted.
  5. Restart the Tivoli Access Control Facility daemons using the **Start TACF Servers** task.

  Note: You can remove the Tivoli Access Control Facility administrator role from **root** using the **Add/Remove TACF Administrator/Auditor** task in the Tivoli Access Control Facility Tasks task library.

Product notes

This section contains important information to consider when using Tivoli Management Framework. It contains the following topics:

- "General product notes"
- "Windows 2000 and Windows Server 2003 and 2008" on page 40

General product notes

- The **–e** option of the **lcfd** command is ignored and has no effect when the **lcfd** is started. An lcfd.id file is created and each endpoint returns a unique ID whether this option is specified or not. If there are multiple endpoints on one machine, each endpoint is installed in a different directory, and a separate lcf.id file is created for each endpoint.

- As a result of APAR IY30330, object dispatchers create additional threads to improve performance. The default value of 250 for **rpc_max_threads**, which sets the thread limit for concurrent remote procedure calls, should be sufficient for most deployments. However, some customers might need to increase the **rpc_max_threads** value using the **odadmin** command. If your **rpc_max_threads** value is set too low, you might see an error message such as "`method fork failed`" or "`RPC Request rejected outstanding threads: number_of_threads_running`."
- Kerberos and the following commands are disabled: **kadmin**, **kadmind**, **kdb_destroy**, **kdb_edit**, **kdb_init**, **kdb_util**, **kdestroy**, **kerberos**, **kinit**, **klist**, **kpasswd**, **ksrvtgt**, **kstash**.
- The following Tivoli GNU Revision Control System (RCS) commands are disabled: **wci**, **wco**, **widen**, **wmerge**, **wrcs**, **wrcsdiff**, **wrcsmerge**, **wrlog**.
- ADE and AEF are disabled.
- Tier 2 support is being deprecated and will be disabled at the next release of Tivoli Management Framework.
- The Tivoli desktop for OS/2 is supported at the Tivoli Management Framework 4.1.1 level.
- The OS/2 and NetWare gateways are supported at the Tivoli Management Framework 4.1.1 level.
- The SIS is supported at the Tivoli Management Framework 4.1.1 level.
- Commands run in the Tivoli environment are referred to as methods. To increase security, Tivoli runs methods with the lowest possible authority. This often means that methods run as the unprivileged nobody account. Also, in many scenarios the method runs as the login ID of the Tivoli administrator who issued the command. A method will run as the root user only when it is required. This increases security because the method has very little authority in the operating system. However, this increased security requires that all users have read and execute access to the Tivoli install tree. Tivoli does not make use of setuid or setgid binaries (this can be verified using the following examples: `$BINDIR -perm 4000 -o -perm 2000 -o -perm 6000`). Because Tivoli does not use setuid or setgid binaries, there is no security hole by allowing users to execute Tivoli binaries; the binaries are not be able to do anything that they cannot already do on the system.
- Applications not linked to Version 3.7.*x* libraries or higher cannot take advantage of port consolidation or SSL over their BDT channels. For example, an application built on Tivoli Management Framework, Version 3.6.*x* does not have access to the new features of SSL encryption and port consolidation for BDT channels. These applications perform IOM and other BDT operations in the pre-3.7.1 manner; that is, according to the port range and without SSL.

  Note: A managed node or application that is not SSL-capable cannot encrypt BDT or oserv communications using SSL.

  Implications include the following:

  – Use caution when specifying the **FORCE_SSL** option on SSL-capable nodes in a Tivoli environment where incapable managed nodes or applications exist. Version 3.6.*x* applications, pre-3.7.1 managed nodes, and certain interps are not capable of communicating with SSL. For example, you cannot consolidate BDT operations between Tivoli Desktop for Windows and a Tivoli server set to **FORCE_SSL**. The same is true for any Version 3.6.*x*-linked applications; that is, **FORCE_SSL** options within the Tivoli environment can cause the applications to fail to operate.

– In a Tivoli environment where 3.6.*x* applications are in use, it might not be possible to tighten firewall restrictions to the full extent intended by the design of single-port BDT. Configuring your firewalls to be restricted according to single-port BDT design can cause 3.6.*x* applications to fail if and when they attempt to make BDT connections. Keep in mind that pre-3.7.1 managed nodes also are not capable of using single-port BDT.

Recommendation: You should not modify firewall configurations to take advantage of port consolidation if you are using either of the following within the firewall environment:

– Tivoli Enterprise products that were not designed to take advantage of Tivoli Management Framework, Version 4.1 features

– Pre-3.7.1 managed nodes

In either case, the existing firewall configurations for pre-3.7.1 communications should remain unchanged. If this is a new Tivoli implementation, you can set up the firewall configuration to use the pre-3.7.1 based port range settings.

- The BDT service runs in its own process, named **bdt_service**.

  Because two processes cannot use the same port, there is a built-in failover when a BDT port is in use. Instead of the gateway failing, the gateway process attempts to open the specified BDT port (for example, port 13000), waiting 10 seconds between each attempt (up to a maximum of 3 times). If the port is still in use, the bdt_service process increases the value of the port by 1 (for example, 13000 to 13001) and attempts to use that port. If the port+1 value also is in use, the bdt_service fails to start.

Windows 2000 and Windows Server 2003 and 2008

Product notes regarding Windows 2000, Windows Server 2003, and Windows Server 2008 operating systems include the following:

- To maintain the same directory permissions that are allowed in Windows NT, the tmersrvd account (the Tivoli unprivileged operations account) is granted read and execute permission for files in the `%SystemRoot%\System32` directory during installation on a Windows 2000 system. You do not have to perform this action when installing Tivoli Management Framework.
- When a Windows 2000 server is configured to be a domain controller, the **Power Users** group does not exist. The installation neither fails nor adds the tmersrvd account to an alternate group.

  If you want to manage the Tivoli server and managed nodes on Windows 2000 domain controllers, manage them as endpoints. If you install applications with high resource requirements on Windows 2000 domain controllers, you must either give the tmersrvd account explicit read and execute permissions to certain directories or add the tmersrvd account to the **Server Operators** or **Account Operators** groups for equivalent Windows NT permissions.

Chapter 8. Interpreter type mappings

The following table lists the operating systems supported by Tivoli Management Framework. For each operating system, the table lists the resources you can create on that operating system and the interpreter type (interp) associated with that operating system and resource combination. The resource types are Tivoli server, managed node, gateway, and endpoint.

Operating system	Interpreter type	Resource type
Generic	**generic**	All
AIX	**aix4-r1**	Tivoli server Managed node Gateway Endpoint
OS/400	**os400**	Endpoint
NetWare	**nwr-ix86**	Gateway Endpoint
OS/2	**os2-ix86**	Gateway Endpoint
OS/390	**os390**	Endpoint
HP-UX	**hpux10**	Tivoli server Managed node Gateway Endpoint
Linux on Intel	**linux-ix86**	Tivoli server Managed node Gateway Endpoint
Linux on zSeries	**linux-s390**	Tivoli server Managed node Gateway Endpoint
Linux on pSeries	**linux-ppc**	Tivoli server Managed node Gateway Endpoint
Solaris on Sparc	**solaris2**	Tivoli server Managed node Gateway Endpoint
Solaris on Intel	**solaris2-ix86**	Tivoli server Managed node Gateway Endpoint
Windows XP	**w32-ix86**	Endpoint
Windows 2000 Windows Server 2003	**w32-ix86**	Tivoli server Managed node Gateway Endpoint

If your Tivoli region contains tier 2 operating systems, you might encounter the interpreter types listed in the following table. This is not a comprehensive list of tier 2 operating systems. To determine whether an unlisted operating system is supported, contact your IBM support provider.

Note: Tier 2 support is being deprecated and will be disabled at the next release of Tivoli Management Framework.

Interpreter type	Operating system and hardware
mips-irix5	SGI Mips IRIX 5
osf-axp	Tru64 UNIX(Compaq Alpha / OSF1)
reliant-unix	Pyramid/SNI Reliant UNIX
sequent	Sequent/Dynix/ptx
uw2-ix86	i486 / UnixWare

Chapter 9. Software limitations, problems and workarounds

This chapter contains the software limitations, problems, and workarounds for Tivoli Management Framework, Version 4.3.1 in English locales. For information about limitations and problems for Tivoli Management Framework, Version 4.3.1 in non-English locales, see Chapter 10, “Internationalization notes,” on page 47.

Limitations

This section contains the known software limitations for Tivoli Management Framework, Version 4.3.1.

- **Adaptive Bandwidth Control**

  Adaptive Bandwidth Control is only supported on Windows and Linux Gateways. All endpoint types are supported. Adaptive Bandwidth may increase the CPU load on the Gateway. A dual-core processor or better should be used when enabling adaptive bandwidth control.

  Adaptive is designed to sense the network and give priority to other network traffic. There are scenarios where the algorithm may not have enough information to accurately determine network load. In this case, it will always error on the side of caution ... slowing down rather than sending too quickly. If adaptive is sending too slowly, it can be ″reset″ by pausing and then resuming the distribution.

  Adaptive will not work if the gateway sender is also the source of an IPSec encrypted tunnel. IPSec will encrypt the information that adaptive requires to determine network load.

  ```
  wmdist -s adaptive_log_level=3
  ```

  or 4 is for detailed tracing, and will generally create too many log messages for a production environment.

- Defect 179228: The oserv may fail to start on Solaris 10 unless inetconv is used to convert inetd.conf entries into SMF service manifests:

  ```
  inetconv -i /etc/inetd.conf
  ```

  .

- Defect 136410: The installation of a Tivoli server or managed node on a UNIX system creates a special account under which Tivoli operations run. These account differ by operating system. Ensure that the `/etc/passwd` file on the system has one of the following accounts defined:

  For AIX

  ```
  nobody:*:4294967294:4294967294::/:
  ```

  For HP-UX

  ```
  tmersrvd:*:59999:59999:Reserved forTME:/:/bin/false
  ```

  For Solaris

  ```
  nobody:*:60001:60001::/:
  ```

  When this account does not exist, Tivoli Management Framework randomly selects an account ID under which it runs required operations. As a rule, Tivoli Management Framework selects an account ID high enough so that conflicts do not occur. To ensure that these conflicts do not arise, add the appropriate line to the `/etc/passwd` file.

- For shell scripts to run on Windows endpoints, you must place a dependency on **sh.exe** on the **run_task** method of the TaskEndpoint object. The dependency causes **sh.exe** to be downloaded when a task is run on a Windows endpoint, if it is not already there. Follow these steps to define the dependency:
  1. Get the object ID (OID) of the current dependency set (if any) associated with the **run_task** method:
     ```
     wchdep -g Classes:TaskEndpoint run_task
     ```
  2. Create the dependency:
     ```
     wdepset -c task-library-tool-base \
     -a w32-ix86 bin/w32-ix86/tools/sh.exe +a +p %TOOLS% \
     -a w32-ix86 bin/w32-ix86/tools/win32gnu.dll +a +p \
     %TOOLS%
     ```
  3. If there is *not* an existing dependency set, associate the dependency with the **run_task** method on the TaskEndpoint object:
     ```
     wchdep @Classes:TaskEndpoint \
     @DependencyMgr:task-library-tool-base run_task
     ```

     If there is an existing dependency set, add a nested dependency set to the existing dependency set:
     ```
     wdepset -e current_depset_OID \
     -a depset @DependencyMgr:task-library-tool-base
     ```
  4. Synchronize the gateway's method cache with the Tivoli server database:
     ```
     wgateway gateway dbcheck
     ```
     where *gateway* is the name of your gateway.

  Complete these steps for each gateway.

Known defects and workarounds

This section lists current defects for Tivoli Management Framework, Version 4.3.1. A workaround, if known, is also described.

Endpoint and gateways

- Defect 225205: The mdist2_db2_sql script may fail on DB2 9.x version. There are changes between DB2 8.x and DB2 9.x that cause an additional error message to be displayed when creating the mdist2 database.

  SQL5153N The update cannot be completed because the following relationship would be violated:
  ```
  softmax <= 100 * logprimary
  ```

  .

  The error is generated when this statement in mdist_db2_admin.sql is executed:
  ```
  UPDATE DATABASE CONFIGURATION FOR mdist2 USING LOGPRIMARY 2;
  ```
  DB2 9.x differs from DB 8.x in that autoconfig is turned on. If autoconfig is turned on then databases created have dynamically generated values for configuration parameters such as SOFTMAX. The dynamically generated value is often 520 whereas the default value is 100.

  The "softmax <= 100 * logprimary" error message can be ignored in which dynamically configuration values are used including for LOGPRIMARY since the attempt to set it failed. Alternatively the error message can be prevented by turning off autoconfig prior to creating the mdist2 database:
  ```
  db2set DB2_ENABLE_AUTOCONFIG_DEFAULT=NO
  ```
  Variables such as the above may be viewed:

```
db2set -all
```

Once the the mdist2 database is created and connected to with the above set it's SOFTMAX value may be viewed:

```
db2 get db cfg | grep SOFTMAX
```

Percent log file reclaimed before soft chckpt (SOFTMAX) = 100

The above value should works correctly with mdist_db2_admin.sql

- APAR IY34015: The Sybase RIM agent does not work with Sybase open client version 12.5 on AIX. Sybase 12.5 does not automatically include links between the Sybase 12.5 libraries and the Sybase 12.0 names.

  Workaround: To manually link the Sybase 12.5 and Sybase 12.0 libraries, perform the following steps:

  1. Source the Sybase environment.
  2. Navigate to the $SYBASE/OCS-12_5/lib directory.
  3. Use the following commands to link the CT and CS libraries:

     ```
     ln -s libct.so libct.so.a
     ln -s libcs.so libcs.so.a
     ```

  4. Test the RIM object again.
- Defect 166989: Viewing lcfep statistics while uninstalling an endpoint can cause visual corruption in the window tabs.

  Workaround: Click OK to close the lcfep statistics window, then reopen the window by clicking the task tray icon.
- Defect 128718: The `$LCF_DATDIR/updata` directory is created when **allow_proxy_upcalls** is set to **TRUE**.

  Workaround: To prevent the `$LCF_DATDIR/updata` directory from being created each time the endpoint starts, set **filefree_upcalls=TRUE** before setting **allow_proxy_upcalls=TRUE**.
- Defect 130738: When migrating an endpoint from a gateway with encryption level **NONE** to a gateway with encryption level **DES**, you will receive errors when attempting a downcall.

  Workaround: After migrating the endpoint, run the **wep set gateway –g** *gw_label* command. You do not need to run this command when the migration is between gateways with the same encryption level.
- Defect 149821: Endpoints not at the 431xx, or 41xxx level cannot log in to a multicast-enabled gateway.

  Workaround: Upgrade the endpoint to at least the 43100 level.

Endpoint installation

- Defect 128142: Remote endpoint installation on Windows XP Professional systems, which are not members of a domain, cannot be rebooted remotely when no one is logged on to the system.

  Workaround: Do one of the following:

  – Add the system to a domain before starting the installation.
  – Log on to the system before starting the installation.
  – Do not reboot the system during the remote installation. Manually reboot it manually after the installation completes.
- Defect 148569: On UNIX operating systems, when you do not have authorization to the $DBDIR directory and run the **winstlcf** command, the following error is displayed:

  ```
  Size of the encrypted password is zero.
  ```

Workaround: Run the **winstlcf** command as a user with full access to $DBDIR.

Multiplexed Distribution

- Defect 142049: Windows 2000 operating systems have a Media Sense feature that is enabled. If you disconnect the network cable for a multicast-enabled gateway, you need to restart that gateway after reconnecting the cable.
- Defect 148964: From a hub Tivoli region the **wmcast –p** command shows only successful operations.

Object dispatcher

- Defect 125485: The port range for an object dispatcher is not dynamically updated when it is set or modified using the **odadmin set_port_range** command.

  Workaround: After setting or modifying the port range, recycle the object dispatcher using the **odadmin reexec** command.
- Defect 137445: The **odadmin reexec all** command does not work.

  Workaround: Instead of running this command, use one of the following options:
  - For all systems, perform the following steps:
    1. From the Tivoli server, run the following command to shut down all managed nodes and gateways:

       ```
       odadmin shutdown clients
       ```
    2. When all client oservs have terminated, run the following command to restart the Tivoli server:

       ```
       odadmin reexec 1
       ```
    3. After the oserv on the Tivoli server has fully restarted, run the following command to restart the managed nodes and gateways:

       ```
       odadmin start clients
       ```

Product installation

- Defect 147350: When running the **wuninst** command to determine the list of options to uninstall Tivoli Java Client Framework using the following command **wuninst JCF**, the product is uninstalled from the entire Tivoli region instead of showing the list of options.

Chapter 10. Internationalization notes

There are no new language components in Tivoli Management Framework, 4.3.1. The language packs are supported at the Tivoli Management Framework, 4.1.1 level. The new messages that were added after the release of Tivoli Management Framework, 4.1.1, and for the Tivoli Management Framework, 4.3.1, are not translated.

Tivoli Management Framework at the 4.1.1 level is translated in the following languages:

- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Italian
- Japanese
- Korean
- Spanish

In this release, non-English characters are not supported for host names and host labels. For some locales, using non-English characters, including DBCS characters, can cause problems when specifying:

- User and group names
- Passwords
- File, directory, and object names

If you have a problem in one of these areas, avoid using non-English characters. In general, the following limitations apply to object names (labels) for Tivoli resources:

- The label can include any alphanumeric characters
- The label can include underscores (_), hyphens (-), a period (.), and spaces.

Installation and upgrade notes

Enabling language support

To enable these languages, you must install their language support components. Each Tivoli Enterprise product has its own language support CD. To fully enable additional languages, you must install the Tivoli Management Framework language support component as well as the language support component for each Tivoli Enterprise product in your Tivoli environment.

Note: If your Tivoli environment contains Tivoli Enterprise applications that use both Java Client Framework, Version 4.1.1, and Java Client Framework, Version 3.7.*x*, you must install the language packs for both versions. If only the language pack for Version 3.7.*x* is installed, the text for the **OK** and **Cancel** buttons are not found and error messages are used for the button text.

Installing language support now follows the procedure for installing any Tivoli Enterprise product. Refer to the *Tivoli Enterprise Installation Guide* for instructions for installing products and for information about setting up a non-English system environment.

Because no translatable resources were changed in the Tivoli desktop for Windows, Version 4.1.1, there are no new language components. To enable language support, you must use version 4.1 of the language support components, which are included on the Tivoli Management Framework, Version 4.1.1 Language Support CD.

Because no translatable resources were changed in the WEBAPP, Version 4.1.1, there are no new language components. To enable language support, you must use version 4.1 of the language support components, which are included on the Tivoli Management Framework, Version 4.1.1 Language Support CD.

System requirements for Asian environments

This section provides information about system requirements for using Tivoli Management Framework in Asian environments. These notes supplement the general system requirements in "System requirements" on page 16.

Java requirements

On AIX 5.1 operating systems in a non-UTF8 CKJ locale, either install Fixpack10 or individually install the following listed filesets:

- X11.fnt.fontserver 4.3.3.12
- X11.fnt.ucs.ttf (for ja_JP or Ja_JP)
- X11.fnt.ucs.ttf_CN 4.3.3.1 (for zh_CN or Zh_CN)
- X11.fnt.ucs.ttf_KR (for ko_KR)
- X11.motif.lib 5.1.0.15 (for ja_JP or Ja_JP AIX 5.1 users)
- X11.fnt.ucs.ttf_TW (for zh_TW or Zh_TW)
- jkit.Wnn6.base 2.1.1.5 (for ja_JP or Ja_JP Wnn6 users)
- bos.loc.com.JP 4.3.3.11 (for ja_JP or Ja_JP)
- bos.loc.utf.ZH_TW 4.3.3.11 (for zh_TW or Zh_TW)
- devices.rsa_sio.baud.rte 4.3.2.1

These fixes are required by IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.3.0. If these filesets are not installed, they can be found on the AIX 4.3.3 installation media, or you can use the FixDist tool available from the following Web site:

`http://techsupport.services.ibm.com/rs6000/support`

Endpoint notes

- Japanese OS/2 4.0 requires FixPaks WX02204 and FX00001.
- Korean OS/2 4.0 requires patch `kjr11660.zip`, which can be downloaded from **ftp:/service.boulder.ibm.com/**.

  Note: After connecting to this site, navigate to **ps/products/os2/fixes/v4warp/korean**. Review the README file in this directory.
- Traditional Chinese OS/2 4.0 requires FixPak 30.

NEC PC98 systems

The following sections list system requirements and supported operating systems for NEC PC98. The NEC PC98 system hardware is usually sold only in Japan.

Endpoints on NEC PC98*xx*: The Tivoli endpoint is supported on PC98*xx* systems running the following operating systems:

- Microsoft Windows 98J
- Microsoft Windows 4.0J with Service Pack 4

The following table shows the NEC PC9800 models supported for Tivoli Management Framework, Version 4.3.1.

PC9800 Series Family Name	Model Name
Aile	PC9821LA13S14R
La Vie	PC9821NR150/S20
MATE	PC9821XA200W30R
	PC9821RA266M30R
MATE X	PC9821Xc16
	PC9821Xa20
VALUESTAR	PC9821V200/S5 model D3

Endpoints on NEC PC98NX: The Tivoli endpoint is supported on PC98NX systems running the following operating systems:

- Microsoft Windows 98J
- Microsoft Windows 4.0J with Service Pack 4

The following table shows the NEC PC98NX models supported for Tivoli Management Framework, Version 4.3.1.

NX Series Family Name	Model Name
Aile NX	AL20C/TS model AAF1
La Vie NX	LW20/32A
MATE NX	IMA35D/S5 model BAC42
	IMA26D/C5 model ATC42
VALUESTAR	VC33/47C
	VS30/35D
VersaPro NX	VA23C/WX model BAB33

Cantonese Chinese

This version of Tivoli Management Framework does not handle the 3,000 unique Cantonese characters because these characters are not part of Unicode.

Microsoft Windows NT Workstation Pan Chinese 4.00.1381 is supported.

Software limitations, problems, and workarounds

- Defect 167825: Some double-byte character set (DBCS) characters do not display correctly on HP-UX systems.

  Workaround: Do not run the X Font Server with Asian TrueType fonts in versions of the HP-UX Runtime Environment for the Java platform prior to version 1.4. Perform the following steps:

  – Download the HP-UX Runtime Environment for the Java platform, version 1.4.1.02 or later.

– Perform the following command:

```
cd $BINDIR
```

– Perform the following command:

```
cp -r JRE JRE_Tivoli
```

– Perform the following command:

```
cd JRE
```

– Perform the following command:

```
rm -rf 1.3.0
```

– Perform the following command:

```
ln -s /opt/java1.4/jre 1.3.0
```

- The JRE 1.3.1_03, which is included with Tivoli Management Framework, Version 4.1.1, does not support the GB18030 code set in a Solaris Operating Environment.

  Workaround: You can manually upgrade to JRE 1.3.1_09 and apply a font patch, which can be found at the following Web sites:

  http://java.sun.com/j2se/1.3/ReleaseNotes.html

  http://jp.sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fpatches%2F114246&zone_32=GB18030

  Note: This code has not been tested and is not supported by IBM.
- APAR IY49303: To use Linux endpoints in non-English environments, you must set the LANG environment variable in both the **lcfd.sh** and **Tivoli_lcf***n* files, where *n* is the endpoint number.
- Defect 166286: Simplified Chinese fonts do not display correctly in Java GUIs on Solaris machines.
- Defect 136326: On UNIX systems, certain Java GUI panels may not display correctly when using DBCS languages.

  Workaround: Set the screen resolution higher or use the CLI command.
- Some text in the Tivoli desktop is not translated.
- In some cases, English text, resource names, resource types, and roles are not fully translated.
- Usage statements for some commands are not fully translated.
- Manual pages on all UNIX operating systems are not translated.
- For Tivoli Desktop for Windows to work in any Spanish locale, the Regional Setting Properties must be set to Spanish (Traditional). When set to any other Spanish setting in the Regional Setting Properties dialog, the login dialog is displayed in English.
- Defect 97676: The UserLink HTML page is in English.
- Defect 115491: The gateway and status Web pages are not enabled.
- Defect 114995: The **odadmin info all** command returns a date that is not localized.
- Defect 115291: For some locales, the string not found window is truncated on the top.
- Defect 136125: For AIX5L operating systems in the Chinese EUC locale, the Tivoli desktop panels display text incorrectly.

  Workaround: Install the patch `bos.rte 5.1.0.25`.
- Defect 146385: Although the panels displayed during the installation of the Tivoli server on Windows operating systems is locale-specific, the information displayed in command windows is in English.

- Defect 147967, 166555: In a Linux with DBCS system, the Tivoli Desktop for X Windows may have problems displaying the DBCS characters on the dialogs.

  Workaround: This problem is due to inappropriate fonts on the X Windows system used to display the Tivoli desktop. To get the list of available fonts, use the **xlsfonts** command. From this list, you can get an available font to display your language.

  To specify a different font when starting the Tivoli desktop, enter the following command:

  ```
  tivoli -fn font
  ```

  Alternatively, you can override the resource files by entering the following command:

  ```
  tivoli -xrm "*fontList: font:font"
  ```

  For example, for the Tivoli Desktop running in a Japanese locale, you can enter the following command:

  ```
  tivoli -xrm "*fontList: a14:k14:r14:"
  ```

  If you do not want to pass parameters, you can create a command alias or a resource file by performing the following steps:

  1. Set the Tivoli environment variables:

     ```
     . /etc/Tivoli/setup_env.sh
     ```

  2. Get the value for the XUSERFILESEARCHPATH variable:

     ```
     echo $XUSERFILESEARCHPATH
     ```

     This value shows a directory like `/usr/lib/X11/app-defaults/%L/%N`.

  3. Replace `%L` with `$LANG`, and replace `%N` with `Tivoli`.
  4. Add an entry with the font pattern you want to use to the `/usr/lib/X11/app-defaults/$LANG/Tivoli` file in the format:

     ```
     "*fontList: font:font"
     ```

  To use with more than one language, add your entry to the `/usr/X11R6/lib/X11/app-defaults/Tivoli` file.

Part Number: CT2JRIE

Printed in USA

(1P) P/N: CT2JRIE

GI11-0890-02