IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines 7.2 Fix Pack 8

Installation and Configuration Guide

SC14-7490-01

Note

Before using this information and the product it supports, read the information in “Notices” on page 21.

This edition applies to version 7.2.0.8 of IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines (product number 5724-L92) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview of the agent

The IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines (product code V1) provides you with the capability to monitor Linux Kernel-based Virtual Machines.

IBM® Tivoli® Monitoring is the base software for the Linux Kernel-based Virtual Machines agent.

IBM Tivoli Monitoring

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

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

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

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

See the IBM Tivoli Monitoring publications listed in "Prerequisite publications" in the Documentation library topic for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

Functions of the monitoring agent

Display health and performance of Linux KVM host hypervisor/RHEVM systems and guest virtual machines

You can use the Linux Kernel-based Virtual Machines agent to visualize host capacity, cluster, data center, storage pool and virtual machine consumption in Linux KVM systems.

New in this release

Edit online

For version 7.2.0.8 of the Linux Kernel-based Virtual Machines agent, the following enhancements were made since version 7.2, including the fix packs.

- Added support for ITM 6.3.0 FP 07 Service Pack 12
- Upgraded JRE version to 1.8.0_321

Components of the IBM Tivoli Monitoring environment

Edit online

After you install and set up the Linux Kernel-based Virtual Machines agent, you have an environment that contains the client, server, and monitoring agent implementation for Tivoli Monitoring.

This Tivoli Monitoring environment contains the following components:

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

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

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

Tivoli Enterprise Monitoring Agent, Linux Kernel-based Virtual Machines agent
This monitoring agent collects data and distributes the data to the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, Tivoli Enterprise Portal, Tivoli Data Warehouse, and Tivoli Integrated Portal.

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

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

IBM Tivoli Enterprise Console®
The Tivoli Enterprise Console is an optional component that acts as a central collection point for events from various sources, including events from other Tivoli software applications, Tivoli partner applications, custom applications, network management platforms, and relational database systems. You can view these events through the Tivoli Enterprise Portal (by using the event viewer), and you can forward events from Tivoli Monitoring situations to the Tivoli Enterprise Console component. If you do not already use Tivoli Enterprise Console and need an event management component, you can choose to use IBM Tivoli Netcool/OMNIbus.

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

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

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

IBM Dashboard Application Services Hub
The Dashboard Application Services Hub has a core set of components that provide such administrative essentials as network security and database management. This component replaces the Tivoli Integrated Portal component after version 2.2.

Tivoli Integrated Portal
Tivoli Integrated Portal helps the interaction and secure passing of data between Tivoli products through a common portal. Within the same dashboard view, you can launch from one application

to another and research different aspects of your managed enterprise. This component is installed automatically with the first Tivoli product that uses the Tivoli Integrated Portal framework. Subsequent products can install updated versions of Tivoli Integrated Portal. After version 2.2, this component is replaced by the Dashboard Application Services Hub.

Agent Management Services

Edit online

You can use IBM Tivoli Monitoring Agent Management Services to manage the Linux Kernel-based Virtual Machines agent.

Agent Management Services is available for the following IBM Tivoli Monitoring OS agents: Windows, Linux®, and UNIX. The services are designed to keep the Linux Kernel-based Virtual Machines agent available, and to provide information about the status of the product to the Tivoli Enterprise Portal. IBM Tivoli Monitoring V6.2.2, Fix Pack 2 or later provides support for Agent Management Services. For more information about Agent Management Services, see "Agent Management Services" in the *IBM Tivoli Monitoring Administrator's Guide*.

User interface options

Edit online

Installation of the base IBM Tivoli Monitoring software and other integrated applications provides various interfaces that you can use to work with your resources and data.

The following interfaces are available:

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

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

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

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

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

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

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

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

IBM Dashboard Application Services Hub
The Dashboard Application Services Hub provides an administrative console for applications that use this framework. It is a web-based console that provides common task navigation for products, aggregation of data from multiple products into a single view, and the passing of messages between views from different products. This interface replaces the Tivoli Integrated Portal component after version 2.2.

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

Data sources

The Linux Kernel-based Virtual Machines agent collects data from the following sources:

Ovirt Java SDK
The agent uses application-specific API calls to gather metrics.

SNMP
SNMP (Simple Network Management Protocol) is the network management protocol used almost exclusively in TCP/IP networks. By using SNMP, you can monitor and control network devices, and manage configurations, statistics collection, performance, and security. This agent supports SNMP V1, V2c, and V3.

SNMP Events
SNMP is the network management protocol used almost exclusively in TCP/IP networks. SNMP resources send asynchronous notifications in the form of traps or informs to a manager. This agent receives traps or informs and makes them available in IBM Tivoli Monitoring. This agent supports SNMP V1, V2c, and V3.

WMI
By using WMI (Windows Management Instrumentation), you can monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, and groups. WMI is built into clients with Windows 2000 or later, and can be installed on any 32-bit Windows client.

Perfmon
Use the Windows Performance Monitor, or Perfmon, to view various system and application performance metrics for collection and use by management applications. You typically view system metrics on a Windows system through the 'perfmon' application.

JMX
Use the Java Management Extensions (JMX) interface to gather various metrics from Java applications supporting the monitored resource.

JDBC
Use the Java Database Connectivity (JDBC) interface to gather information from database tables supporting the monitored resource.

Availability
Use the agent to monitor availability of the application and related components in the following ways:

Scripts
The agent uses application-specific commands and interfaces to gather metrics.

SSH Scripts
The agent uses application-specific commands and interfaces to gather metrics remotely by using an SSH connection to the monitored resource.

Log files
The agent uses the file system to monitor application log files or other data files to gather metrics.

Windows Event Log
The agent collects Windows Event Log entries related to the monitored resource and forwards them to IBM Tivoli Monitoring.

HTTP
Use Hypertext Transfer Protocol (HTTP) to monitor the availability and basic content of URLs supporting the monitored application.

ICMP Ping
Use ICMP packets commonly known as "ping" to monitor systems that support the monitored resource.

CIM
Use Common Information Model (CIM) messages over HTTP to gather data related to the monitored resource.

Chapter 2. Installing and configuring the agent

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

To install and configure the Linux Kernel-based Virtual Machines agent, use the *Installing monitoring agents* procedures in the *IBM Tivoli Monitoring Installation and Setup Guide* along with the agent-specific installation and configuration information.

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

Requirements

Edit online

Before installing and configuring the agent, make sure your environment meets the requirements for the IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines.

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

Installing language packs

Edit online

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

To install a language pack for the agent support files on the Tivoli Enterprise Monitoring Server, the Tivoli Enterprise Monitoring Agent, and the Tivoli Enterprise Portal Server, make sure that you installed the product in the English language. Then, use the steps for installing on Windows systems, installing on UNIX or Linux systems, or installing silently.

Installing language packs on Windows systems

Edit online

You can install the language packs on a Windows system.

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

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

10. Restart the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Eclipse Help Server if any of these components are installed.

Installing language packs on UNIX or Linux systems

Edit online

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

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

1. Enter the `mkdir` command to create a temporary directory on the computer, for example, `mkdir dir_name`. Make sure that the full path of the directory does not contain any spaces.
2. Mount the language pack CD to the temporary directory that you created.
3. Enter the following command to start the installation program:

   ```
   cd dir_name lpinstaller.sh -c install_dir
   ```

   Where: *install_dir* is where you installed IBM Tivoli Monitoring. Typically, the directory name is `/opt/IBM/ITM` for UNIX and Linux systems.
4. Select the language of the installer and click **OK**.
5. In the Introduction panel, click **Next**.
6. Click **Add/Update** and click **Next**.
7. Select the folder where the National Language Support package (`NLSPackage`) files are located. Typically, the `NLSPackage` files are located in the `nlspackage` folder where the installer executable file is located.
8. Select the language support for the agent of your choice and click **Next**. To make multiple selections, press Ctrl and select the language that you want.
9. Select the languages that you want to install and click **Next**.
10. Examine the installation summary page and click **Next** to begin installation.
11. After installation completes, click **Finish** to exit the installer.
12. Restart the Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Eclipse Help Server if any of these components are installed.

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

Edit online

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

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

1. Copy and paste the `ITM_Agent_LP_silent.rsp` response file template as shown in "Response file example" on page 9.
2. Change the following parameter settings:

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

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

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

LANG_SELECTION_LIST
Language you want to install.

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

     ```
     lpinstaller.bat -f path_to_response_file
     ```

   - For UNIX or Linux systems:

     ```
     lpinstaller.sh -c candle_home -f path_to_response_file
     ```

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

Response file example

```
#     IBM Tivoli Monitoring Agent Language Pack Silent Installation Operation
#
#This is a sample response file for silent installation mode for the IBM Tivoli
#Monitoring Common Language Pack Installer.
#.
#This file uses the IBM Tivoli Monitoring Common Agent Language Pack with the
#install package as an example.
#Note:
#This response file is for the INSTALLATION of language packs only.
#This file does not support UNINSTALLATION of language packs in silent mode.
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#To successfully complete a silent installation of the the example of Common Agent
#localization pack, complete the following steps:
#
#1.Copy ITM_Agent_LP_silent.rsp to the directory where lpinstaller.bat or
#lpinstaller.sh is located (IBM Tivoli Monitoring Agent Language Pack build
#location).
#
#2.Modify the response file so that it is customized correctly and completely for
#your site.
#  Complete all of the following steps in the response file.
#
#3.After customizing the response file, invoke the silent installation using the
#following command:
#For Windows:
#    lpinstaller.bat -f <path_to_response_file>
#For UNIX and Linux:
#    lpinstaller.sh -c <candle_home> -f <path_to_response_file>
#Note:<candle_home> is the IBM Tivoli Monitoring base directory.
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#Force silent install mode.
#-----------------------------------------------------------------------------
INSTALLER_UI=silent
#-----------------------------------------------------------------------------
#Run add and update actions.
#-----------------------------------------------------------------------------
CHOSEN_INSTALL_SET=ADDUPD_SET
#-----------------------------------------------------------------------------
#NLS Package Folder, where the NLS Packages exist.
#For Windows:
#   Use the backslash-backslash(\\) as a file separator (for example,
#C:\\zosgmv\\LCD7-3583-01\\nlspackage).
#For UNIX and Linux:
#   Use the slash-slash (//) as a file separator (for example,
#//installtivoli//lpsilenttest//nlspackage).
#-----------------------------------------------------------------------------
#NLS_PACKAGE_FOLDER=C:\\zosgmv\\LCD7-3583-01\\nlspackage
NLS_PACKAGE_FOLDER=//tmp//LP//nlspackage
#-----------------------------------------------------------------------------
#List the packages to process; both variables are required.
#Each variable requires that full paths are specified.
#Separate multiple entries with a semicolon (;).
#For Windows:
#           Use the backslash-backslash(\\) as a file separator.
```

```
#For Unix and Linux:
#           Use the slash-slash (//) as a file separator.
#-------------------------------------------------------------------------------
#PROD_SELECTION_PKG=C:\\zosgmv\\LCD7-3583-01\\nlspackage\\KIP_NLS.nlspkg
#BASE_AGENT_FOUND_PKG_LIST=C:\\zosgmv\\LCD7-3583-01\\nlspackage\\KIP_NLS.nlspkg
PROD_SELECTION_PKG=//tmp//LP//nlspackage//kex_nls.nlspkg;//tmp//LP//nlspackage//
koq_nls.nlspkg
BASE_AGENT_FOUND_PKG_LIST=//tmp//LP//nlspackage//kex_nls.nlspkg;//
tmp//LP//nlspackage//koq_nls.nlspkg
#-------------------------------------------------------------------------------
#List the languages to process.
#Separate multiple entries with semicolons.
#-------------------------------------------------------------------------------
LANG_SELECTION_LIST=pt_BR;fr;de;it;ja;ko;zh_CN;es;zh_TW
```

Installing and configuring: agent-specific

Edit online

In addition to the installation and configuration information in the *IBM Tivoli Monitoring Installation and Setup Guide*, use this agent-specific installation and configuration information to install the Linux Kernel-based Virtual Machines agent.

Virtualization hosts

Edit online

The Linux Kernel-based Virtual Machines agent supports connection to both the Enterprise Linux based KVM hypervisor and Red Hat Enterprise Virtualization Manager (RHEVM) environments.

The configuration attributes define which data sources are monitored.

- To monitor an Enterprise Linux based KVM hypervisor, add a data source under Hypervisor section of agent configuration .
- To connect to RHEVM environment, add a data source under RHEVM Connection Details section.

Consider how the hosts are organized by identifying whether you have multiple kinds of virtualized loads and whether you want to migrate virtual machines between hosts. Also, consider how you want to secure communications between the Linux Kernel-based Virtual Machines agent and the RHEV-M or the hypervisors. Follow the instructions before you begin the configuration.

- For RHEVM configuration:
  1. Download the security certificate that is available at the following path: `http://[RHEVM-IP]/ovirt-engine/services/pki-resource?resource=cacertificate&format=X509-PEM-CA` .
     Depending on the browser, the certificate is either downloaded or imported into the browser's Keystore.
     - If the browser downloads the certificate: Save the file as `rhvm.cer`.
     - If the browser imports the certificate: Export it from the browser's certification options and save it as `rhvm.cer`.
  2. Use the **keytool** utility to import the security certificate file to generate a local keystore file:

     ```
     keytool -import -alias ALIAS -file CERTIFICATE_FILE -keystore KEYSTORE_FILE
     ```

     Example:

     ```
     keytool -import -alias RHEVM36vmwt9 -file hjs495-vmw-t-9.cer -keystore RHEVM36KeyStore
     ```

     where

ALIAS
A unique reference for each certificate that is added to the certificate truststore of the agent, for example, an appropriate alias for the certificate from *datasource.example.com* is *datasource*.

CERTIFICATE_FILE
The complete path and file name to the data source certificate that is being added to the truststore.

KEYSTORE_FILE
The name of the keystore file that you want to specify.

Tip: The **keytool** utility is available with Java Runtime Environment (JRE). The keystore file is stored at the same location from where you run the command.

3. Ensure that the user, who connects to the RHEVM, is an administrator with the SuperUser role.
4. Create a user account with read-only access to the REST API of the Red Hat Enterprise Virtualization Manager (RHEV-M) to collect information about clusters, hosts, and virtual machines that RHEV-M manages. If there is no user domain, such as an LDAP or an Active Directory, configured, then use the default "admin" user and "internal" domain in the configuration steps to connect to RHEVM, or complete the following steps:
   a. Open the **Red Hat Enterprise Virtualization Manager Web Administration** portal.
   b. Click **Configure**.
   c. In the **Configuration** window, select **Roles**.
      i) To create a role, click **New**.
      ii) In the **New Role** window, add the name of the role and select **Admin** as the account type. Then, in the **Check boxes to Allow Action** pane, leave the check boxes clear. Click **OK**.
   d. In the **Configuration** window, select **System Permission**.
      i) To grant a user permission, click **Add**.
      ii) In the **Add System Permission to User** window, select the user to whom you want to grant the permission.
      iii) From the **Assign role to user** list, select the role that you created in step 4 (c) and click **OK**.

- For Linux based KVM hypervisor configuration:

  The Linux Kernel-based Virtual Machines agent collects its metrics by connecting remotely to each `libvirt` hypervisor managing your QEMU-KVM virtual machines. The `libvirt` hypervisor can use several different remote transport protocols, as described on the Remote support page of the Libvirt Virtualization API website (http://libvirt.org/remote.html). The Linux Kernel-based Virtual Machines agent supports the SSH protocol, the TLS protocol, and the TCP protocol. While the SSH protocol and the TLS protocol provide production-level security, the use of the TCP protocol by the Linux Kernel-based Virtual Machines agent supports only an authentication of *none* and is intended for testing. Follow the instructions for implementing the SSH protocol, the TLS protocol, and the TCP protocol in the context of `libvirt` remote connections.

SSH protocol

Edit online

For the SSH agent, assume you install the Linux Kernel-based Virtual Machines agent on Host A and you want to remotely monitor the hypervisor on Host B. First, you must configure the SSH agent so the SSH agent can make a connection from Host A to Host B without requiring you to include a password.

After configuration, you can start the Linux Kernel-based Virtual Machines agent and begin to monitor Host B. Assume you have several hosts that you want to monitor, for example, several Host Bs. For some helpful instructions on this topic, see the following procedure for accessing an SSH agent without a password at the Using the ssh-agent with ssh website (http://mah.everybody.org/docs/ssh).

1. Log on to Host A with the same ID that will run the Linux Kernel-based Virtual Machines agent process, for example, the root user ID. Have available the ID on Host B that will be making the SSH connection, often also the root user ID.
2. Generate the `id_rsa` and `id_rsa.pub` keys on Host A. The keys are saved in `~/.ssh`:

```
$ ssh-keygen -t rsa
```

3. Copy the authorized keys from Host B, so you can add the public key for Host A to it:

```
$ scp Id on Host B@name or IP address of Host B:~/.ssh/authorized_keys ~/.ssh/
authorized_keys_from_B
```

4. Append the public key for Host A to the end of the authorized keys for Host B:

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys_from_B
```

5. Copy the authorized keys back to Host B. If you are monitoring multiple hosts, repeat steps 3, 4, and 5 for each host. You can remove `~/.ssh/authorized_keys_from_B` after this step:

```
$ scp ~/.ssh/authorized_keys_from_B Id on Host B@name or IP address of Host B:~/.ssh/
authorized_keys
```

6. Add the following command to the `~/.bash_profile` of the current ID on Host A: **$ eval `ssh-agent`**. Ensure you use the single back quotation mark (`), located under the tilde (~) on US keyboards, rather than the single quotation mark (').
7. Add the identity to Host A. You are asked for the passphrase you used when the ID was created. If you receive the message "`Could not open a connection to your authentication agent.`", run the **exec ssh-agent bash** command (you can replace *bash* with the shell you are using) and then run the **ssh-add** command again:

```
$ ssh-add ~/.ssh/id_rsa
```

8. Test that the SSH agent can make a connection from Host A to Host B without entering the SSH password. If you are monitoring multiple hosts, test the connection for each host:

```
$ ssh Id on Host B@name or IP address of Host B
```

When you have finished the configuration, check your work by using the **virsh** command by entering

```
virsh -c qemu+ssh://Id on Host B@name or IP address of Host B:port/system
```

You can omit the **:port** section of the command if you have not changed the default SSH port. If the **virsh** command succeeds, the Linux Kernel-based Virtual Machines agent can connect.

Note: You must rerun the **ssh-add** command and supply the passphrase each time you restart Host A before you restart the Linux Kernel-based Virtual Machines agent on Host A. If you use SSH keychains, you can avoid having to reenter the passphrase. A discussion of SSH keychains is beyond the scope of this guide, but information is available on the Internet.

TLS protocol

Edit online

TLS (Transport Layer Security) is often implemented in an organization to authenticate server-to-server communications. If you have already established TLS authentication on your servers, you can also use TLS for libvirt-to-libvirt communications.

For the TLS protocol, assume you install the Linux Kernel-based Virtual Machines agent on Host A and you want to remotely monitor the hypervisor on Host B.

1. Log in to Host B and confirm you have installed the `gnutls` and `gnutls-utils` packages.
2. Edit `/etc/libvirt/libvirtd.conf` to make sure that **listen_tls** is enabled and the **tls_port** is 16514 (the default).

3. Go to `libvirt.org/remote.html` and follow the instructions for setting up a certificate authority between Host A and Host B. Pay special attention to the sections of Setting up a Certificate Authority (CA), Issuing server certificates, and Issuing client certificates.
4. Restart the libvirt daemon on Host B in listening mode by running it with the **`--listen`** flag or by editing `/etc/sysconfig/libvirtd` and uncommenting the `LIBVIRTD_ARGS="--listen"` line.

When you have finished the configuration, check your work using the **`virsh`** command by entering `virsh -c qemu+tls://`*`name or IP address of Host B`*`:port/system`. You can omit the **`:port`** section of the command if you have not changed the default TLS port. If the **`virsh`** command succeeds, the Linux Kernel-based Virtual Machines agent can connect.

TCP protocol

Edit online

Use the TCP protocol only for testing.

For TCP, assume you install the Linux Kernel-based Virtual Machines agent on Host A and you want to remotely monitor the hypervisor on Host B. Follow these steps:

1. Log in to Host B.
2. Edit `/etc/libvirt/libvirtd.conf` to make sure that **`listen_tcp`** is enabled and **`tcp_port`**is 16509 (the default).
3. Edit `/etc/libvirt/libvirtd.conf` to set **`auth_tcp`** to "none". This step instructs TCP not to perform any authentication.
4. Restart the libvirt daemon on Host B in listening mode by running it with the **`--listen`** flag or by editing `/etc/sysconfig/libvirtd` and uncommenting the `LIBVIRTD_ARGS="--listen"` line.

When you have finished the configuration, check your work using the **`virsh`** command by entering `virsh -c qemu+tcp://`*`name or IP address of Host B`*`:port/system`. You can omit the **`:port`** section of the command if you have not changed the default TCP port. If the **`virsh`** command succeeds, the Linux Kernel-based Virtual Machines agent can connect.

Configuration values

Edit online

For both local and remote configuration, you provide the configuration values for the agent to operate.

When you are configuring an agent, a panel is displayed so you can enter each value. When a default value exists, this value is pre-entered into the field. If a field represents a password, two entry fields are displayed. You must enter the same value in each field. The values that you type are not displayed to help maintain the security of these values.

The configuration for this agent is organized into the following groups:

Data Provider (DATA_PROVIDER)
This section provides the logging characteristics that the data provider uses.

The configuration elements defined in this group are always present in the agent's configuration.

This group defines information that applies to the entire agent.

Maximum Number Of Data Provider Log Files (KV1_LOG_FILE_MAX_COUNT)
This is the number of log files that is created before rolling over.

The type is numeric.

This value is required.

Default value: 10

Maximum Size in KB of Each Data Provider Log (KV1_LOG_FILE_MAX_SIZE)
This value is the maximum size in KB that a log file reaches before moving to the next log file.

The type is numeric.

This value is required.

Default value: 5190

Level of Detail in Data Provider Log. (KV1_LOG_LEVEL)
This value controls how many log messages the agent writes and at what level of detail.

The type is one of the following values: "Off", "Severe", "Warning", "Info", "Fine", "Finer", "Finest", "All".

This value is required.

Default value: INFO

Hypervisor (HYPERVISOR)
This section provides the connection information for each hypervisor being monitored.

The configuration elements defined in this group are always present in the agent's configuration.

Use the information in this group to create additional subnodes.

Connection Instance Type (CONNECTION_MODE)
This value controls whether the local libvirt connects to the privileged system driver or the per-user unprivilege session driver.

The type is one of the following values: "system (If you are unsure, this is probably the right answer.)", "session".

This value is required.

Default value: system

Host (HOST_ADDRESS)
The host name or IP address of the KVM hypervisor.

The type is string.

This value is required.

Default value: None

Port (PORT)
The port used by the transport protocol to make the libvirt connection. It is only needed if the standard ports have been changed (22 for SSH, 16514 for TLS, 16509 for TCP).

The type is numeric.

This value is optional.

Default value: None

Remote Transport (PROTOCOL)
This value controls which protocol the local libvirt uses to connect to remote libvirts.

The type is one of the following values: "SSH", "TLS", "TCP (Unencrypted -- not recommended for production use.)".

This value is required.

Default value: ssh

User (USERNAME)
A user name on the KVM hypervisor that has sufficient privileges to collect monitoring data. It is only needed for SSH transport.

The type is string.

This value is optional.

Default value: None

Hypervisor ID (Hypervisor ID)
A unique identifier for this hypervisor.

The type is string.

This value is required.

Default value: None

RHEVM Connection Details (RHEVM)
This section provides the connection information in relation to RHEVM that is monitored.

The configuration elements defined in this group are always present in the agent's configuration.

Use the information in this group to create additional subnodes.

RHEVM ID (RHEVM ID)
A unique identifier for this rhevm.

The type is string.

This value is required.

Default value: None

Domain (RHEVM_DOMAIN)
The user domain to which the user belongs.

The type is string.

This value is optional.

Default value: None

Host (RHEVM_HOST_ADDRESS)
The host name or IP address of the rhevm connection.

The type is string.

This value is required.

Default value: None

KeyStorePath (RHEVM_KEYSTOREPATH)
The path of the local key store that has the security certificate from the RHEVM server.

The type is string.

This value is required.

Default value: None

Password (RHEVM_PASSWORD)
The password or user name that has sufficient privileges to connect to RHEVM

The type is password.

This value is required.

Default value: None

Port (RHEVM_PORT)
The port that is used by the RHEVM connection.

The type is numeric.

This value is required.

Default value: None

User (RHEVM_USERNAME)
A user name that has sufficient privileges to connect to RHEVM.

The type is string.

This value is required.

Default value: None

Remote installation and configuration

Edit online

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

When you install the agent remotely, you must provide the configuration values for the agent to operate. See “Configuration values” on page 13.

To install from the portal, see the *IBM Tivoli Monitoring Installation and Setup Guide*.

To remotely install or configure an agent through the Tivoli Enterprise Portal, application support for that agent must be installed (Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal). Also, the agent bundle must be installed in the Remote Deploy Depot.

For information about displaying the configuration options that are available to use with the **configureSystem** command, see "tacmd describeSystemType" in the *IBM Tivoli Monitoring Command Reference*.

If you are using the command line, the following commands are examples of remote installation and configuration for Windows operating systems:

Remote installation

```
tacmd addbundles -t v1 -i <Installer_package_Path/ITMfVE_Agents/unix/>

tacmd addsystem -t v1 -n Primary:sample.node.name:LZ -p Instance=inst1
```

Remote configuration

The following example illustrates configuration by using all configuration variables. Typically, you specify only the variables and values that you want to change.

Hypervisor and RHEVM Instance Configuration:

```
tacmd addSystem -t v1 -n Primary:sample.node.name:LZ
-p INSTANCE=dualinst
DATA_PROVIDER.KV1_LOG_FILE_MAX_COUNT=value
DATA_PROVIDER.KV1_LOG_FILE_MAX_SIZE=value
DATA_PROVIDER.KV1_LOG_LEVEL=value
HYPERVISOR:Source1.CONNECTION_MODE=value
HYPERVISOR:Source1.HOST_ADDRESS=value
HYPERVISOR:Source1.PORT=value
HYPERVISOR:Source1.PROTOCOL=value
HYPERVISOR:Source1.USERNAME=value
RHEVM:Source1.RHEVM_DOMAIN=value
RHEVM:Source1.RHEVM_HOST_ADDRESS=value
RHEVM:Source1.RHEVM_KEYSTOREPATH=value
RHEVM:Source1.RHEVM_PASSWORD='value'
RHEVM:Source1.RHEVM_PORT=value
RHEVM:Source1.RHEVM_USERNAME=value
```

RHEVM Instance Configuration:

```
tacmd addSystem -t v1 -n Primary:sample.node.name:LZ
-p INSTANCE=inst1
DATA_PROVIDER.KV1_LOG_FILE_MAX_COUNT=value
DATA_PROVIDER.KV1_LOG_FILE_MAX_SIZE=value
DATA_PROVIDER.KV1_LOG_LEVEL=value
RHEVM:inst1.RHEVM_DOMAIN=value
RHEVM:inst1.RHEVM_HOST_ADDRESS=value
RHEVM:inst1.RHEVM_KEYSTOREPATH=value
RHEVM:inst1.RHEVM_PASSWORD='value'
RHEVM:inst1.RHEVM_PORT=value
RHEVM:inst1.RHEVM_USERNAME=value
```

Hypervisor Instance Configuration:

```
tacmd addSystem -t v1 -n Primary:sample.node.name:LZ
-p INSTANCE=instA
DATA_PROVIDER.KV1_LOG_FILE_MAX_COUNT=value
DATA_PROVIDER.KV1_LOG_FILE_MAX_SIZE=value
DATA_PROVIDER.KV1_LOG_LEVEL=value
HYPERVISOR:instAB.CONNECTION_MODE=value
HYPERVISOR:instAB.HOST_ADDRESS=value
HYPERVISOR:instAB.PORT=22
HYPERVISOR:instAB.PROTOCOL=value
```

Configuring a connection to the RHEVM server

Edit online

To configure a connection to the RHEVM server, you must run the script and respond to prompts.

1. On the command line, run the following command:

   install_dir/bin/linux_kvm-agent.sh config instance_name

   Example **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config instance_name**

   Where

   instance_name
   The name that you want to give to the instance.

   install_dir
   The path where the agent is installed.
2. Respond to the prompts and specify values for the configuration parameters.

   For information about the configuration parameters, see “Configuration values” on page 13.
3. Run the following command to start the agent:

   install_dir/bin/linux_kvm-agent.sh start instance_name

   Example **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start instance_name**

Configuring environment variables

Edit online

Refer this topic to configure environment variables.

1. Stop all the agent instances
2. Follow the procedure given in this step for Unix platform
   a) On Unix platforms, locate the agent instance file `v1.ini` in the given paths:
   - 32-bit Agent system: `$CANDLEHOME/config`
   - 64-bit Agent system: `$CANDLEHOME/config`
3. Set the required environment variable with desired value in the agent instance file located in Step 2
   For example, *KV1_DATA_PROVIDER_CONNECTION_RETRY_COUNT=6*
4. Start the agent instances

Appendix A. Documentation library

A variety of documentation is available for IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines.

Three documents are specific to the Linux Kernel-based Virtual Machines agent. The IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines *Reference Guide*, *Installation and Configuration Guide* and *Troubleshooting Guide* provides agent-specific information for configuring, using, and troubleshooting the Linux Kernel-based Virtual Machines agent.

The Prerequisites topic in the information center contains information about the prerequisites for each component.

Prerequisite documentation

Edit online

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

The following information for Tivoli Monitoring is available in the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter) to gain prerequisite knowledge:

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

Related documentation

Edit online

The documentation for related products provides useful information.

See the following products in IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/):

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

- Tivoli Netcool/OMNIbus

Terminology that is relevant to IBM products is consolidated in one convenient locations at the IBM Terminology website (http://www.ibm.com/software/globalization/terminology).

Other sources of documentation

Edit online

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

See the following sources of technical documentation about monitoring products:

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

Notices

Edit online

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

© IBM 2009. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2009. All rights reserved.

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

Trademarks

Edit online

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

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

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

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

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

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

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

Privacy policy considerations

Edit online

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

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

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

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

Index

SC14-7490-01