Creating a Highly Secure IBM Tivoli Monitoring Agent Configuration

Version 1.0

Version	Date	Comment
1	04/03/12	Initial Public Release

Table of Contents

1.Introduction

IBM® Tivoli® Monitoring agents that run in autonomous or centrally managed modes present new additional options for highly secure deployments of monitoring agents. With a few small postinstallation environment configuration steps, you can have exceptionally secure monitoring agent deployments in highly-constrained environments such as a DMZ.

The Autonomous agent deployment model is similar to the standard centrally managed Tivoli Monitoring agent deployment model where agents communicate with their

infrastructure over secure connections and agents use local configuration files that administrators can manage.

In a secure environment, the agents are invisible to outside network traffic, minimize their communication pathways, and lock down access to the agent files on the file system. A highly secure configuration also ensures strong authenticated encryption on any communication pathways.

This paper includes the steps that are required to lock down open-by-default network connections and to verify the installation is secure from within.

2. Creating a Secure Configuration Security Profile

1. **Anonymous Network Status**

   The goal is to provide no accessible external network trace of the SNMP agent, the Tivoli Monitoring Agent, or both.

   - This involves disabling the normal agent service console ports that follow 1918+x*4096 and 3660+x*4096 (for SSL) on IPv4 and IPv6. Disabling these listener ports does not reduce functionality, but requires the agents to connect to the external Tivoli Enterprise Monitoring Server or SNMP Server instead of allowing them to query the agent directly on their own.

   - General, well-known Service console ports are opened on Port 1920 and 3661 for easy remote access. Disabling these ports prevents the service console from being enabled. After that, configuration can only occur from the CLI or GUI.

   - There are two more ports opened on a per-agent basis for the agent-specific service console that is referenced from the 1920 and 3661 ports.

   - Disable IPv6 or IPv4 to exclusively use one or the other in order to reduce the network exposure profile.

2. **Secure File Permissions**

   To prevent insider unauthorized access to the encryption keys, certificates or logs, the file permissions of the `ITMHOME` directory and all subdirectories must be locked down to well known user IDs and group IDs that are auditable and world read/write/execute access must be removed.

3. **Secure and Confidential Inter-Component Communication/Authentication**

   Authenticate that components are members of the same trusted certificate

authority by using TLS certificate validation that provides confidentiality, data integrity, and a limited form of authentication.

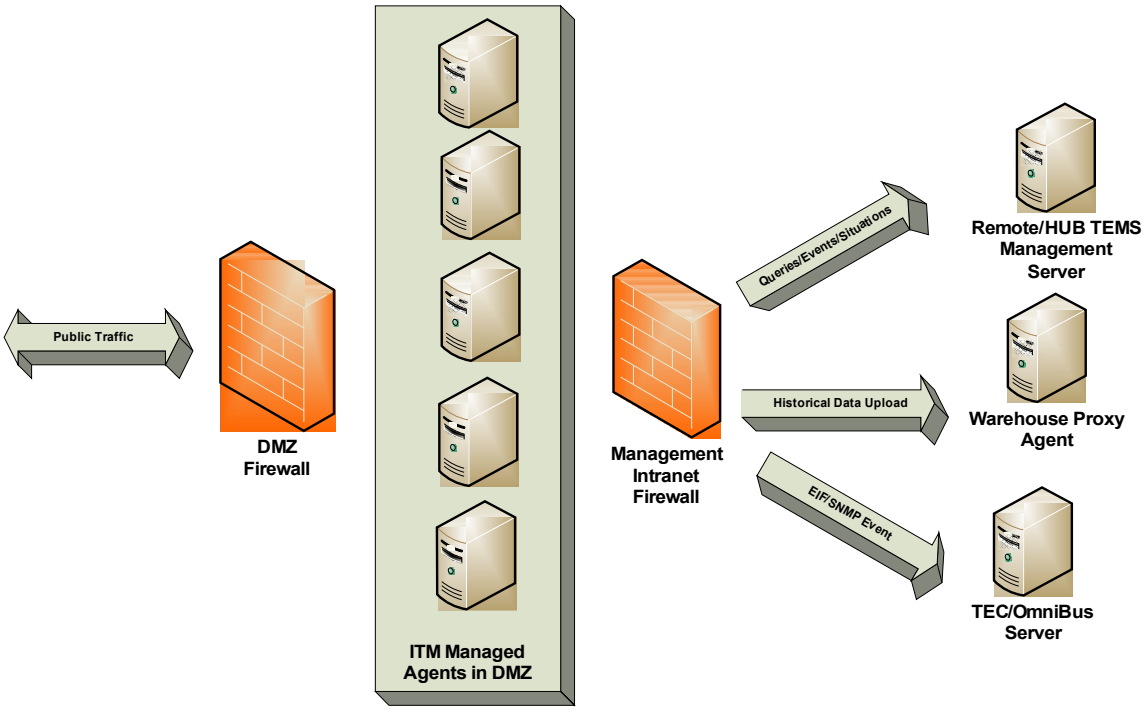
3. Deployment Scenarios

These scenarios are for an agent running in a DMZ that is protected by a firewall on the left and blocked by a firewall on the right from the management infrastructure. The firewall is not required for configuration of the agents in secure mode.

1 Managed Tivoli Monitoring Agent

A highly-secure managed Tivoli Monitoring infrastructure offers two different configurations, depending on whether the customer wants the agents to initiate connections to the monitoring infrastructure servers or the monitoring infrastructure connects to the monitoring agents. This difference impacts your firewall and whether the agents themselves have open ports for a connection to be initiated by a Tivoli Enterprise Monitoring Server.

Managed Agent Deployment Scenario



This agent configuration is intended to accomplish the following things:

- Deliver alerts, heartbeats, and attribute data to Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal users

- Deliver alerts and heartbeats to an event management system (IBM Tivoli Netcool/OMNIbus in this example)
  Optionally, upload data to the Tivoli Data Warehouse components of Tivoli Monitoring and authenticate all possible connections

The standard deployment scenario closes all open ports opened by the Tivoli Monitoring agents (primarily the service console ports). The monitoring agents listen to no ports and only make outgoing connections to the Tivoli Monitoring infrastructure or event servers.

The intranet firewall must be configured to allow outgoing connections from the agents to the configured intranet management servers.

1. Configuring for UNIX and Linux Systems:

1. Optional: Configure the agent to use the Firewall-Gateway mode for allowed proxy servers. Follow the Tivoli Monitoring Firewall-Gateway configuration guide for details.

2. Enable the agent to use ephemeral ports and not static listening ports:

   a. Modify the `<agent product code>.ini` file or the `<agent product code>ENV` configuration file in the agent configuration directory to disable the HTTP server, to disable agent-specific Service Consoles, and to disable non-SSL HTTP servers.

   b. Add the following line to the configuration file. Be sure to write this as one line:

      ```
      KDC_FAMILIES=$NETWORKPROTOCOL$ EPHEMERAL:Y
      HTTP_CONSOLE:N HTTP_SERVER:N HTTP:0
      ```

2) Disable IPv6
3)

   Set the *KDEB_INTERFACELIST_IPV6*=- variable in the custom agent environment file to disable IPv6.
4)

   There is no way to currently disable IPv4 connections.

3. Configure the agent according to the instructions in the "IBM Tivoli Monitoring Certificate Authentication" technote to authenticate the Tivoli Data Warehouse Proxy Agent.
   For every agent that is installed, repeat steps 1- 3.

```
bash-3.00# pwd
/opt/IBM/ITM/config
bash-3.00# tail  ux.ini
KDC_FAMILIES=$NETWORKPROTOCOL$ EPHEMERAL:Y
HTTP_CONSOLE:N HTTP_SERVER:N HTTP:0
KDEB_INTERFACELIST_IPV6=-
bash-3.00#
```

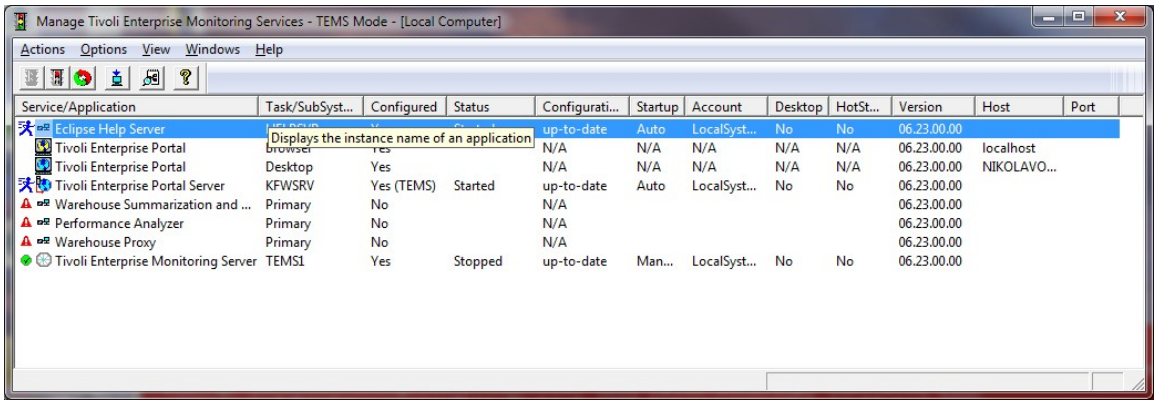
Sample 3 - Secure Custom Managed Agent Configuration File

2. Configuring Windows Agents

Manage Tivoli Enterprise Monitoring Services Configuration

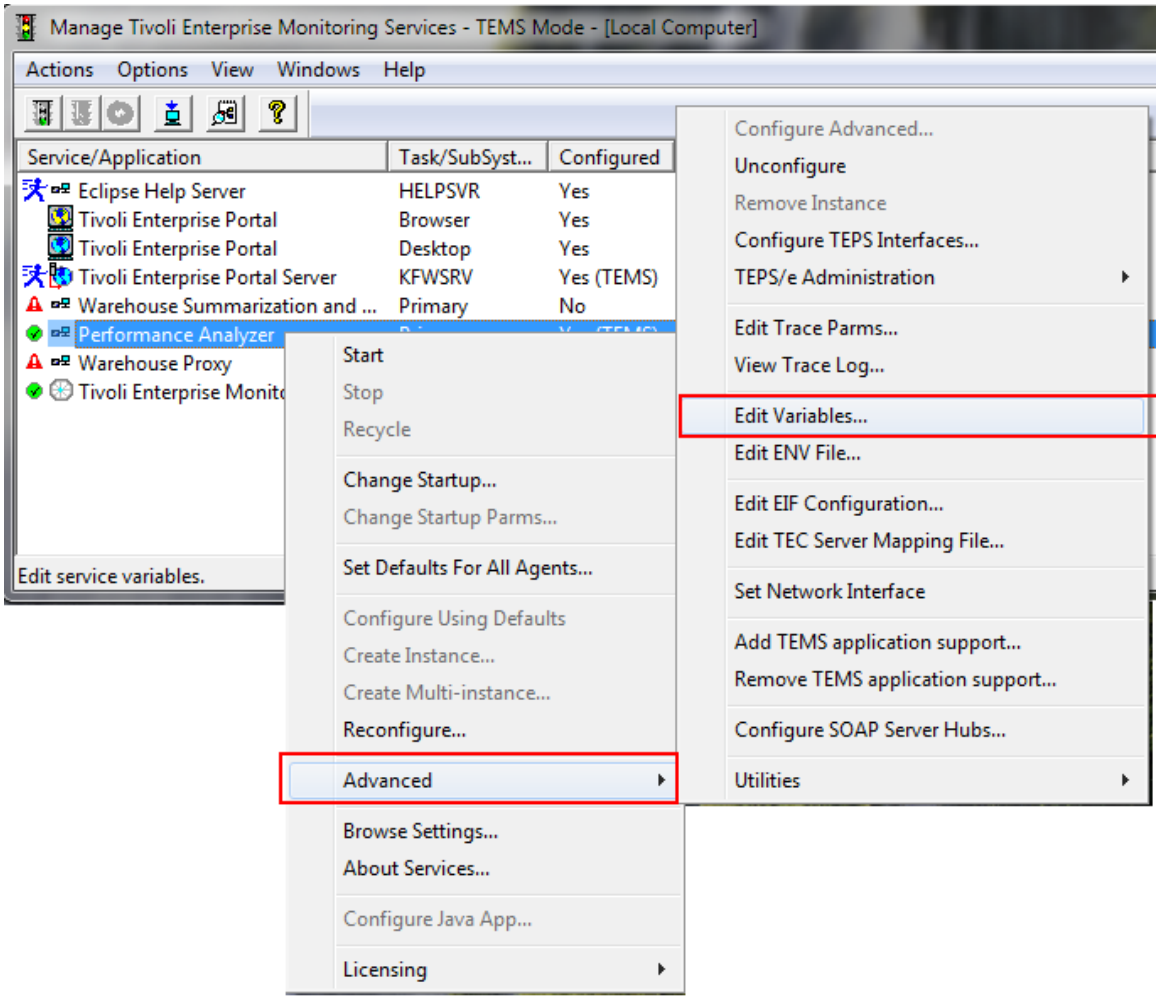
Unlike UNIX and Linux agents, Windows OS agents can have their runtime configuration stored in the local `KxxENV` file in the Tivoli Monitoring home directory or stored in the Windows registry. To properly override these configuration options, you must use Manage Tivoli Enterprise Monitoring Services (MTEMS).

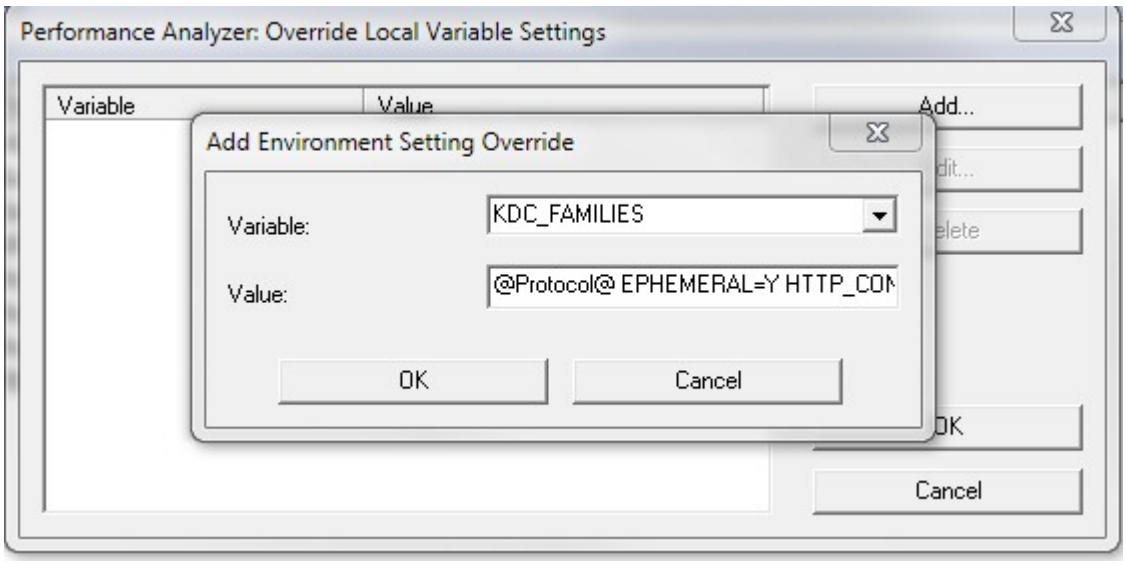
1. Open MTEMS.



2. For each agent that you want to reconfigure, right-click the agent and click **Advanced > Edit Variables**.

Important: The agent must already be configured to be available.

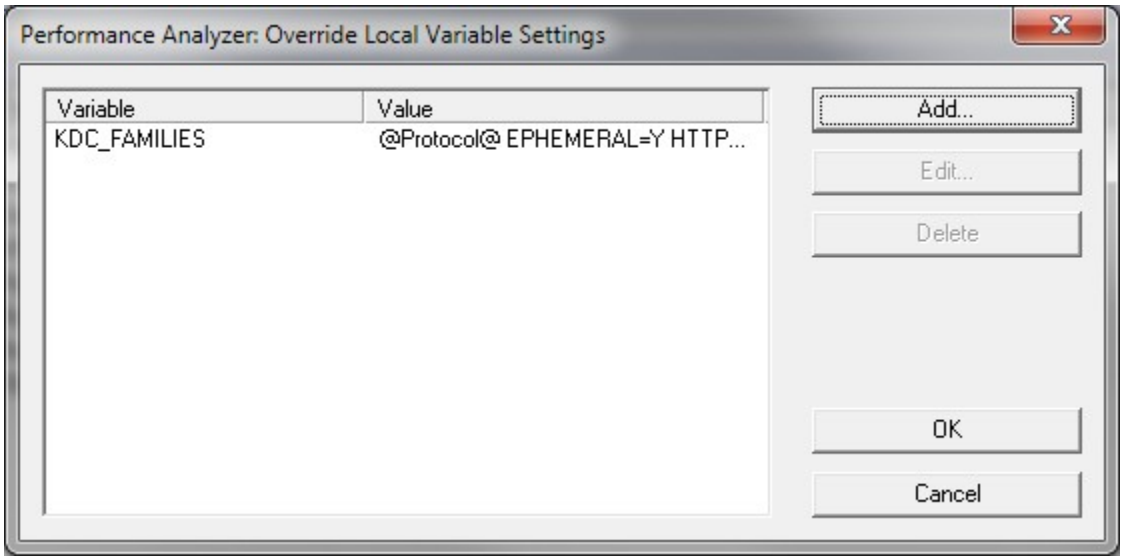

Manage Tivoli Enterprise Monitoring Services - TEMS Mode - [Local Computer]
Actions Options View Windows Help
Service/Application
Task/SubSyst...
Configured
Eclipse Help Server HELPSVR Yes
Tivoli Enterprise Portal Browser Yes
Tivoli Enterprise Portal Desktop Yes
Tivoli Enterprise Portal Server KFWSRV Yes (TEMS)
Warehouse Summarization and ... Primary No
Performance Analyzer
Warehouse Proxy
Tivoli Enterprise Monit
Edit service variables.
Start
Stop
Recycle
Change Startup...
Change Startup Parms...
Set Defaults For All Agents...
Configure Using Defaults
Create Instance...
Create Multi-instance...
Reconfigure...
Advanced
Browse Settings...
About Services...
Configure Java App...
Licensing
Configure Advanced...
Unconfigure
Remove Instance
Configure TEPS Interfaces...
TEPS/e Administration
Edit Trace Parms...
View Trace Log...
Edit Variables...
Edit ENV File...
Edit EIF Configuration...
Edit TEC Server Mapping File...
Set Network Interface
Add TEMS application support...
Remove TEMS application support...
Configure SOAP Server Hubs...
Utilities


Performance Analyzer: Override Local Variable Settings
Variable
Value
Add...
Add Environment Setting Override
Variable:
KDC_FAMILIES
Value:
@Protocol@ EPHEMERAL=Y HTTP_CON
OK
Cancel
OK
Cancel

3. Add a new variable and select **KDC_FAMILIES** from the **Variable** list. Set the following value:

```
@Protocol@ EPHEMERAL=Y HTTP_CONSOLE:N HTTP_SERVER:N HTTP:0
```

4. Click **OK,** and then click **OK** again to save the variable.



The agent is now configured to not bring up any listening ports.

Windows Registry (Alternative configuration method)

As a last option, you can directly edit the Windows Registry, although any changes to the registry are lost after any upgrades.

Open the Windows Registry with RegEdit:

1. Tivoli Monitoring configuration variables are in the following location:
   `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KXX`

2. For each agent (not KHD [Warehouse Proxy Agent], KMS [Tivoli Enterprise Monitoring Server], KFW [Tivoli Enterprise Portal Server]):

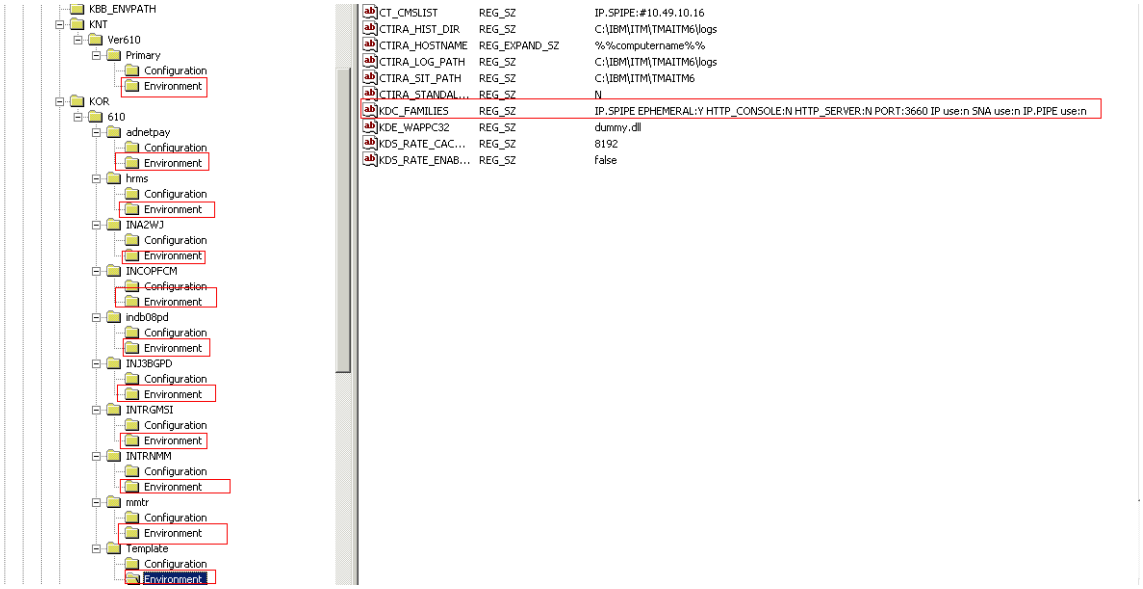
   - If the KDC_FAMILIES key is defined, make the following modification:

IP.SPIPE EPHEMERAL:Y HTTP_CONSOLE:N HTTP_SERVER:N PORT:3660 IP use:n SNA use:n IP.PIPE use:n

KDC_FAMILIES	REG_SZ	IP.SPIPE EPHEMERAL:Y HTTP_CONSOLE:N HTTP_SERVER:N PORT:3660 IP use:n SNA use:n IP.PIPE use:n

- Create the KDC_FAMILIES key, if it is not defined.
- If the KDE_TRANSPORT key is defined, modify it to the same value instead of KDC_FAMILIES.

  The KDE_TRANSPORT key will override the KDC_FAMILIES key.



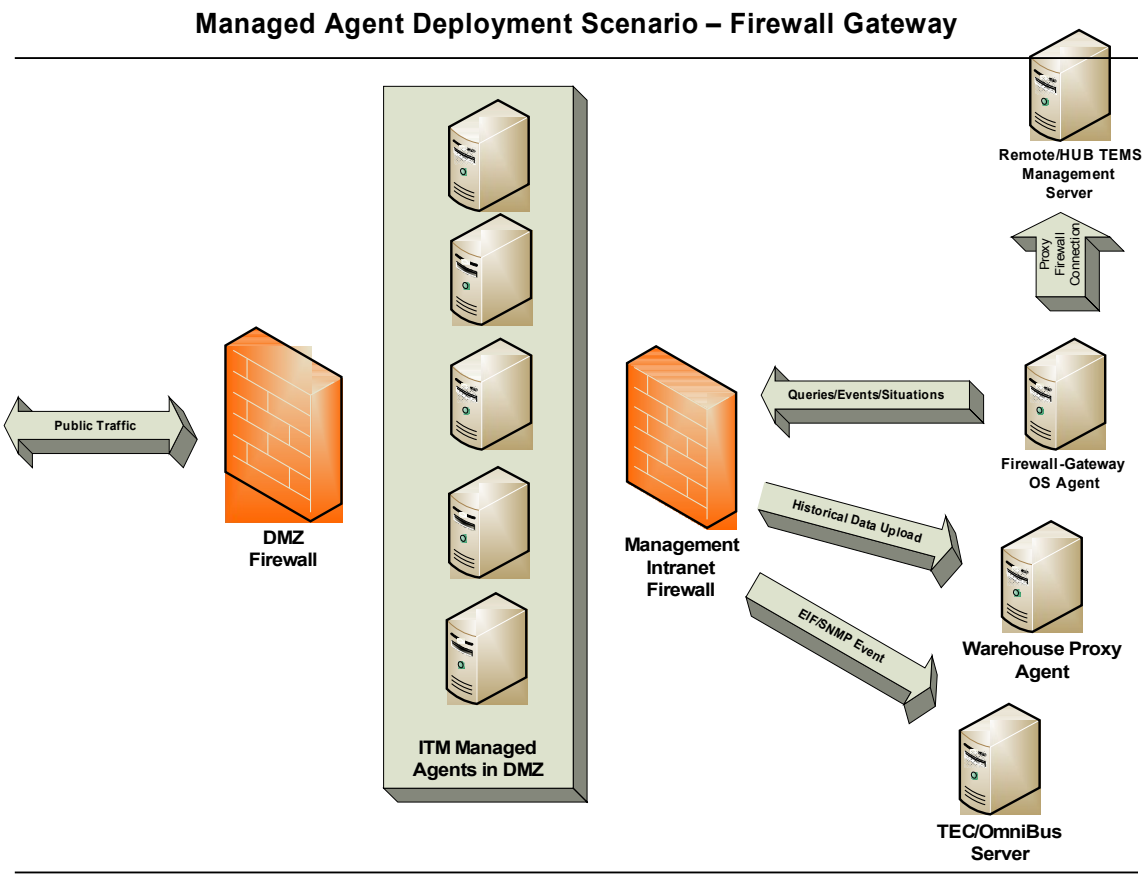
The Windows Registry settings override any environment file values.

2 Managed Tivoli Monitoring Agents using a Firewall Gateway

The configuration of agents that connects through a firewall gateway is the same as the standard managed configuration, except for the additional configuration requirement for the Warehouse Proxy Agent.

When configuring agents behind a firewall-proxy gateway, ensure that you configure the KPX_WAREHOUSE_LOCATION if the Warehouse Proxy agent is not co-located with the RTEMS that the agent is connected to.

For more information on historical warehousing behind a firewall gateway, see the Tivoli Monitoring installation guide appendix on firewalls: (http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.itm.doc_6.2.2fp2/ephemeral_pipe.htm).



This agent configuration is intended to accomplish the following things:

- Deliver alerts, heartbeats, and attribute data to Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal users

- Deliver alerts and heartbeats to an event management system (IBM Tivoli Netcool/OMNIbus in this example)
  Optionally, upload data to the Tivoli Data Warehouse components of Tivoli

Monitoring

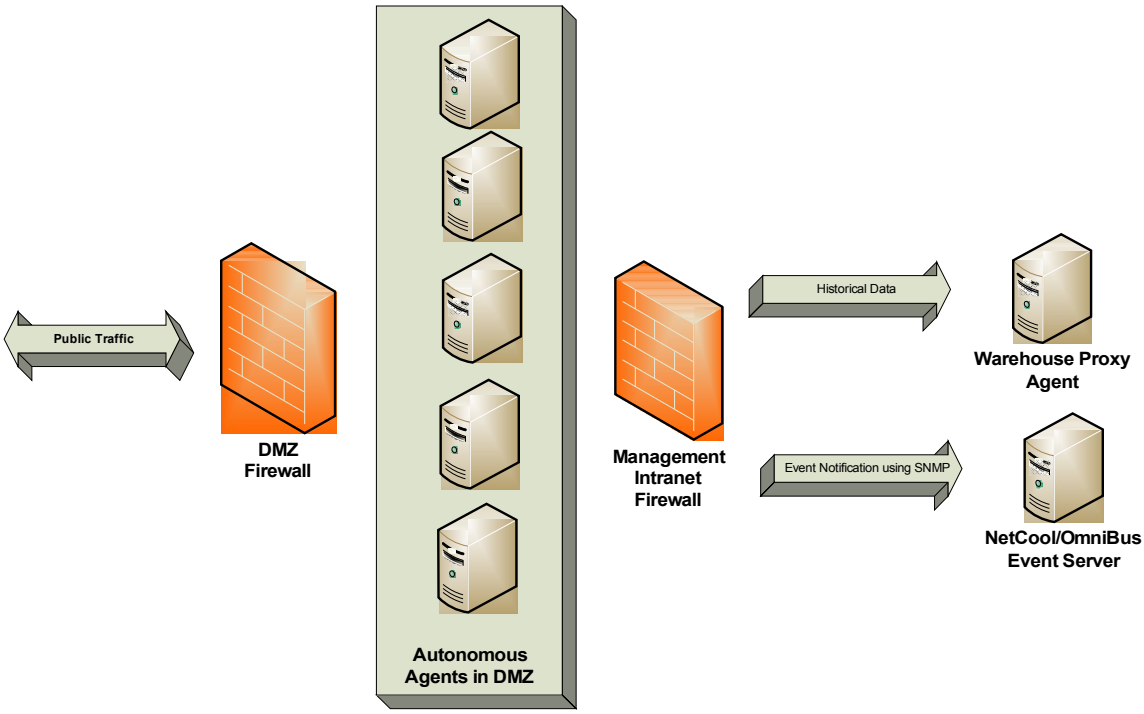
- Allow the IT administrator to force the Tivoli Enterprise Monitoring Server to connect to authorized agents

- Authenticate all network connections

An alternative deployment scenario that you can choose uses the Tivoli Monitoring Firewall-Gateway mechanism to proxy communications between Tivoli Monitoring agents in a DMZ and the management infrastructure behind a firewall. Using this option reduces the number of ports that must be forwarded from the DMZ to the intranet through the intranet management firewall from three to two but does require that each of the agents have their service consoles active.

3 Autonomous Tivoli Monitoring Agent

Autonomous Agent Deployment Scenario



This agent configuration is intended to accomplish the following things:

- Deliver its alerts and heartbeats to an event management system (IBM Tivoli Netcool®/OMNIbus in this example)

- Authenticate all possible connections
  Optionally, upload data to the Tivoli Data Warehouse components of Tivoli Monitoring

Heart beating to the event management system is a standard way for the agent to be monitored from a central location, to ensure timely notification of system or agent failures. The following deployment includes on-box monitoring of the agent through Agent Management Services, which is a local watchdog that ensures that the agents are operational and working within allotted CPU and memory bounds.

In this deployment model, the agent is configured entirely with local configuration files. IT administrators have to allow the Tivoli Monitoring agents to access the event management system and, optionally, the Tivoli Data Warehouse.

2. Configuring for UNIX and Linux Systems:

The following steps apply to UNIX and Linux systems, which rely on the configuration files in the `$ITMHOME/config` directory for all agent configuration.

1. Enable the agent to use ephemeral ports and not static listening ports:
2.

   Create a new `<agent name>.environment` file or edit an existing custom configuration file in the agent configuration directory.
3.
4. Disable the HTTP Server, disable the Agent-Specific Service Consoles, disable the non-SSL HTTP servers:

   Add the following line to the configuration file. Be sure to write this as one line:

   ```
   KDC_FAMILIES=$NETWORKPROTOCOL$ EPHEMERAL:Y HTTP_CONSOLE:N
   HTTP_SERVER:N HTTP:0
   ```

5. Disable IPv6.
6.

   Set the *KDEB_INTERFACELIST_IPV6*=- variable in the custom agent environment file to disable IPv6.
7.

   There is no way to currently disable IPv4 connections.

8. Configure SNMPv3 to use SHA-1 and DES encryption.

9. Configure the agent according to the directions in the "IBM Tivoli Monitoring Certificate Authentication" technote to authenticate the Tivoli Data Warehouse Proxy Agent.

10. For every agent that is installed, repeat steps 1 - 6.

Note that there should be only one KDC_FAMILIES entry in each configuration file.

```
bash-3.00# pwd
/opt/IBM/ITM/config
bash-3.00# cat 1b.environment
KDC_FAMILIES=$NETWORKPROTOCOL$ EPHEMERAL:Y HTTP_CONSOLE:N HTTP_SERVER:N
HTTP:0
KDEB_INTERFACELIST_IPV6=-
bash-3.00#
```

Sample 1 - Secure Custom Autonomous Configuration File

3. Configuring Windows Agents

Windows OS agent configuration is the same as managed Tivoli Monitoring agents, as described previously.

4. Verification

After agents are configured in ephemeral mode and the HTTP servers are disabled, you can use the **`netstat`** command to verify that there are no listening ports by any Tivoli Monitoring components.

Tivoli Monitoring allocates ports for its agent communication using the following algorithm:

1918 + 4096*X where 0 <= X <= 15
3660 + 4096*X where 0 <= X <= 15

There are additional ports opened for any HTTP applications (service console, service interface, soap server, index page):

The 1920 and 3661 ports are used by the HTTP server for the index page by the first agent that starts up, and additional ports are dynamically allocated by additional agents. These ports are chosen by the system dynamically and requests are automatically redirected to them from the 1920/3661 ports so they are not detected in the standard **`netstat`** scan.

1. Verify that the Index Page is no longer being generated:
   In a browser go to http://<server>:1920/ and https://<server>:3661/ .
   An error that the destination server is not found should be generated.

2. 'netstat –an | egrep "1918|3660" should come back clean with no entries.
   If any of the installed applications have a service console or other HTTP process started, then they will register on this port first.

3. The full grep shown below tests for all predictable port values for IP.PIPE/IP.SPIPE and HTTP/HTTPS listening sockets.

   If your configuration was successful, there will be no sockets listening on IPv4 and IPv6.

```
        netstat -an |egrep "1918|6014|10110|14206|18302|22398|26494|30590|34686|
38782|42878|46974|51070|55166|59262|63358|67454|3660|7756|11852|15948|20044|
24140|28236|32332|36428|40524|44620|48716|52812|56908|61004|65100|69196|

        Example: This example shows that not all servers were shutdown

        [root ~]# netstat -an |egrep "1918|6014|10110|14206|18302|22398|26494|30590|
34686|38782|42878|46974|51070|55166|59262|63358|67454|3660|7756|11852|15948|
20044|24140|28236|32332|36428|40524|44620|48716|52812|56908|61004|65100|
69196"
        tcp4       0      0  *.1920                 *.*                    LISTEN
        tcp4       0      0  X.X.X.X.58294      Y.Y.Y.Y.1918       ESTABLISHED
        tcp4       0      0  *.3661                 *.*                    LISTEN
        tcp4       0      0  *.6014                 *.*                    LISTEN

         [root ~]#
```

5. File Permission

An important consideration is access control to the installed agent files and active processes to prevent unauthorized modification of files and to limit exposure.

Be aware that Tivoli Monitoring version 6.2.3 provides this lock down support as part of the installer. The user must ensure the group already exists prior to execution.

Configuration Steps

1. Designate and create a user and group for the exclusive use of Tivoli Monitoring agents (for example, itm/itm).
   Run the **`secureMain -g ITMGROUP`** script to lock down most of the permissions.

2. Change to the `ITMHOME` directory and run the **`chmod -R o-rwx`** command to remove any third party access. Remove group write access to the key files and certificates with **`chmod -R g-w keyfiles`**.

3. Some agents, such as the DB2 or Domino agents, require running with alternative user identities. Add the user identities into the selected ITMGROUP group so they can also write into the Tivoli Monitoring HOME tree.

```
bash-3.00# pwd
/opt/IBM/ITM
bash-3.00# useradd itm
bash-3.00# groupadd itm.
bash-3.00# chown -R itm:itm .
bash-3.00# gpasswd -a db2inst1 itm ; # use system-specific mechanism to add to
group
bash-3.00# gpasswd -a domino itm # use system-specific mechanism to add to group
bash-3.00# cd bin
bash-3.00# ./secureMain -g itm lock
Enter the root password if prompted
== baseSecureLock
== xxSecureLock 1b
== xxSecureLock 1d
== SecureSkip ax
== xxSecureLock gs
== xxSecureLock ux
== SetPerm -a
bash-3.00# cd ..
bash-3.00# chmod -R o-rwx .
bash-3.00# ls -l
total 28
drwxr-x---   2 itm      itm        1024 Nov 24 14:28 bin
drwxrwx---   5 itm      itm        1536 Nov 24 14:28 config
drwxr-x---   2 itm      itm         512 Nov 24 14:28 keyfiles
drwxr-x---   3 itm      itm         512 Nov 24 14:28 licenses
drwxrwx---   9 itm      itm         512 Nov 24 14:28 localconfig
drwxrwx---   2 itm      itm        1536 Nov 24 14:44 logs
drwxr-x---   2 itm      itm         512 Nov 24 14:41 registry
```

```
-rw-------   1 itm      itm           0 Nov 24 14:41 samples
drwxr-x---   5 itm      itm         512 Nov 24 14:28 sol286
drwxr-x---   3 itm      itm         512 Nov 24 14:28 sol296
drwxr-x---   5 itm      itm         512 Nov 24 14:28 tmaitm6
drwxrwx---   2 itm      itm        1536 Nov 24 14:28 tmp
bash-3.00# chmod –R g-w keyfiles
bash-3.00# ls -l keyfiles/
total 280
-rw-r-----   1 itm      itm          48 Nov 24 14:28 KAES256.ser
-rw-r-----   1 itm      itm          88 Nov 24 14:28 keyfile.crl
-rw-r-----   1 itm      itm      125088 Nov 24 14:28 keyfile.kdb
-rw-r-----   1 itm      itm          88 Nov 24 14:28 keyfile.rdb
-rw-r-----   1 itm      itm         129 Nov 24 14:28 keyfile.sth
```

Sample 2 - Secure Permission Setting

6. Additional Considerations

1. The SNMP stack currently implements RFCs 3411-3418. The encryption methods detailed in this set of specifications (MD5/SHA1/DES) are not FIPS 140-2 compliant.

2. The agents are completely passive with no network accessible ports. The agents must be configured using the local system account configured for managing Tivoli Monitoring.

3. Configuration with symmetric certificate authentication requires careful management of certificates and certificate databases. Refer to the technote "Enabling IBM Tivoli Monitoring Symmetric Certificate Authentication" for more details on configuring your environment and components to use both client and server certificate validation.

7. Conclusions

Following the standards that are recommended in this paper, deployed agents become invisible to external network entities and communicate using secure techniques while still remaining completely functional.

Notices

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785 U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan, Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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

IBM Corporation

2Z4A/101

11400 Burnet Road

Austin, TX 78758 U.S.A.

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

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

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

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

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

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the

names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks