Tamino

Setting Up Tamino

Version 8.2.2

October 2013

This document applies to Tamino Version 8.2.2.

Document ID: INS-AFTERINSTALL-822-20130226

Table of Contents

Preface

Tamino is installed using the webMethods Installer. Please refer to the webMethods Installer documentation, which you can find at **http://documentation.softwareag.com/**.

Before You Start Using Tamino

- **Customizing the Environment**
- **Configuring the Web Server**
- **Other Issues**
- **Prerequisites for Reading the Online Documentation**
- **Problems with Blocked Content**
- **Next Steps**

1 Before You Start Using Tamino

Customizing the Environment

HP-UX

Tamino requires some settings of system variables to be adjusted. You can do this using the “smh” tool. The “smh” tool requires a working X11 display server; ensure that the `DISPLAY` environment variable points to a suitable machine.

Execute the following command as the root user:

```
/usr/sbin/smh
```

A window appears. Select the option **Kernel Configuration**, then select the option **Tunables**. A new window appears, displaying several kernel parameters and their values. Scroll down until you see the entry you intend to change.

Select the entry, then choose **Modify Tunable** to change its value to the required value, which you can take from the table below:

```
Variable Name    Required Value
max_thread_proc  256
maxdsiz          0X0C000000
msgmap           512
msgmax           8192
msgmnb           64000
msgmni           512
msgseg           8192
msgssz           8
msgtql           512
semaem           16384
semmap           512
semmni           512
semmsl           512
semmns           1024
semmnu           1024
semume           36
semvmx           32767
shmmax           512000000
shmmni           100
```

Tip: If you use many XML work threads or work with a large number of clients, you should consider setting the `max_thread_proc` parameter to an even higher value in order to avoid possible emergency stops.

Caution: Do not change the `maxdsiz_64` parameter regardless of whether you are running a 64 bit or a 32 bit environment!

Linux

After installing Tamino, ensure that the shared memory limit is at least 512 megabytes. To check the current value, examine the value of the Linux kernel parameter `shmmax` as follows:

```
cat /proc/sys/kernel/shmmax
```

To set `shmmax` to a value of 512 megabytes (which should be sufficient for medium-size databases), enter the following command:

```
echo "512000000" > /proc/sys/kernel/shmmax
```

We recommended setting the variable `shmmax` to the value of the size of the physical memory in bytes. You can find out how much memory there is in your machine with

```
cat /proc/meminfo
```

For very large databases, it might be necessary to increase the value of the parameter `shmmax`.

Note that this change is not persistent, so after a reboot the parameter will have the old (default) value. In order to change this, add the following line to the */etc/sysctl.conf* script:

```
kernel.shmmax = 512000000
```

To ensure that */etc/sysctl.conf* is parsed after a reboot, enter the following command:

```
/sbin/chkconfig boot.sysctl on
```

Solaris 9

Note: This section applies only to Solaris 9. Under Solaris 10 there is no need to customize the Solaris environment for Tamino.

Under Solaris 9, Tamino requires kernel parameters to be set. The minimum values for these parameters are shown in the following list. Check the file */etc/system* to see if the current parameter values match those listed below. If you modify these values you must reboot the machine so that the changes take effect.

```
set pt_cnt=512

* set incode cache
set ufs_ninode=32000

* set DNLC (Directory Name Lookup Cache)
set ncsize=32000

set msgsys:msginfo_msgmap=512
set msgsys:msginfo_msgmax=8192
set msgsys:msginfo_msgmnb=64000
set msgsys:msginfo_msgmni=512
set msgsys:msginfo_msgseg=8192
set msgsys:msginfo_msgssz=8
set msgsys:msginfo_msgtql=512
set semsys:seminfo_semaem=16384
set semsys:seminfo_semmap=512
set semsys:seminfo_semmni=512
set semsys:seminfo_semmsl=512
set semsys:seminfo_semmns=1024
set semsys:seminfo_semmnu=1024
set semsys:seminfo_semume=36
set semsys:seminfo_semvmx=32767
set shmsys:shminfo_shmmax>=512000000
set shmsys:shminfo_shmmni=100
set npty=512
```

It is recommended to set the variable `<shmmax>` to the size of the physical memory in bytes. You can find out how much memory there is in your machine on Solaris with the command `prtconf | fgrep "Memory size"`.

Configuring the Web Server

This document contains information about managing web servers.

Usually, client applications access Tamino using HTTP via a web server.

Note: With Tamino XML Server version 4.1 or later, databases can also be accessed via a webserverless mode.

To specify that a particular database may only be accessed through a particular web server, define the web server as described below and assign it to a particular database via the Web Servers object in the tree-view frame.

The following topics are covered:

- Overview of Web Servers
- Apache for Microsoft Windows

- Apache for UNIX
- Microsoft IIS
- Tomcat
- Activating Web Server Authentication Mechanisms

Overview of Web Servers

Usually, client applications access Tamino using HTTP via a web server. Each web server that is required to provide access to Tamino must be configured accordingly.

Note: Tamino version 4.1 or later can also be used without a web server. This is done by some Tamino APIs and tools, for example.

If you use a web server, it does not need to be located physically on the machine on which Tamino is installed; it can be located anywhere in the network where Tamino is installed. For example, it is possible to have Tamino running on a Windows machine and the web server running on a UNIX machine in the same network or vice versa.

A single web server can be configured to access Tamino servers on several machines.

Apache for Microsoft Windows

General

The Tamino interface is a DSO (dynamic shared object: Apache terminology for DLL/shared library), so your Apache must have DSO support. DSO support is included in the default configuration of Apache. Apart from this, there are no special requirements for Tamino. For Apache configuration, tuning etc., it makes no difference whether the requested resources are in a file system or in a Tamino database.

The Tamino installation kit for Microsoft Windows contains a binary distribution of Apache. Apache is not installed during the Tamino installation, but the binary distribution of Apache is copied to the subfolder *X_Port/Apache/dist* of the Tamino installation area on disk during the Tamino installation procedure. You can install this Apache kit manually if you want to use Apache to communicate with Tamino and you do not have an Apache installed yet. Please note that this distribution is not modified or customized for Tamino in any way. Furthermore, Software AG does not maintain this distribution. If you already have Apache installed, we recommend using your existing installation. The Apache distribution in the Tamino kit was current when the kit was frozen; if a newer patch level of Apache is available when you do the installation, we recommend using it.

Source Distribution

The Tamino interface is provided in binary form; these binary files work for current standard Apache distributions. However, under certain circumstances, it may be desirable or necessary to compile and link the Tamino interface. Possible reasons are:

- Your Apache is built with compile/link options that are incompatible with the provided binary files.
- You prefer to use open source software.

The Tamino installation provides the Apache interface in the directory *X_Port\Apache*. This directory contains the source code, the necessary header files and link libraries, and an example *makefile* that can be adapted to the current platform. If the platform supports both 32-bit and 64-bit versions, the appropriate link libraries can be found in corresponding subdirectories.

Configure Apache

Apache must be configured as described below.

Note: We strongly recommend that you make a backup copy of the Apache configuration file *httpd.conf* before proceeding.

Copy the file *Apache2ModuleIno.dll* to your Apache *modules* directory.

Add the following to the Apache *httpd.conf* file:

```
LoadModule  ino_module modules/Apache2ModuleIno.dll

<Location /tamino>
SetHandler ino
</Location>
```

This results in an attempt to establish a connection between Tamino and the web server using XTS. If this fails, e.g. because the server property `communication method` has been set to "TCP/IP", the local configuration information is searched for the XML port of the database. In this case a native TCP/IP connection is established, if the database is local.

Note: If you use Apache 2.2.*x*, the name of this file is *Apache22ModuleIno.dll*.

It is only necessary to specify host and port information as shown in the following example if you want to use native TCP/IP communication to access a Tamino database server on a remote system.

If the Apache web server and the Tamino server are not on the same machine, then in order to enable the Apache web server to access Tamino databases via native TCP/IP, add the following section to the *httpd.conf* file for each database:

```
<Location /tamino/mydb>
SetHandler ino
InoHost xyz.abc.de
InoTcpipPort 4711
</Location>
```

Replace `mydb` by the name of the database, replace `xyz.abc.de` by the name of the host where the database server is running, and replace `4711` by the number of the database's XML port, which you can find via Tamino Manager (in the **Properties** dialog of the database).

Configuring Apache for Authorization in Conjunction with Tamino

Note that it is not possible to use Apache *.*htaccess* files ("distributed configuration files") in conjunction with Tamino to specify authorization information. These files are typically located in the same directory as the files to be read, but there is no such directory in the case of Tamino. This problem can easily be circumvented by specifying exactly what would otherwise be the content of your *.*htaccess* file in a <Location> directive in your *httpd.conf* file, for example:

```
<Location /tamino>
# Put here exactly the contents of your *.htaccess file
</Location>
```

Apache for UNIX

Tamino interface to Apache

The Tamino interface is a DSO (dynamic shared object: Apache terminology for DLL/shared library), so your Apache must have DSO support. DSO support is included in the default configuration of Apache. Apart from this, there are no special requirements for Tamino. For Apache configuration, tuning etc., it makes no difference whether the requested resources are in a file system or in a Tamino database.

Supported Apache Variants

UNIX-based operating systems, including Linux and AIX, normally include Apache or a derivative of Apache as part of the distribution. In the case of IBM's AIX, the standard server is called "IBM HTTP Server". X-Machine's Apache interface can also be used in these systems. Tamino has been tested with the following Apache or Apache-derived web servers:

AIX
: The IBM HTTP Server.

HP-UX
: The HP-UX Apache-based Web Server.

Linux

The Apache web server that is delivered with the respective Linux distribution.

Apache Portability Runtime Library Name

On UNIX (including Linux) systems, Tamino's Apache interface is linked against the Apache portability runtime (APR) library (*libapr.so*). The name of this library can be customized in Apache. If *libapr.so* has a different name in your Apache (e.g. a versioned name like *libapr-0.so*), please create a file system link between the real name and *libapr.so*, or use the source distribution (see above).

Modifying the httpd.conf File

Modify the file *$SAG>/ino/vxx/X_Port/Apache/TaminoApache.conf*, an example of which is shown below.

Note: In the *TaminoApache.conf* file that is installed on your system, *$SAG* and v*xx* will be replaced by the appropriate values. As indicated in the comments, you must specify either "32bit" or "64bit" as appropriate, and also *Apache2ModuleIno.so* if you are using Apache v2.0 or *Apache22ModuleIno.so* if you are using Apache v2.2.

```
## BEGIN Software AG, Tamino
#  Thu Nov 13 09:51:07 CET 2008
#
#
# This file is included from the Apache conf file "http.conf".
# This configuration file can be used with Apache v2.0.xx and above.
#
#
# the tamino module
# e.g.  Apache 2.0.xx, 32-bit:  $SAG/ino/vxx/X_Port/Apache/32bit/Apache2ModuleIno.so
#      Apache 2.0.xx, 64-bit:  $SAG/ino/vxx/X_Port/Apache/64bit/Apache2ModuleIno.so
#      Apache 2.2.xx, 32-bit:  $SAG/ino/vxx/X_Port/Apache/32bit/Apache22ModuleIno.so
#      Apache 2.2.xx, 64-bit:  $SAG/ino/vxx/X_Port/Apache/64bit/Apache22ModuleIno.so
#
LoadModule ino_module "$SAG/ino/vxx/X_Port/Apache/32bit/Apache2ModuleIno.so"
#
<Location /tamino>
    SetHandler ino
    InoRegfile "$SAG/common/rgs/REGFILE"
</Location>



<Directory $SAG>
Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

```
#
#
# documentation of Tamino
#
Alias /tamino-v8.0/en/Documentation  "$SAG/ino/vxx/Documentation/en"
Alias /tamino-v8.0/en/tii            ↩
"$SAG/ino/vxx/X_Tools/Tamino_Interactive_Interface/en"
Alias /tamino-v8.0/README.TXT        "$SAG/ino/vxx/README.TXT"

#
# documentation of SMH
#
Alias /common/arg/help/doc     "$SAG/common/arg/help/doc"
#
# optional links (only if tools were installed)
#
Alias  /tamino-v8.0/tii      "$SAG/ino/v80/X_Tools/Tamino_Interactive_Interface"
#
## END Software AG, Tamino
```

Include the following line in your *httpd.conf* file:

```
Include "<path_to_tamino/$SAG>/ino/vxx/X_Port/Apache/TaminoApache.conf"
```

It is only necessary to specify host and port information as shown in the following example if you want to use native TCP/IP communication to access a Tamino database server on a remote system.

If the Apache web server and the Tamino server are not on the same machine, then in order to enable the Apache web server to access Tamino databases via native TCP/IP, add the following section to the *httpd.conf* file for each database:

```
<Location /tamino/mydb>
SetHandler ino
InoHost xyz.abc.de
InoTcpipPort 4711
</Location>
```

Replace `mydb` by the name of the database, replace `xyz.abc.de` by the name of the host where the database server is running, and replace `4711` by the number of the database's XML port, which you can find via Tamino Manager (in the **Properties** dialog of the database).

Microsoft IIS

This section describes installation and configuration aspects of Tamino and Microsoft Internet Information Services (IIS). The following topics are covered here:

- Installation of modiis.dll as a Filter in IIS
- Correcting the Configuration of Microsoft IIS if HTTP Error 403 (read access forbidden) Occurs when Trying to Access Tamino in Conjunction with IIS

Installation of modiis.dll as a Filter in IIS

To install *modiis.dll* as a filter in IIS

1. Copy the file *modiis.dll*, which you can find in the folder *X_Port\IIS* folder of your installed Tamino environment, to the directory to which the IIS *virtual* directory *inoScripts* points (*C:\Inetpub\inoScripts* by default).

   Note: If the *virtual* directory *inoScripts* does not exist, create it and copy *modiis.dll* into it.

2. From the IIS Administrator, select the web server to which the filter should be added.
3. Select **Properties** (for instance, using the right mouse button).
4. Select the **ISAPI Filter** tab.
5. Select **Add** and enter Tamino as **Filter Name** and the *modiis.dll* of the scripts directory (*C:\Inetpub\inoScripts*) as **Executable**.
6. In IIS 6.0, add the file *modiis.dll* in the IIS Administrator/Web Service Extension as the extension for Tamino and enable the extension as all executables need to be explicitly permitted in IIS version 6.0.

Restarting the IIS web server enables it to access local Tamino databases.

If XTS communication is not used, then in order to enable an IIS web server to access remote Tamino databases, locate the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Software AG\Tamino\IIS Mapping\Prefix
```

Under this key you may have a list of keys for the individual path prefixes you want to map (for each remote Tamino database you want to access, enter a key `tamino/dbname`, where `dbname` is to be replaced by the name of your database). This sub key has three subordinate string values:

- one is named “Host” and its value is the host name of the Tamino server;
- another is named “Port” and its value is the Tamino server's XML port number;
- the third is named “Location” and its value is the actual path prefix.

Example of database *mydb* (in regedit format):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Software AG\Tamino\IIS Mapping]
[HKEY_LOCAL_MACHINE\SOFTWARE\Software AG\Tamino\IIS Mapping\Prefix]
[HKEY_LOCAL_MACHINE\SOFTWARE\Software AG\Tamino\IIS Mapping\Prefix\tamino/mydb]
"location"="tamino/mydb"
"Host"="mypc.mycompany.com"
"Port"="5005"
```

Note that the forward slash between the strings “tamino” and “mydb” is correct and necessary, because *tamino/mydb* is part of a URL.

After changing the registry, the World Wide WEB Publishing Service must be restarted (item **Services** in the Windows control panel).

Correcting the Configuration of Microsoft IIS if HTTP Error 403 (read access forbidden) Occurs when Trying to Access Tamino in Conjunction with IIS

HTTP Error 403 (read access forbidden) may occur due to incorrect configuration of IIS. You can verify this situation and correct the configuration as follows:

To verify and correct the configuration for using Tamino with IIS

Verification: To test this, enter a Tamino-URL in the browser, e.g. *http://MYHOST/tamino/myDB?_diagnose=ping*. If HTTP error 403 occurs and you are using the Microsoft Internet Information Server (IIS) web server, you should proceed as follows:

1. Open the Microsoft Management Console (MMC) in order to configure the IIS;
2. With your host name, open “Default Web Site”;
3. Click the right mouse button on “inoScripts”;
4. Change the properties of this folder;
5. Make sure that under “Virtual Directory” the “Permissions” are set to “Execute”.

Note: This value may be set to “Scripts” e.g. by the “Microsoft Lockdown” utility.

Tomcat

A standalone Tomcat server cannot be used to communicate to X-Machine via HTTP. Programs running under Tomcat can use the webserverless interface instead.

Activating Web Server Authentication Mechanisms

This section discusses how to activate the authentication mechanisms of the various web servers that Tamino supports.

- For Apache
- For Microsoft IIS

For Apache

The following example is an extract of a suitable Apache configuration file *httpd.conf* to set the authentication mechanism for all databases:

```
# ------------------------------------------------------------------
# Enable Apache Web Server Authentication for Tamino Security
# Note: The AuthUserFile is created with pgm ../apache/bin/htpasswd.exe
#       Enter command 'htpasswd -h' for pgm usage description
#       Restart Apache Web Server after modification
# If authorization fails:
# - Check Apache error.log file
# - Enter browser command http://localhost/tamino/secdb?_diagnose=echo

<Location /tamino>
AllowOverride AuthConfig
AuthName "Tamino"
AuthType Basic
AuthUserFile "bin/userids"   <== file created with htpasswd.exe
require valid-user
</Location>
```

It is also possible to set the authentication mechanism for individual databases. To do so, add the database name to the location:

```
<Location /tamino/mydb>
```

For Microsoft IIS

Activate the checkbox **Integrated Windows Authentication** in the “Authentication Methods” dialog box.

Caution: Do not activate the checkbox “Basic Authentication (password is sent in clear text)”, because this option can cause severe problems.

To get to the “Authentication Methods” dialog box, choose the **File Security** tab in the “modiis.dll Properties” window of the IIS, then choose **Edit** in the “Anonymous access and authentication control” section.

Other Issues

All Operating Systems

Extended Transport Service (XTS)

To enable clients to locate Tamino databases by name, even in a distributed environment, Tamino uses the XTS (eXtended Transport Service) directory service.

XTS provides a uniform mechanism for Software AG products to communicate with each other across diverse platforms using multiple protocols and different types of hardware.

XTS offers two methods of maintaining the directory:

1. **Software AG directory server**

   A standalone service, included in the distribution as an installable package

2. **Flat file implementation**

   Can be used if all participants are on the local machine. The flat file implementation is used under the condition that an environment variable XTSDIR is defined and contains a valid path pointing to a directory where the flat file is created and maintained by XTS.

Starting with Tamino v8.0 the default mechanism for XTS was changed from the Software AG directory server to the flat file implementation.

That means that for each client accessing a Tamino database the XTSDIR environment variable must be defined and contain the same value as the database server uses (the XTSDIR setting of the Tamino 8.2 databases can be found in the registry under *HKEY_LOCAL_MACHINE\SOFTWARE\Software AG\System Management Hub\Products\Tamino\v82\Environment*).

"Client" in this case means the instance addressing the database server via XTS. For example, if Tamino is accessed via an Apache web server then the XTSDIR environment variable must be defined for the Apache web server process.

However, for replication, due to the fact that the databases reside on different nodes, it is necessary to use the Software AG directory server.

Further reading:

Switching between the two XTS directory methods	*Installing Tamino XML Server > Complete the Installation*
Setting up the Software AG directory server	*Setting Up Tamino > Before You Start Using Tamino > Other Issues*

To use XTS with the Software AG directory server, Tamino must be able to resolve SAGXTSDShost and SAGXTSDSport to IP addresses (if SAGXTSDSport cannot be resolved, a default value is used). This can either be done by a DNS server (or by entering the two well-known names in your local hosts file).

The entries in the hosts file are as follows:

```
<IP address of the master node>         SAGXTSDShost
x.y.0.0                                 SAGXTSDSport
```

where *master node* is the node where the directory of the Extended Transport Service is running.

The port number is calculated as 256 * x + y. Thus, for example, if the port number should be set to 12731, then SAGXTSDSport must be defined as 49.187.0.0 (12731/256 = 49, remainder 187).

This information is provided in case you want to custom configure the `SAGXTSDSport`.

Note: Tamino registers with XTS using host names, not IP addresses. For a remote client to resolve the host name into an IP address, the host name either has to be present in DNS or an entry for that host name must be entered in the client's local *etc/hosts* file.

Linux

Parallel Boot Mode

If the system is configured to run in parallel boot mode, set the parameter `RUN PARALLEL="no"` in the file */etc/sysconfig/boot*.

Prerequisites for Reading the Online Documentation

- **HTML Browser**

  For viewing the online documentation, a browser capable of supporting Java, JavaScript, and Cascading Style Sheets (CSS) is recommended. The documentation has been successfully tested with these products:

  - **Microsoft Internet Explorer** version 8.x.
  - **Microsoft Internet Explorer** version 7.x.

- **Mozilla Firefox** version 3.x.

These browsers are freely available for download.

- **Java Browser Plug-in**

The documentation has been successfully tested with the following browser plug-ins:

- Sun JVM 1.6.0

Caution: Using Sun Java 6 update 10 may lead to problems.

We recommend going to **http://java.com/** to acquire a free Java browser plug-in.

- **PDF Viewing Software**

For viewing the PDF documentation:

- A PDF reader such as the **Adobe Reader** must be installed.

The Adobe Reader is freely available for download.

Problems with Blocked Content

Software AG documentation uses active content (JavaScript and Java applets). With Service Pack 2 (SP2) for Windows XP, Microsoft introduced a range of powerful new security features. One effect of these security features is that warning messages appear whenever you try to display HTML pages that use active content, for example Software AG documentation, in the Internet Explorer. A typical warning message that appears in the Internet Explorer information bar is:

Caution: To help protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options...

To continue using the documentation, you can do one of the following:

- Use a different web browser. This problem only affects Microsoft's Internet Explorer.

Note: Software AG does not endorse or recommend any web browser.

- Change the Internet Explorer options to allow active content to run in files on your computer.

To unblock active content

In the Microsoft Internet Explorer:

1 Choose **Tools**> **Internet Options**.

2. Choose the tab **Advanced**.
3. Scroll down to the section **Security**.
4. Check (tick) the box **Allow active content to run in files on My Computer**.
5. Choose **OK**.
6. Restart the Internet Explorer.

The warning messages should now no longer appear.

- Click on the information bar and choose the option **Allow Blocked Content...**. You will have to do this for each affected page.

Next Steps

You have now completed the installation of Tamino and set up the environment, and are ready to start using Tamino. The next steps are described in the section *Getting Started*.

Index