Technical Note: Deploying Access Manager to an Application Server Cluster

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–6769–10
May 2006

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, Java et Solaris sont des marques de fabrique ou des marques déposées, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

060718@14986

Technical Note: Deploying Access Manager Instances to an Application Server Cluster

This document describes how to deploy Sun Java™System Access Manager 7 2005Q4 to a Sun Java System Application Server Enterprise Edition 8.1 2005Q4 cluster, either on a single host server or on multiple host servers, including:

- "Before You Get Started" on page 3
- "Installation and Configuration Steps" on page 4
- "Accessing Sun Resources Online" on page 9
- "Revision History" on page 10

Before You Get Started

This document is intended for system administrators and software technicians. You should be familiar with the administrative commands for your deployment platform (Solaris™ system or Linux system) and the following tasks.

Task	Where to Find More Information
Running the Java ES installer to install Java ES components. The examples in this technical note will use separate machines for the following. with Access Manager installed on all three machines: ■ Sun Java System Application Server with cluster instances ■ Sun Java System Directory Server Access Manager requires Directory Server. Either install a new Directory Server or use an existing one. ■ Sun Java System Web Server as a Load Balancer.	*Sun Java Enterprise System 2005Q4 Installation Guide for UNIX*
Applying any required patches for Access Manager and other Java ES components.	Check for required patches in the Java ES 2005Q4 Release Notes Collection: `http://docs.sun.com/coll/1315.1` Also, check with your Sun Microsystems technical representative. You can download patches from SunSolve Online: `http://sunsolve.sun.com/`
Administering Access Manager, Application Server, and Directory Server	Java ES component documentation: ■ Access Manager: `http://docs.sun.com/coll/1292.1` ■ Application Server: `http://docs.sun.com/coll/1310.1` ■ Directory Server: `http://docs.sun.com/coll/1316.1`

Installation and Configuration Steps

To deploy Access Manger instances to an Application Server 8.1 2005Q4 cluster, follow these steps:

- "Install and Configure Application Server" on page 4
- "Install and Configure Access Manager" on page 6
- "Add Instances to the Platform Server List and Realm/DNS Aliases" on page 7
- "Add Listeners to the Clusters for the Load Balancer" on page 8
- "Restart All Application Server Instances" on page 9

Install and Configure Application Server

In this section, one machine will contain the DAS host server and the Application Server `host-server1`). Two additional servers (`server1` and `server2`) will contain the Application Server instances.

1. Install Application Server using the Java ES installer with the Configure Now option. When you install Application Server, the Java ES installer also creates the node agent. .
2. Install the Application Server command line utilities on `server1` and `server2`. You will install node agents on these servers (See Step 3c). The examples in this document use `nodeagent1, nodeagent2, nodeagent3` as the node agent names
3. Configure the Application Server Cluster. Examples in the following steps use the Application Server `asadmin` command-line utility; however, you can use the Application Server Administration Console, if you prefer.
   a. Start the node agent on the DAS (`host-server1`). For example:

      ```
      asadmin> start-node-agent --user admin --passwordfile password-file nodeagent1
      ```

   b. Create node agents on `server1` and `server2`.

```
asadmin> create-node-agent --host host-server1.example.com --port 4849 --user admin
--passwordfile password-file nodeagent2
asadmin> create-node-agent --host host-server1.example.com --port 4849 --user admin
--passwordfile password-file nodeagent3
```

   c. Start the node agents on `server1` and `server2`. For example:

      ```
      asadmin> start-node-agent --user admin --passwordfile password-file nodeagent2
      asadmin> start-node-agent --user admin --passwordfile password-file nodeagent3
      ```

   d. Create the cluster on the DAS. For example:

      ```
      asadmin create-cluster --user admin --passwordfile password-file amcluster
      ```

   e. Create a server instance for the cluster at the DAS. For example:

      ```
      asadmin> create-instance --user admin --passwordfile password-file
      --cluster amcluster --nodeagent nodeagent1
      --systemproperties HTTP_LISTENER_PORT=8182: instance1

      asadmin> create-instance --user admin --passwordfile password-file
      --cluster amcluster --nodeagent nodeagent2
      --systemproperties HTTP_LISTENER_PORT=8182: instance2

      asadmin> create-instance --user admin --passwordfile password-file
      --cluster amcluster --nodeagent nodeagent3
      --systemproperties HTTP_LISTENER_PORT=8182: instance3
      ```

Note – If you are creating an instance on a remote server, specify the node agent name on the remote server. Also, make sure that the node agent is running on the remote server.

Install and Configure Access Manager

Perform the following steps on all of the servers:

1. Install Access Manager using the Java ES installer with the Configure Later option. Access Manager requires Sun Java System Directory Server. Either install Directory Server before you install Access Manager. Or, use an existing Directory Server.
2. Start all instances of Application Server to verify that they are installed properly.
3. Create an `amsamplesilent` file on the DAS machine (`host-server1`) and set the following attributes:

   SERVER_NAME=host-server1
   SERVER_HOST=$SERVER_NAME.example.com
   SERVER_PORT=8082
   ADMIN_PORT=4849
   DS_HOST=*qa-host-server1.example.com*DS_DIRMGRPASSWD=*password*
   ROOT_SUFFIX="dc=example,dc=com"
   ADMINPASSWD=*password*
   AMLDAPUSERPASSWD=*password*
   COOKIE_DOMAIN=.example.com
   AM_ENC_PWD=""
   NEW_OWNER=root
   NEW_GROUP=other
   PAM_SERVICE_NAME=other
   WEB_CONTAINER=AS8

   AS81_HOST=host-server1.example.com
   AS81_INSTANCE=amcluster
4. Save and deploy the `ampsamplesilent` file. For example:

   amconfig -s amsamplesilent
5. Restart Access Manager and the cluster instance
6. Log in to Access Manager as `amadmin` on the DAS machine and add the additional server instances to the Platform server list. For more information, see "Add Instances to the Platform Server List and Realm/DNS Aliases" on page 7.
7. Copy the `ampsamplesilent` file to `/usr/tmp` directory on both `server1` and `server2`.
8. On the DAS machine, locate the AM_ENC_PWD property in `amconfig.properties` (located in `/etc/opt/SUNWam/config`):

   am.encryption.pwd=RrO0vsw+sg8D1+3ldZ6imu9yhjhyksS2
9. Copy the value of the `AM_ENC_PWD` from the DAS machine and replace the value in the `amsamplesilent` file for both `server1` and `server2`:

   SERVER_NAME=server1
   AM_ENC_PWD=RrO0vsw+sg8D1+3ldZ6imu9yhjhyksS2

SERVER_NAME=server2
AM_ENC_PWD=RrO0vsw+sg8D1+3ldZ6imu9yhjhyksS2

10. Deploy the configuration file on `server1` and `server2`. The applications will produce error messages when attempting to deploy, because the applications are already in the domain. The configuration files need to be created and the command line utilities need to be defined. To do so, run the `amconfig` command for each installed instance. For example:

    ```
    amconfig -s /usr/tmp/ amsamplesilent
    ```

    For more information, see the Access Manager Administration Guide.

    Note – Certain error messages will be sent, but these are expected and can be ignored.

    - Access Manager 7 errors:

```
Directory Server is already loaded with Access Manager DIT.
CLI171 Command deploy failed : Application amserver is already deployed on other targets. Ple
ase use create-application-ref command to create reference to the specified target; requested
 operation cannot be completed
Failed to deploy /amserver
cp: cannot access /var/opt/SUNWappserver/domains/domain1/config/domain.xml
cp: cannot access /var/opt/SUNWappserver/domains/domain1/config/server.policy
CLI167 Could not create the following jvm options. Options exist:
-Djava.protocol.handler.pkgs=com.iplanet.services.com
-DLOG_COMPATMODE=Off
-Ds1is.java.util.logging.config.class=com.sun.identity.log.s1is.LogConfigReader
-Dcom.iplanet.am.serverMode=true
CLI137 Command create-jvm-options failed.
```

11. Repeat these steps for other instances in the cluster.

Add Instances to the Platform Server List and Realm/DNS Aliases

To add Access Manager instances to the Platform Server List and Realm/DNS Aliases, use the Access Manager Admin Console on the first host server (`host-server1`)

1. Log in to the Access Manager Console as `amadmin` on the first host server (`host-server1`).
2. In the Access Manager Console, click `Configuration`, `System Properties`, and then `Platform`.
3. Add each additional instance to the Platform Server List:
   a. Under `Instance Name`, click `New`.
   b. In `New Server Instance`, add the `Server` and `Instance Name`. For example:

      ```
      Server: http://host-server1.example.com:8182
      ```

```
Instance Name: 02
```

c. Click OK to add the instance.

d. After you have added all instances, click Save.

Your Platform Server List will like similar to this list:

```
http://host-server1.example.com:8182|01
http://server1.example.com:8182|02
http://server2.example.com:8182|03
```

In this example, all instances are on the same server. If instances are on remote servers, specify the remote host server names when you add the servers to the list.

If you have instances on remote servers, update the Realm/DNS Aliases (sunOrganizationAliases) with the remote host names:

1. In the Access Manager Console on the first host server (host-server1), click Access Control and then the root (top-level) realm under Realm Name.
2. Under Realm Attributes, add each remote instance to the Realm/DNS Aliases and then click Add. For example:

```
host-server2.example.com
```

3. After you have added all remote instances, click Save.

Your Realm/DNS Aliases will like similar to this list:

```
host-server1.example.com
server1.example.com
server2.example.com
```

Install Web Server as a Load Balancer

Install Web Server on one of the machines and configure it as a load balancer. For information, see the Sun Java System Web Server documentation at http://docs.sun.com/app/docs/coll/1308.1.

Be sure to add the load balancer's site and address to Access Manager's platform list.

Add Listeners to the Clusters for the Load Balancer

Log in to the machine that has Web Server configured as the load balancer plug-in. You will create a listener for each instance of the cluster and the contexts roots for Access manager.

1. Locate the loadbalancer.xml file.
2. Add the listeners to the file. For example:

```
 <instance  name="instance1" enabled="true" disable-timeout-in-minutes="60"
listeners="http://host-server1.expamle.com.com:8182"/>
        <instance  name="instance2" enabled="true" disable-timeout-in-minutes="60"
listeners="http://server1.example.com:8182"/>
        <instance  name="instance3" enabled="true" disable-timeout-in-minutes="60"
listeners="http://server2.exapmle.com:8182"/>

        <web-module context-root="/amserver" enabled="true" disable-timeout-in-minutes="60"
error-url="sun-http-lberror.html" />
        <web-module context-root="/ampassword" enabled="true" disable-timeout-in-minutes="60"
error-url="sun-http-lberror.html" />
        <web-module context-root="/amcommon" enabled="true" disable-timeout-in-minutes="60"
error-url="sun-http-lberror.html" />
```

3. In `loadbalancer.xml`, change `property name` to the following:

   ```
   <property name="response-timeout-in-seconds" value="120"/>
   ```

4. Restart the Web Server.

Restart All Application Server Instances

Restart all Application Server instances using the following commands:

```
asadmin> stop-cluster --user admin --passwordfile password-file amcluster
asadmin> start-cluster --user admin --passwordfile password-file amcluster
```

Accessing Sun Resources Online

The docs.sun.com web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to `http://www.sun.com`:

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research
- Communities (for example, Sun Developer Network)

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this document is 819-6769.

Revision History

Release Date	Description of Changes
May 26, 2006	Review draft.