Running SAS Deployment Wizard on UNIX with a Nonroot User Account and IBM WebSphere Application Server

Below are the two types of user accounts that play an important role in installing, configuring, and administering SAS with IBM WebSphere Application Server.

You need one or more UNIX user accounts for these tasks:

- Install WebSphere Application Server.
- Run SAS Deployment Wizard to install SAS.
- Run SAS Deployment Wizard to configure SAS and WebSphere Application Server.
- Perform subsequent administration of SAS and WebSphere Application Server.

You can use an optional WebSphere Application Server administrative user account for these tasks:

- Log on to the IBM WebSphere Integrated Solutions Console (known as the *administrative console)* if you have enabled WebSphere Application Server administrative security.
- Perform command-line WebSphere Application Server administration.

UNIX user accounts are the most important consideration in this deployment scenario because they are given user and group ownership of any files and directories that are created when SAS and WebSphere Application Server are installed and configured. You need the WebSphere Application Server administrative user account only if you enable WebSphere Application Server administrative security. WebSphere Application Server administrative security does not affect user and group ownership of files and directories when you install and configure SAS or WebSphere Application Server. As a result, the UNIX user account and WebSphere Application Server administrative user account can be different user accounts because they represent different types of security.

When you install WebSphere Application Server 6.1 on UNIX, IBM recommends that you use the root user account. Otherwise, WebSphere Application Server Secure Sockets Layer (SSL) components are not installed. IBM discusses this limitation in "Limitations of nonroot installers." SAS customers who decide to use SSL after installing WebSphere Application Server with a nonroot UNIX user account need to reinstall WebSphere Application Server. As a result of using the root user account for the installation, the root user account owns all WebSphere Application Server files and directories.

An additional step is required on UNIX after the root user account has installed WebSphere Application Server so that a nonroot user account can administer SAS and WebSphere Application Server. This step configures some WebSphere Application Server directories to permit write privilege for a UNIX group. Permitting group write privilege lets a SAS customer run SAS

Deployment Wizard as a nonroot user account and create the WebSphere Application Server profiles for the SAS Web applications. The nonroot user account that runs SAS Deployment Wizard owns the files that SAS Deployment Wizard creates. To preserve user and group ownership of the files, log on to UNIX with the same nonroot user account to perform administration of the WebSphere Application Server profiles that SAS Deployment Wizard created.

You can then enable WebSphere Application Server administrative security. This lets only WebSphere Application Server administrators update the profiles that SAS Deployment Wizard created. It provides WebSphere Application Server administrative security, which is different from the file and directory security that is associated with UNIX user accounts. This step establishes a WebSphere Application Server administrative user account for logging on to the administrative console. This administrative user account can be different from the nonroot user account that owns SAS and the WebSphere Application Server profiles.

Stage 1: Allowing Creation of Nonroot WebSphere Profiles

These instructions are based on the IBM Information Center article "Granting write permission of files and directories to a nonroot user for profile creation." They make it possible for you to use the same nonroot user account to administer SAS and WebSphere Application Server regardless of whether WebSphere Application Server administrative security is enabled. If you enable WebSphere Application Server administrative security by performing Stages 2 and 3, you need to log on to the administrative console and to UNIX to administer WebSphere Application Server. You must complete these instructions after installing WebSphere Application Server 6.1 with the root user account but before running SAS Deployment Wizard.

1. Use UNIX commands to create a group for UNIX user accounts that you can use to administer WebSphere Application Server. Assign user accounts to the group. Follow the instructions in the IBM Information Center article, which provides sample commands. The user account that you use to run SAS Deployment Wizard must be in this group of administrative user accounts because only that user account owns the WebSphere Application Server profile directories that SAS Deployment Wizard creates.
2. Use UNIX commands to grant read and write group permissions to some WebSphere Application Server files and directories. Refer to the IBM Information Center article for specific commands.
3. Below are additional commands that you need. APP_SERVER_ROOT represents the location where WebSphere Application Server is installed.

   a. Add additional group permissions:

      Note: If the directories in the following commands do not exist, then you can create them and perform the `chgrp` and `chmod` commands, or you can skip this step. The SAS Deployment Wizard creates any of these directories that do not exist.

      ```
      chgrp profilers APP_SERVER_ROOT/profiles/
      chmod g+wr APP_SERVER_ROOT/profiles/

      chgrp profilers APP_SERVER_ROOT/properties/
      chmod g+wr APP_SERVER_ROOT/properties/
      ```

```
chgrp profilers APP_SERVER_ROOT/properties/profileRegistry.xml
chmod g+wr APP_SERVER_ROOT/properties/profileRegistry.xml

chgrp profilers APP_SERVER_ROOT/properties/fsdb/
chmod g+wr APP_SERVER_ROOT/properties/fsdb/

chgrp profilers APP_SERVER_ROOT/properties/fsdb/_was_profile_default/
chmod g+wr APP_SERVER_ROOT/properties/fsdb/_was_profile_default/

chgrp profilers APP_SERVER_ROOT/logs/
chmod g+wr APP_SERVER_ROOT/logs/

chgrp profilers APP_SERVER_ROOT/logs/manageprofiles/
chmod g+wr APP_SERVER_ROOT/logs/manageprofiles/
```

b. If the following lock file exists, make sure that it is deleted:

```
rm APP_SERVER_ROOT/properties/profileRegistry.xml_LOCK
```

c. If the following log files exist, make sure that they are deleted:

```
rm –rf APP_SERVER_ROOT/logs/manageprofiles/SASDmgr01/*
rmdir APP_SERVER_ROOT/logs/manageprofiles/SASDmgr01
rm –rf APP_SERVER_ROOT/logs/manageprofiles/SASAppSrv01/*
rmdir APP_SERVER_ROOT/logs/manageprofiles/SASAppSrv01
```

4. Every session where a member of the WebSphere Application Server administrative group is currently logged on must log off before you can continue. Not logging off and on again after setting the above group permissions can result in permission errors occurring during WebSphere Application Server configuration steps in SAS Deployment Wizard that are difficult to diagnose. This happens because the current session permissions are then out of sync with the group permissions that you set.

5. You can now either run SAS Deployment Wizard with a UNIX user account that is a member of the WebSphere Application Server administrative group and not enable WebSphere Application Server administrative security, or you can perform Stage 2 to enable WebSphere Application Server administrative security. In either case, only the user and group of the UNIX user account that is used to run SAS Deployment Wizard will own the WebSphere Application Server profile files and directories that SAS Deployment Wizard created.

Stage 2: Enabling WebSphere Application Server Administrative Security

This optional procedure describes how to enable WebSphere Application Server administrative security in the administrative console and when you run SAS Deployment Wizard. Before you enable WebSphere Application Server administrative security in SAS Deployment Wizard, you must enable it in the administrative console. Log on as root and follow these steps:

1. A WebSphere Application Server profile is required so that you can configure WebSphere Application Server for administrative security before running SAS Deployment Wizard. If WebSphere Application Server was installed without profiles, you can create one by running the following `manageprofiles` command. This example shows the very important naming convention of using the dmgr name to construct both the node and cell names. APP_SERVER_ROOT represents the WebSphere Application Server install location.

   a. Temporarily change the group for the root user account to `profilers` and set the umask so that members of the profilers group can modify files:

   ```
   # newgrp profilers
   # umask 002
   ```

   b. Run the `manageprofiles.sh` command to create the SAS Deployment Manager profile:

   ```
   APP_SERVER_ROOT/bin/manageprofiles.sh –create –profileName SASDmgr01
   -profilePath APP_SERVER_ROOT/profiles/SASDmgr01
   –templatePath APP_SERVER_ROOT/profileTemplates/cell/dmgr
   -nodeName SASDmgr01Node –cellName SASDmgr01Cell
   –defaultPorts -isDefault
   ```

   This command creates a WebSphere Application Server profile named `SASDmgr01`.

2. Use this command to start WebSphere Application Server:

   ```
   APP_SERVER_ROOT/bin/startManager.sh –profileName SASDmgr01
   ```

3. Open a Web browser and log on to the administrative console:

   `http://localhost:9060/ibm/console`

4. Select **Security** > **Secure administration, applications, and infrastructure**.

5. Use the **Security Configuration Wizard** to configure WebSphere Application Server security.

   a. Follow the WebSphere Application Server administrative security documentation.

   b. Deselect the **Enable application security** check box and enable the **Java 2 security** check box.

   c. The WebSphere Application Server administrative user account that you choose is not required to have the same name as the UNIX user account that you configured in Stage 1.

   d. Make sure that the WebSphere Application Server administrative password is at least eight characters long. This length is required; SAS Deployment Wizard does not allow shorter passwords. This is true whether you provide an administrative user account and password that WebSphere Application Server maintains or configure WebSphere Application Server

administrative security to use an operating system user account as your administrative user account.

6. Apply and save the changes you made to the WebSphere Application Server security configuration, and then log off the administrative console.
7. While you are still logged on to UNIX as root, use these commands to stop and start the IBM WebSphere Application Server Network Deployment with Deployment Manager:

```
APP_SERVER_ROOT/bin/stopManager.sh –profileName SASDmgr01
APP_SERVER_ROOT/bin/startManager.sh –profileName SASDmgr01
```

8. Log on to the administrative console. You should be prompted for the WebSphere Application Server administrative user account and password that you provided in the security configuration. This confirms that you configured WebSphere Application Server security as intended.
9. Log off the administrative console and stop WebSphere Application Server.

Stage 3: Running the SAS Deployment Wizard

Follow these steps to run SAS Deployment Wizard:

1. Log on with a nonroot UNIX user account that meets these criteria:
   - The account must be a member of the administrative group that you created in Stage 1.
   - The administrative group is the user account's primary group, or use the `newgrp` command to set the primary administrative group temporarily.

   This is the user account that you will use to run SAS Deployment Wizard and to set user and group ownership of the WebSphere Application Server profiles that SAS Deployment Wizard creates for SAS.
2. SAS Deployment Wizard provides a series of prompts for configuration information. These pages are related to your WebSphere Application Server configuration.
   a. On the **Web Application Server: Administrative Security** page, select the **Administrative Security is Enabled** check box.
   b. On the **External Account: Web Application Server Administrator** page, provide the WebSphere Application Server administrative user account and password that you configured in Stage 2.

Summary

After completing Stage 1 and successfully running SAS Deployment Wizard, you should be able to administer the SAS applications that are deployed on WebSphere by logging on to UNIX with the same nonroot user account that was used to run SAS Deployment Wizard. Because Stage 1 steps did not enable WebSphere administrative security, your administrative console sessions are not password-protected. However, if you performed Stages 1 through 3, you have configured a WebSphere administrative user account and password and also a nonroot UNIX user account for administering SAS and WebSphere.

Recommended Reading

These URLs are current as of December 2008.

IBM Corporation, 2007: "Granting writer permission of files and directories to a nonroot user for profile creation." IBM Information Center. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tpro_nonrootpro.html.

IBM Corporation, 2007: "Limitations of nonroot installers." IBM Information Center. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cins_nonroot.html.