

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

The SAS 9.2 SAS Deployment Wizard offers a feature to automatically configure the SAS Web applications on your Web application server. For deployments that use IBM WebSphere Application Server, the SAS Deployment Wizard must be able to create and modify files in the WebSphere Application Server directories. On UNIX operating environments, IBM recommends installing WebSphere Application Server with the root user account. SAS recommends running the SAS Deployment Wizard with a nonroot installer account. Unless some WebSphere Application Server directories are modified to permit write privilege, there is no way to take advantage of the feature that automatically configures the Web application server. This document describes the changes needed so that you can install WebSphere Application Server as root, install SAS with a nonroot user account, and still take advantage of the feature that automatically configures the Web application server.

You need one or more UNIX user accounts to perform the following tasks:

- Install WebSphere Application Server. IBM recommends using `root`.
- Run SAS Deployment Wizard to install SAS, configure SAS, and configure WebSphere Application Server profiles for the SAS Web applications. SAS recommends creating and using an account named `sas`.
- Perform subsequent administration of SAS and WebSphere Application Server.

The user accounts that are used to perform these tasks are important because they are given user and group ownership of any files and directories that are created. IBM recommends that you use the `root` user account for installing WebSphere Application Server. Otherwise, the 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.

However, the `root` user account is not a good choice for day-to-day administration. An additional step is required on UNIX after the `root` user account has installed WebSphere Application Server so that a nonroot user account can install SAS, configure SAS, and administer both 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.

Stage 1: Allowing Creation of Nonroot WebSphere Profiles

Once you have installed WebSphere Application Server 6.1, you MUST go to the IBM Information Center article “Granting write permission of files and directories to a nonroot user for profile creation” to perform 8 steps required to grant write permission of files and directories to a non-root user. They make it possible for you to use the same nonroot user account to administer SAS and WebSphere Application Server. You MUST complete the following instructions after installing the root user account, but before running the SAS Deployment Wizard.

1. Use UNIX commands to create a group for UNIX user accounts for WebSphere Application Server administration. 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 the SAS Deployment Wizard must be in this group of administrative user accounts because the user must be able to create WebSphere Application Server profile directories.

The IBM Information Center article leaves the WebSphere Application Server installation in a state that does not permit a nonroot user ID from creating profiles in the profiles directory.

2. When the SAS Deployment Wizard is used to automatically configure WebSphere Application Server, the SAS Deployment Wizard creates profiles for a deployment manager and an application server. Below are additional commands that you need to permit write privilege for a user group. APP_SERVER_ROOT represents the location where WebSphere Application Server is installed.

- a. If the profiles directory does not exist, create it:

```
mkdir APP_SERVER_ROOT/profiles
```

- b. Permit group write on the profiles directory:

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

- c. If profiles exist that you want the SAS Deployment Wizard to reconfigure, then permit write privilege to the group:

```
chgrp -R profilers APP_SERVER_ROOT/profiles/profileName  
chmod -R g+rw APP_SERVER_ROOT/profiles/profileName
```

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

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

3. Every session where a member of the WebSphere Application Server administrative group is currently logged on must log off before you can continue. If users do not log off and on again after setting the previous group permissions, the SAS Deployment Wizard may fail to create files or directories. This happens because the current session permissions are then out of sync with the group permissions that you set. The SAS Deployment Wizard errors are difficult to diagnose and resolve.

4. Log on with the SAS installer account and create a test profile and then remove it to confirm that the SAS installer account has write privilege:

- a. Create a profile named testProfile:

```
APP_SERVER_ROOT/bin/manageprofiles.sh -create \  
-profileName testProfile \  
-profilePath APP_SERVER_ROOT/profiles/testProfile \  
-templatePath APP_SERVER_ROOT/profileTemplates/dmgr \  
-cellName testProfile01Cell \  
-nodeName testProfile01Node \  
-isDefault
```

This step confirms that the SAS installer account has write privilege to the WebSphere Application Server directories and can create profiles.

- b. Delete the profile:

```
APP_SERVER_ROOT/bin/manageprofiles.sh -delete \  
-profileName testProfile
```

- c. Remove the test profile directory:

```
rm -rf APP_SERVER_ROOT/profiles/testProfile
```

If any of these commands fail, then review the IBM Information Center article that is identified at the beginning of this stage. These commands must succeed in order to use the SAS Deployment Wizard to automatically configure WebSphere Application Server.

Stage 2: Running the SAS Deployment Wizard

The SAS Deployment Wizard includes an optional feature to automatically configure WebSphere Application Server for the SAS Web applications. SAS recommends using this feature because it eliminates the tedious and error-prone process of configuring resources such as a Java mail session, a JDBC data source, Java Messaging System queues, and JAAS login modules.

If your site has configured WebSphere Application Server to use administrative security, SAS recommends disabling it while the SAS Deployment Wizard is run. One of the actions performed by the SAS Deployment Wizard during the automatic configuration of WebSphere Application Server is to federate the node to the same cell as the deployment manager. If the deployment manager is running on a remote machine and has enabled administrative security, then the command to perform this action fails.

For sites that use administrative security and cannot disable it while the SAS Deployment Manager runs, the following table shows that a manual configuration of WebSphere Application Server and manual deployment of the SAS Web applications is the only choice for such sites.

	WebSphere Administrative Security	
	Enabled	Disabled
SAS Deployment Wizard run on same machine as dmgr	Automatic or manual configuration	Automatic or manual configuration
SAS Deployment Wizard run on different machine as dmgr	Manual configuration only	Automatic or manual configuration

Follow these steps to run the SAS Deployment Wizard:

1. Log on with the SAS installer user ID. This user ID must meet the following criteria:
 - a nonroot UNIX user account
 - The account must be a member of the administrative group that you created in Stage 1.

This is the user ID to use for running the SAS Deployment Wizard. This user ID will have user and group ownership of the WebSphere Application Server profiles that the SAS Deployment Wizard creates for SAS.
2. Run the SAS Deployment Wizard.

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.

SAS and all other SAS Institute product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. Other brand and product names are registered trademarks or trademarks of their respective companies.

® indicates USA registration.

Copyright © 2009 SAS Institute Inc., Cary, NC, USA. All rights reserved.