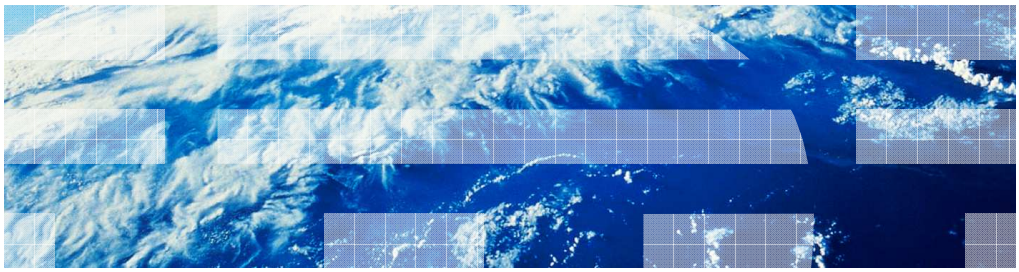
IBM Tivoli System Automation for Multiplatforms

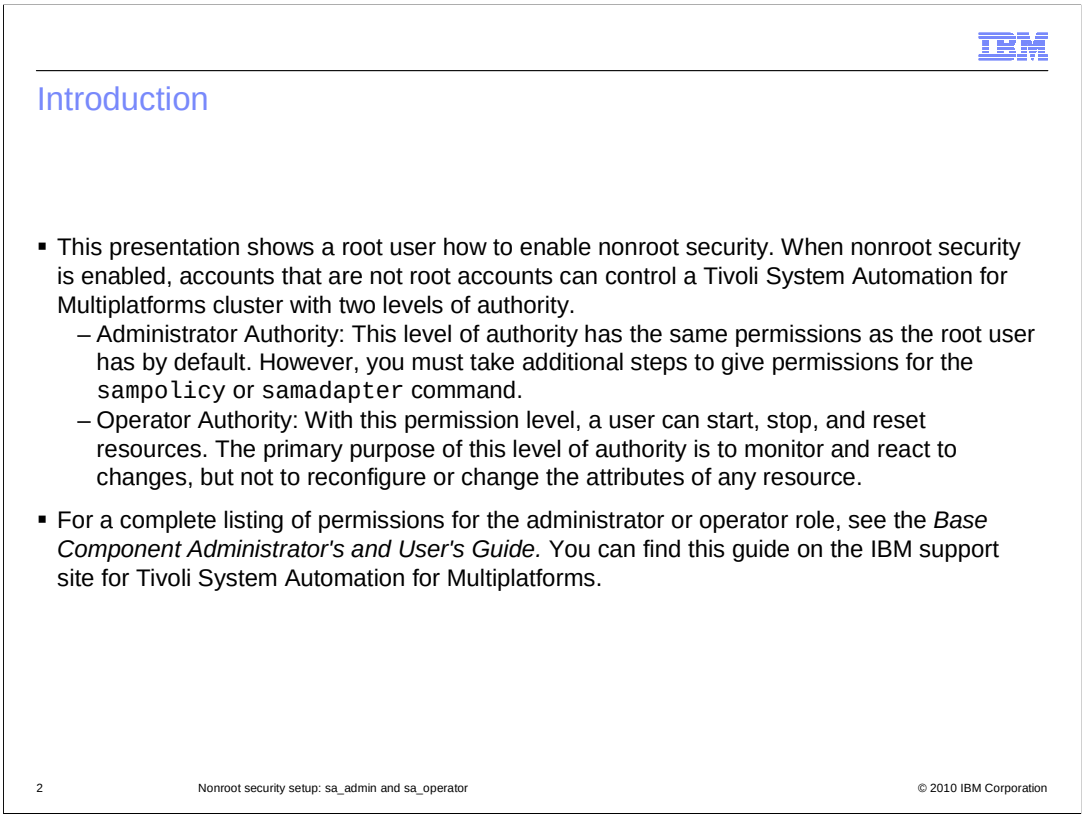
Nonroot security setup: sa_admin and sa_operator



Tivoli software

This presentation focuses on setting up nonroot security so that users and administrators can manage a Tivoli® System Automation for Multiplatforms cluster without needing root access.

In this presentation, you learn how to set up security for the cluster. Two separate levels of permissions are set up, one for the operator role and one for the sysadmin role.



This presentation shows a root user how to enable nonroot security. When nonroot security is enabled, accounts that are not root accounts can control a Tivoli System Automation for Multiplatforms cluster with two levels of authority. Depending on what you require for your users or administrators, each of the levels can be assigned to multiple user accounts, if required.

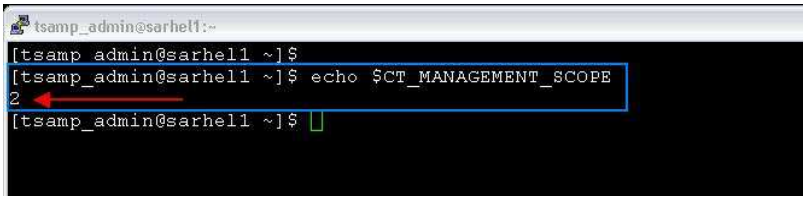
The two authority levels are Administrator and Operator. The administrator authority level is for anyone who is responsible for changing the cluster configuration. System Administrators and Database Administrators have this authority.

The Operator Authority level is for someone who monitors and reports situations or issues that might occur in your cluster. Primarily, this level is for any end user who is responsible for monitoring a network or server cluster.

For a complete listing of the capabilities of the administrator or operator role, see the Base Component Administrators and Users Guide. You can find this guide on the IBM Support site for Tivoli System Automation for Multiplatforms.

Initial steps

- The following process requires root access to all the nodes in the cluster.
- The first step in setting up either admin or operator permissions for a user account is to create the accounts and the group that they will belong to. In this example, you are using two accounts, tsamp_admin and tsamp_operator. They will be added to a user group called tsamp_group.
- For proper cluster operation while logged into any account, you must ensure that the system variable CT_MANAGEMENT_SCOPE is set to a value of 2. Export this variable using a profile for any user account that needs to issue any TSAMP or RSCT commands. Verify that the variable is exported properly, as demonstrated in the following image.



3 Nonroot security setup: sa_admin and sa_operator

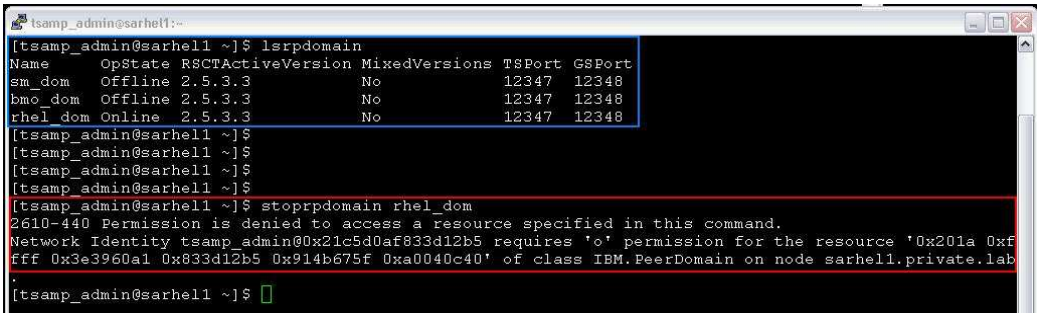
The following process requires root access to all the nodes in the cluster. This process does not interrupt a running cluster, so it is safe to perform this process while an application is online in the cluster.

The first step in setting up either admin or operator permissions for a user account is to create the account or accounts and the group that they will belong to. In this example, you are using two accounts, tsamp_admin and tsamp_operator. They will be added to a user group called tsamp_group. Consult the documentation or a System Administrator to determine how to create the users and the group and add the users to the group.

For proper cluster operation while logged into any account, you must ensure that the system variable CT_MANAGEMENT_SCOPE is set to a value of 2. You should export this variable by using a profile for any user account that needs to issue any TSAMP or RSCT commands. Verify that the variable is exported properly, as shown in the image. If you do not have this variable exported properly, you might experience error messages. You might be using commands that are attempting to pull information from the node or nodes that you are not currently issuing the command from.

Example of permission denied

- In the screen capture, the blue outline shows a command that executes and returns the typical or correct response for that command.
- The red outline shows a command and the error returned from it. This error occurs when a user without the correct permissions tries to run a protected command.



4 Nonroot security setup: sa_admin and sa_operator

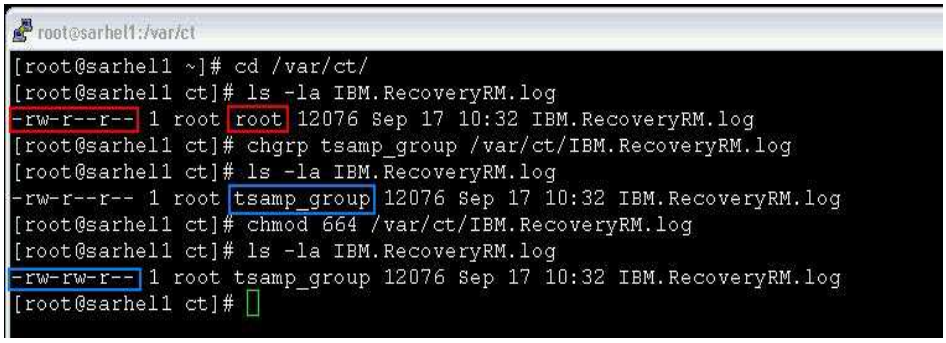
On this slide, you see examples of failed and successful commands that demonstrate the use of this procedure. Many organizations require this type of configuration because they allow very limited access to the root user on the company's production environment.

In the screen capture, the blue outline shows a command that has completed successfully because the permissions are set correctly.

The red outline shows a command and the error returned from it when a user without the correct permissions attempts a protected command.

IBM.RecoveryRM.log ownership and permissions

- Change the group ownership and permissions of the IBM.RecoveryRM log file.
- The name of the file is **/var/ct/IBM.RecoveryRM.log**. You must change the group ownership to the group created earlier. Set the permissions to **664**. The group that you created earlier, tsamp_group, is shown in the following image.



5 Nonroot security setup: sa_admin and sa_operator

In the following process, you are enabling nonroot security on your cluster nodes. The process outlines the steps required to enable the nonroot security configuration. If you encounter anything that you do not understand, consult your local Systems Administrator.

The first step is to change the group ownership and permissions of the IBM.RecoveryRM log file. This file is located in the **/var/ct** directory. If the file is not there, you can create it with the **touch** command. After you create it, you must then change the group ownership and the permissions on it so that the new accounts can write to it.

To change the group ownership of the file, use the **chgrp** command. This command changes the ownership to the tsamp_group that you created earlier.

To change the permissions of the file, use the **chmod** command and change the permissions to **664**.

Map users to permissions: ctsec_map.global

- Map the users to the permissions they are to have in the cluster. Map the users in the **/var/ct/cfg/ctsec_map.global** file.
- If that file does not exist, you can copy it from its default location, **/usr/sbin/rsct/cfg** to a new location, **/var/ct/cfg/ctsec_map.global**. Then, you can edit the file in the new location. Do not edit this file in the default location.

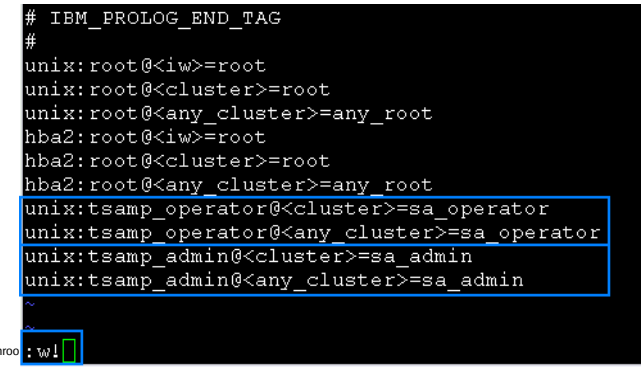
When editing this file, ensure that you are careful with any changes you make. Tivoli System Automation for Multiplatforms support strongly recommends that you back up this file because there are other Tivoli products that use it.

Now, map the users to the permissions they are to have in the cluster. Perform this mapping in the **/var/ct/cfg/ctsec_map.global** file.

If that file does not exist, you can copy it from its default location **/usr/sbin/rsct/cfg** to a new location, **/var/ct/cfg/ctsec_map.global**. Edit this file in the new location, but do not edit the file in the default location.

Map users to permissions in ctsec_map.global

- Add the lines that are outlined in blue to map the user `tsamp_admin` to the Global User ID `sa_admin` and to map the user `tsamp_operator` to the global user `sa_operator`. Only add those lines for the user permissions that are required for your implementation.
- Ensure that when you leave your editor, you save the file. In the screen capture, the file was set as read-only. Forcing the save was the only option.
- Make these changes on all nodes in the cluster.



Add the lines that are outlined in blue to map the user tsamp_admin to the Global User ID sa_admin and to map the user tsamp_operator to the global user sa_operator. Only add those lines for the user permissions that are required for your implementation.

Ensure that when you leave your editor, you save the file. In the screen capture, the file was set as read-only. Forcing the save was the only option.

It is critical that you do not alter any other lines in this file. Doing so can cause cluster issues that do not allow your application to continue to run or fail over. As you can see in the image, the areas bordered in blue are in a very specific order of input for the data into this file. Input the lines exactly as shown. Any variation from this order results in this process failing, and no additional permissions are mapped to the user IDs that need those permissions.

These changes must be done on all nodes in the cluster. In the image, you see sets of lines to add for both the Operator and Administrator roles. For your specific cluster configuration, you might need one or both sets of lines. If you do not understand this step, contact your local system administrator.

Define the global user ID permissions in ctrmc.acls

- The cluster permissions of the Global User ID must be set in the **/var/ct/cfg/ctrmc.acls** file.
- You must comment out the `LOCALHOST` line in the default stanza.
- Then, add the lines shown in the screen capture for the `sa_admin` and `sa_operator` roles. These lines define their permissions in the cluster. Only add the lines for the roles you want to define, depending on your cluster configuration.
- Make these changes on all nodes in the cluster.

```
DEFAULT
    root@LOCALHOST      *       rw
#       LOCALHOST       *       r
        none:root       *       rw              // give root on any node access to all - preprpnode
    none:sa_admin       *       rw              // append this row for sa_admin
 none:sa_operator       *       rso             // append this row for sa_operator
```

8 Nonroot security setup: sa_admin and sa_operator

Back up this file so that any mistakes can be easily backed out by restoring the backup file. There is a clean version of this file in **/usr/sbin/rsct/cfg/**.

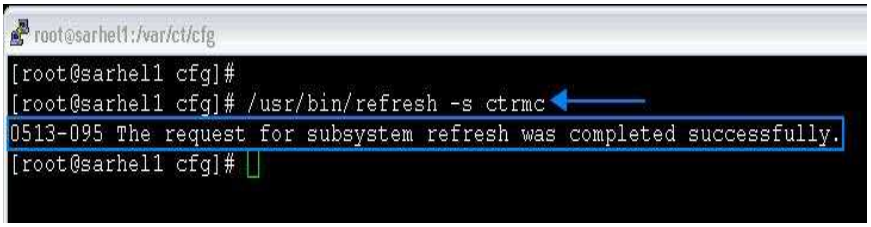
You must set the cluster permissions of the Global User ID in the **/var/ct/cfg/ctrmc.acls** file. Ensure that you do not change anything else in this file because it is used by other applications for security permissions.

You must comment out the LOCALHOST line in the default stanza. To comment out the line, precede any other text in the line with the pound (#) symbol. Then, add the lines shown for the **sa_admin** and **sa_operator** roles that define their permissions in the cluster.

Only add the lines for the roles that you want to define, depending on your cluster configuration. You must make these changes on all nodes in the cluster.

Restart ctrmc subsystem

- The last step is to restart the ctrmc subsystem to make the changes active.



The last step to complete this process is to restart the CTRMC subsystem. You can perform this step while applications are online without causing any interruption to their service. The command is **/usr/bin/refresh -s ctrmc** and the correct response is shown in the screen capture.

You have now completed this presentation.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_non-root-security-setup.ppt

This module is also available in PDF format at: ../non-root-security-setup.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.