

View Roles and Rules

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014, 2015. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Procedure	3



View Roles and Rules



1 Introduction

This document describes how to view the roles retrieved from the Lightweight Directory Access Protocol (LDAP) server, the rules delivered by the system, and custom rules.

The understanding of the roles and rules is a prerequisite for solving any authorization issues.

1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

1.1.1 Conditions

The following conditions must apply:

- The user has the System Security Administrator role.
- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



View Roles and Rules



2 Procedure

To view the roles and rules:

1. Navigate to the `LocalAuthorizationMethod` Managed Object (MO), for example:

```
>dn ManagedElement=NODE06ST,SystemFunctions=1,SecM=1,UserManagement=1,LocalAuthorizationMethod=1
```

2. View the rules for a specific role, for example, the System Administrator role:

```
(LocalAuthorizationMethod=1)>show -r -v Role=SystemAdministrator
```

The following example output shows the permissions for the System Administrator role. The rule named `FaultManagement_1` defines read, write, and execute permissions for the Fault Management MO, its attributes, actions, and its child MOs. A rule MO exists for each predefined rule in the system. Each rule MO is identified by the value of attribute `ruleId`.



```
Role=SystemAdministrator
  roleId="SystemAdministrator"
  roleName="SystemAdministrator" <read-only>
  userLabel="System Administrator Role"
  Rule=FaultManagement_1
    permission=RWX <read-only>
    ruleData="ManagedElement,SystemFunctions,Fm,*" <read-only>
    ruleId="FaultManagement_1"
    ruleName="FaultManagement_1" <read-only>
    userLabel="RWX Rule for FM"
  Rule=PerformanceManagement_1
    permission=RWX <read-only>
    ruleData="ManagedElement,SystemFunctions,Pm,*" <read-only>
    ruleId="PerformanceManagement_1"
    ruleName="PerformanceManagement_1" <read-only>
    userLabel="RWX Rule for PM"
  Rule=SoftwareInventory_1
    permission=RW <read-only>
    ruleData="ManagedElement,SystemFunctions,SwInventory,*" <read-only>
    ruleId="SoftwareInventory_1"
    ruleName="SoftwareInventory_1" <read-only>
    userLabel="RW Rule for SwIM"
  Rule=SoftwareManagement_1
    permission=RWX <read-only>
    ruleData="ManagedElement,SystemFunctions,SwM,*" <read-only>
    ruleId="SoftwareManagement_1"
    ruleName="SoftwareManagement_1" <read-only>
    userLabel="RWX Rule for SwM"
  Rule=SystemManagement_1
    permission=RWX <read-only>
    ruleData="ManagedElement,SystemFunctions,SysM,*" <read-only>
    ruleId="SystemManagement_1"
    ruleName="SystemManagement_1" <read-only>
    userLabel="RWX Rule for SysM"
  Rule=Top_1
    permission=RWX <read-only>
    ruleData="ManagedElement" <read-only>
    ruleId="Top_1"
    ruleName="Top_1" <read-only>
    userLabel="RWX Rule for ME"
  Rule=Top_2
    permission=RWX <read-only>
    ruleData="ManagedElement,SystemFunctions" <read-only>
    ruleId="Top_2"
    ruleName="Top_2" <read-only>
    userLabel="RWX Rule for System Functions"
  Rule=Top_3
    permission=RWX <read-only>
    ruleData="ManagedElement,Transport" <read-only>
    ruleId="Top_3"
    ruleName="Top_3" <read-only>
    userLabel="RWX Rule for Transport"
[...]
```