InterW orks
2001

Understanding ServiceControl Manager Role-Based Authorizations

Donald Suit
Hewlett Packard
3404 Harmony Road, MS 99
Fort Collins, CO 80528-9599
(970) 898-0327
(970) 898-2151 fax
donald_suit@hp.com

InterWorks
2001

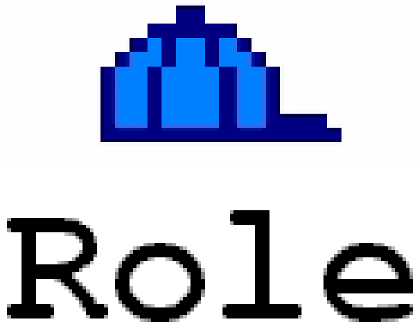
Introduction

- Multi-System management traditionally accomplished with remote shell
- Alternatives
  - ACL
  - sudo, others
- SCM provides
  - Roles
  - Partitioning access to nodes and node groups

Service Control Manager Solution

- Roles
  - Describes an area of responsibility, i.e. database admin, web admin, etc.
  - Associated with a set of SCM tools, i.e. a toolkit
- Role-based Authorizations
  - User, role, node or node group triplet
  - Identifies the targets (node or node group) on which an SCM user may run a specified tool set (role)

Role Attributes



- Name
- Description
- Enablement

Semantics

- Assign common role for similar responsibilities
  - Backup Operator Role
  - All tools that accomplish backup and restoration functions assigned the backup ops role.
- The role links the user with the tool.
- Fixed set of sixteen (16) roles available, currently
  - Can be renamed to meet customer needs -- Exception “Master Role”
  - Cannot be deleted
  - Cannot add additional

SCM Authorizations

- Specify access of SCM user to execute set of SCM tools on set of SCM nodes
- Set of SCM tools specified by using SCM roles
- Set of SCM nodes specified by either indicating an individual node or by indicating an SCM node group

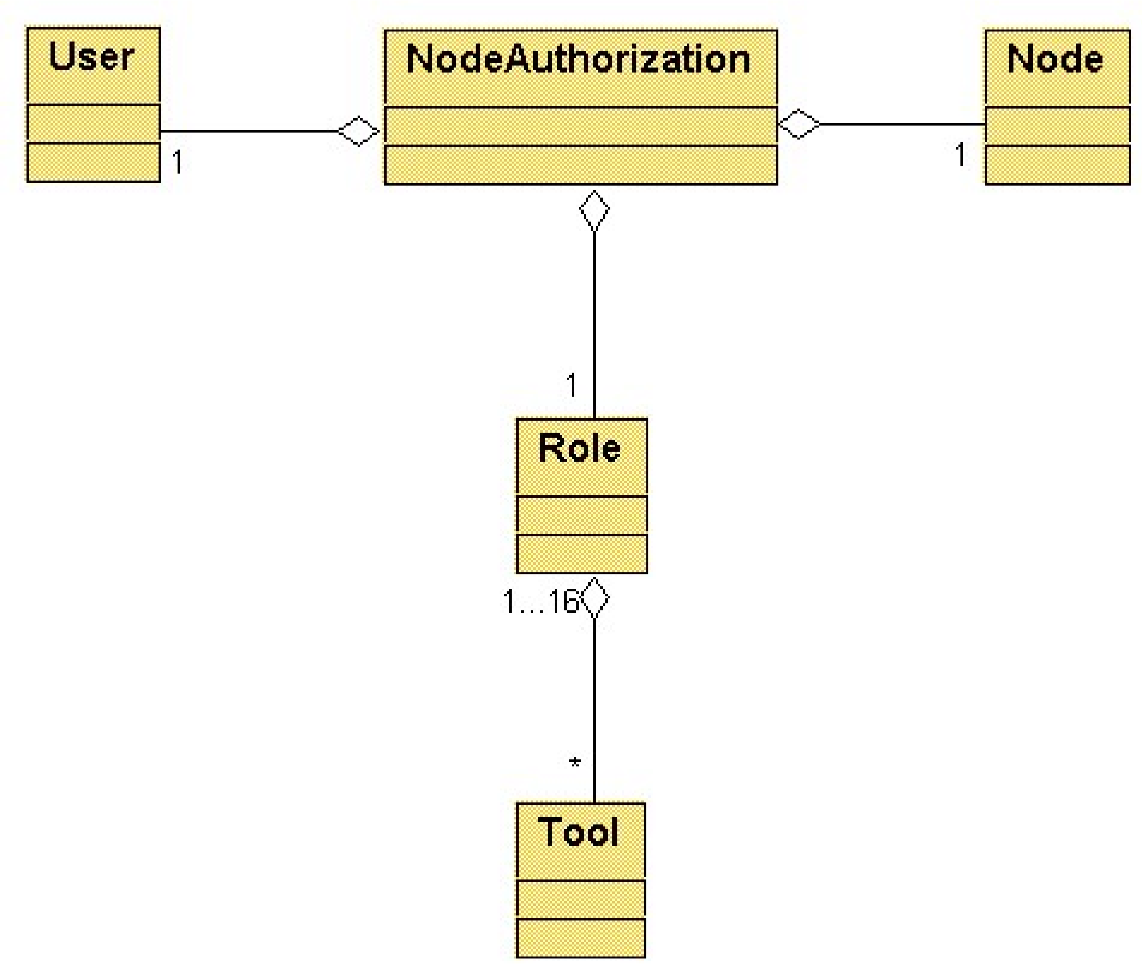
Node Authorization Triplets

- UserName
- RoleName
- NodeName

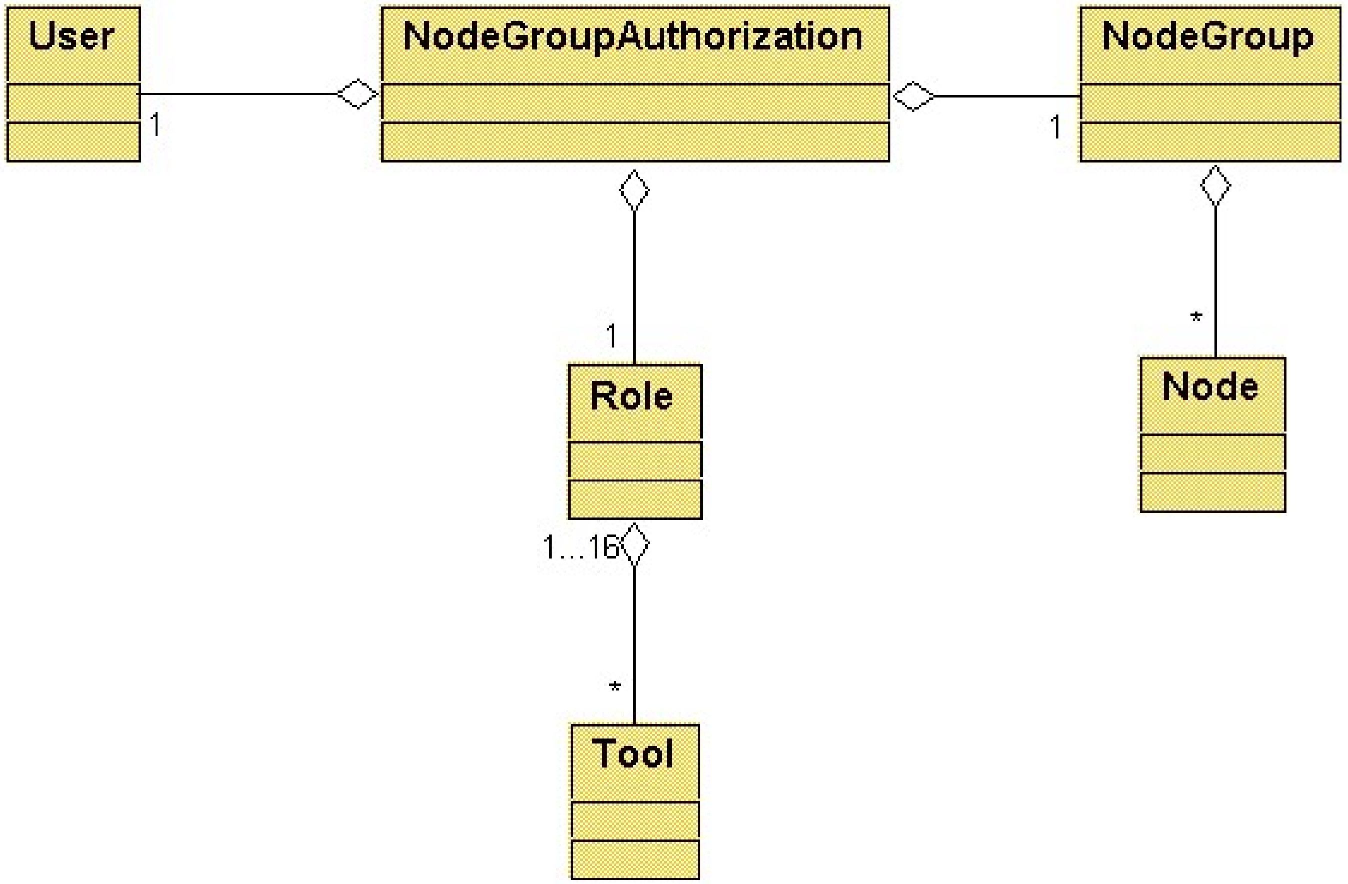
Node Group Authorization Triplet

- User Name
- Role Name
- Node Group Name

Node Authorization (UML)



Node Group Authorization (UML)



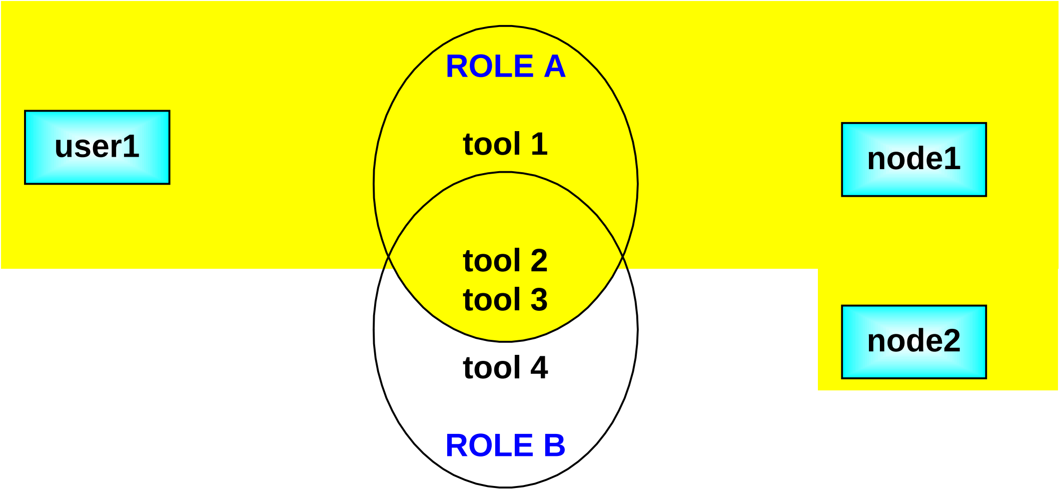
Tools and Roles

Authorizations:

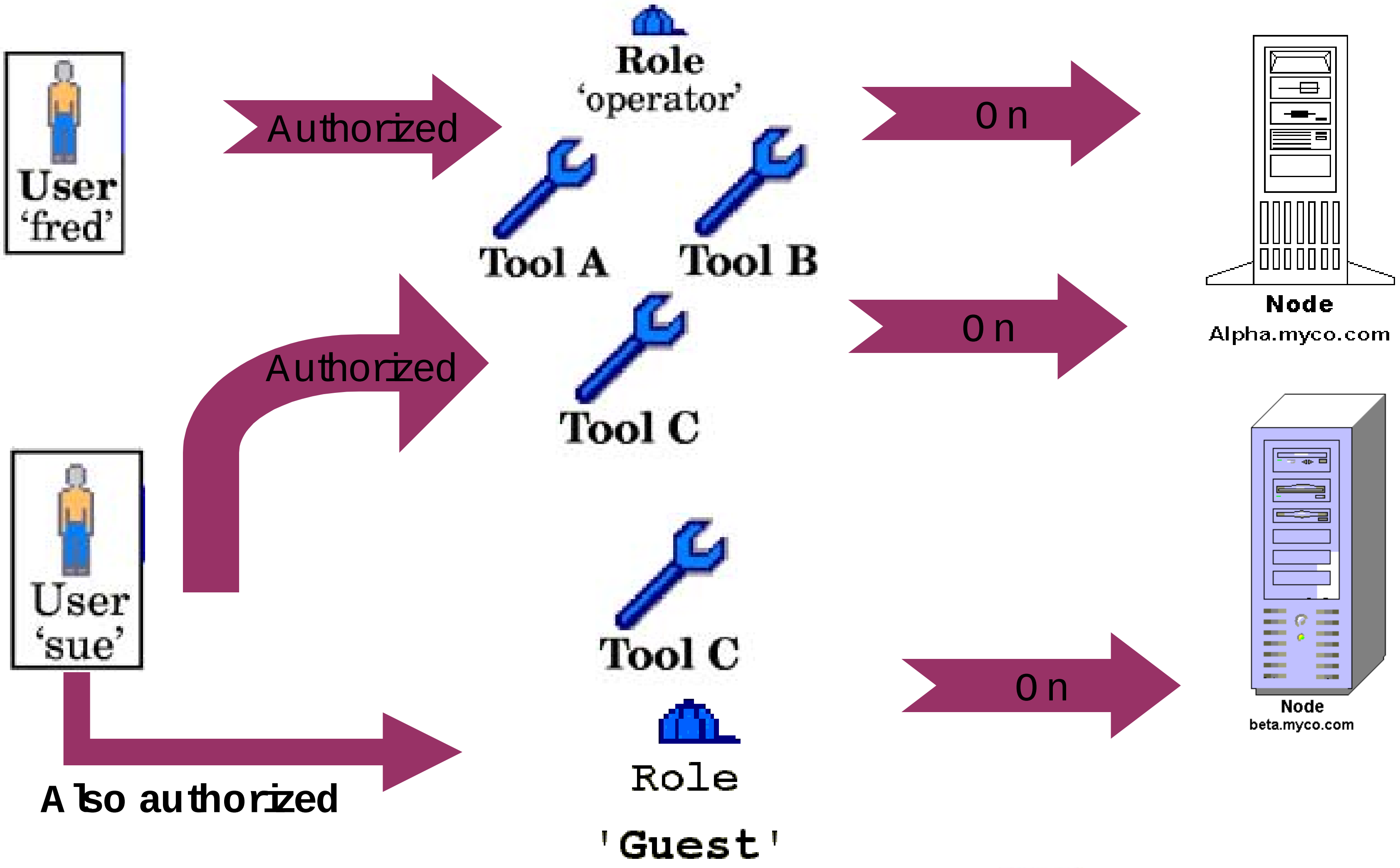
user1 + ROLE A + node1
user1 + ROLE A + node2

Means:

user1 can run tools 1,2,3 on nodes 1 and 2



Role-Based Authorizations



Authorized

On

Authorized

On

On

Also authorized

Role

'Guest'

Master Role

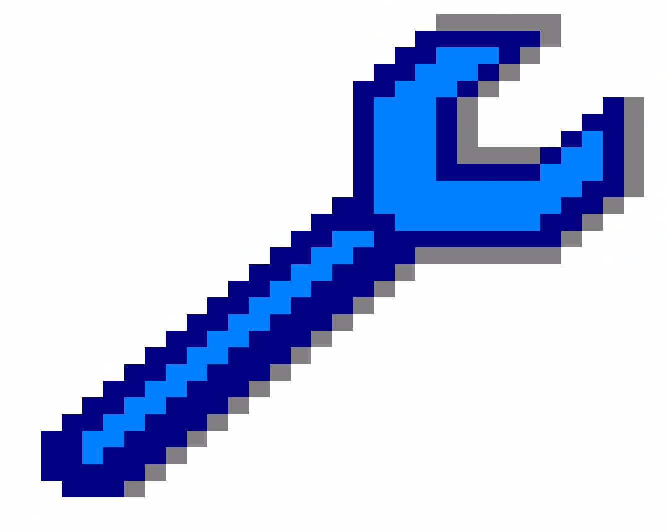
- Assigned to all tools
- Cannot be disabled
- Cannot be removed from any tools
- Cannot be renamed
- Suggestion: Treat this role as the most privileged role

Semantics

- Tools can fail to execute for a number of reasons:
  - The user has no authorizations
  - The user has no authorizations for the target nodes
  - The user has no authorizations for any of the tool's associated roles
  - The tool's roles are disabled for the tool
  - The tool's roles are globally disabled
  - The user specified a node group as the target and either was not authorized for the node group or was not authorized for one or more of the nodes in the node group.
- Tool execution failure reported to the administrator and logged

InterWorks
2001

Authorization Failure (1)



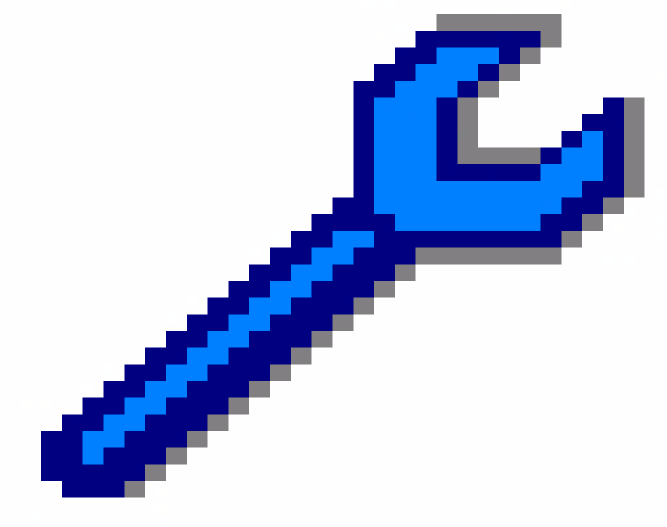
"ToolA"

"MasterRole"
Operator
guest

- No Authorizations
- User – 'hasii'

- -:-:-

Authorization Failure (2)



“ToolA”

“MasterRole”

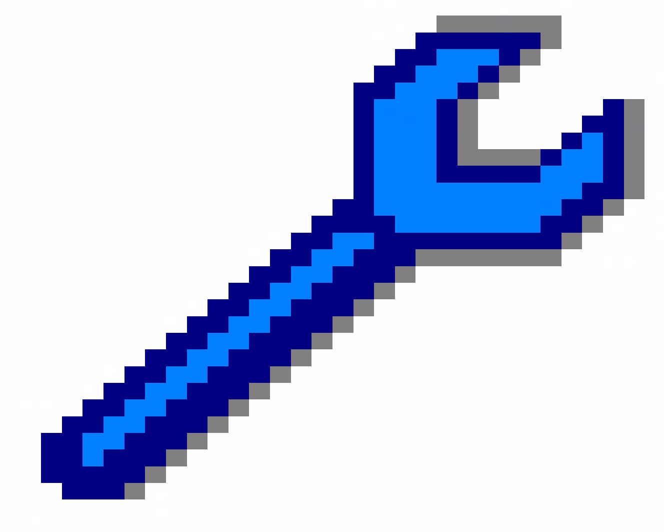
Operator

guest

- The user has no authorizations for the target nodes

- User – ‘hasii’
- hasii:dbadm:Node1
- hasii:guest:Node1
- Cannot run on Node2

Authorization Failure (3)



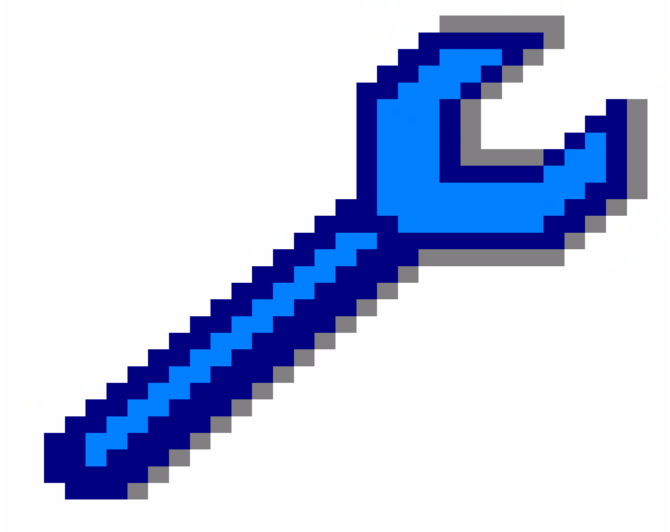
“ToolA”

“MasterRole”
Operator
guest

- No authorizations for any of the tool’s associated roles

- User – ‘hasii’
- hasii:dbadm :Node1
- hasii:lvmadm in:Node1

Authorization Failure (4)



"ToolA"

"MasterRole"

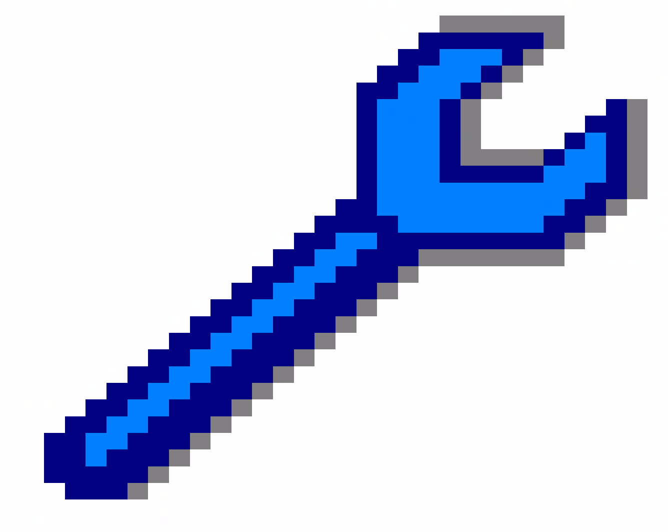
Operator

guest

- Tool's roles are disabled for the tool

- User – 'hasii'
- hasii:dbadm:Node1
- hasii:guest:Node1

Authorization Failure (5)



"ToolA"

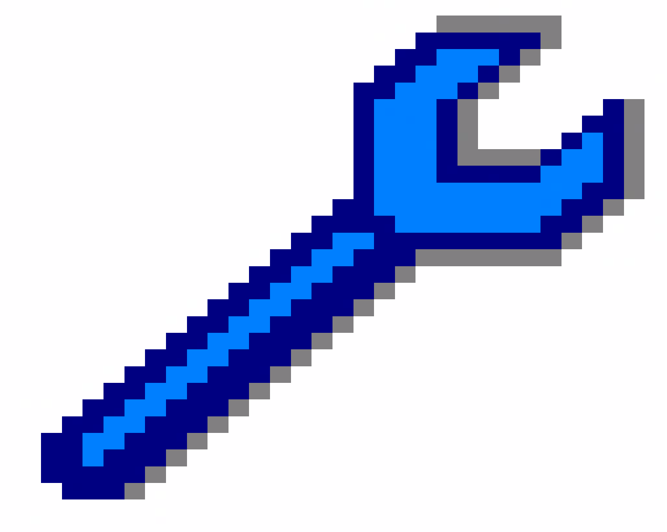
"MasterRole"
Operator
guest

- A role is globally disabled

- User – 'hasii'
- hasii:dbadm:Node1
- hasii:guest:Node1

- mxrole –m guest –e f

Authorization Failure (6)



"ToolA"

"MasterRole"
Operator
guest

- The user specified a node group as the target and either was not authorized for the node group or was not authorized for one or more of the nodes in the node group.

- User – 'hasii'
- Group1 (Node1, Node2)
- hasii:dbadm:Node3
- hasii:guest:Node3

Security Policy Implementation

- Install Agent software on nodes (requires "root")
- Add nodes (CLI/GUI)
- Add node administrators (CLI/GUI)
- Add environment specific tools
- Configure meaningful roles
- Configure authorization triplets

Simple Example

- HP Servers
  - Business processes (payroll, billing, logistics, etc)
  - E-commerce (web servers)
  - Database applications for E-commerce
- Operation/Organizational Roles
  - Backup/Restore
  - HP Customer/Field Support

Configure Roles (1)

```
$ mxrole


  Master Role
  operator
  dbadmin
  webadmin
  lvmadmin
  role6
  … … .
```

Configure Roles (2)

- Trusted User determines he/she needs:

```
operator
ERP admin
backup ops
webadmin
dbadmin
HP CE
```

Configure Roles (3)

```
$ mxrole –m role6       –N “ERP Admin”
$ mxrole –m “ERP Admin” –d “ERP administrators”

$ mxrole –m lvmadmin     –N “backup ops”
$ mxrole –m “backup ops” –d “Role for backup/restore”

$ mxrole –m webadmin –d “Role for web server admin”


$ mxrole –m dbadmin  –d “Role for database admin”


$ mxrole –m role7   –N “HP CE”
$ mxrole –m “HP CE” –d “HP field engineer”
```

Configure Node Authorizations – General Form

- $ mxauth –a –u ***U*** –R ***role-name*** –n **‘*’**

Configure Authorizations Compact Form

- **Problem:** Lots of authorizations
- *mxauth* creates or delete triplets one at a time
- **Solution:**
  - `mxauth –a –f /var/tmp/erp_auths`
- Assume nodes are named $\text{erp}_1 \ldots \text{erp}_N$
- Assume users are named $U_1 \ldots U_N$

CompactForm Format

username:rolename[:n]:nodename

username:rolename:g:groupname

U_1:ERPAdmin:n:erp$_1$

U_1:ERPAdmin:n:e$_2$

...

...

...

U_N:ERPAdmin:n:erp$_N$

Configure Node Group Authorizations – General Form

- $ mxauth –a –u ***U*** –R ***role-name*** –g ***‘*’***
- $ mxauth –a –u ***U*** –R ***role-name*** –g ***group-name***
- Provide more robust authorizations
- Add/remove nodes to node group using `mxngroup` and SCM authorizes based on node group membership

Summary

- Enforce easily configurable and flexible security policy
- Control of tool execution on per node or per node group basis
- Ability to track changes via audit trail