Secure, Role–Based Management of HP–UX Date Centers Using ServiceControl Manager

DONALD SUIT
HEWLET PACKARD
3404 EAST HARMONY ROAD, MS 99
FORT COLLINS, CO 80528-9599
(970) 898-0327
(970) 898-2151 FAX
donald_suit@hp.com

JANUARY 12, 2001

Acknowledgements

The author wishes to acknowledge the original author of most of this paper, Richard Harrah. Richard submitted the original paper as part of the proceedings of InterWorks 2000.

Biographical Sketch

Donald Suit is a software engineer at Hewlett-Packard's Manageability Solutions Lab in Fort Collins, Colorado. He has 20 years of software development experience developing various commercial and government applications. He has a B.S. degree in computer science from the University of Maryland and an M.S. degree in computer science from Johns Hopkins University.

Mailing address:

Donald Suit
3404 East Harmony Road, MS 99
Fort Collins, CO 80528-9599

E-mail address:

donald_suit@hp.com

Abstract

Administrators of Internet data centers have traditionally grappled with their inability to an alternative to “root or nothing” access to system and application administrators. This use model is inflexible and dated.

ServiceControl Manager enables effective administration of the HP-UX data center with secure, role-based administration of multiple HP-UX servers. The ServiceControl Manager grants administrators access to varying responsibilities on differing machines by virtue of their assigned roles.

1 Introduction

Typically, system administrators manage multiple HP-UX servers from a central management console with the remote shell (`r*`) commands. However, concerns around the inherent security problems of the `r*` commands are becoming commonplace. Subsequently, IT professionals require a safer method of centrally managing servers by securely executing a script or application on a remote machine.

Methods to allow administrators to execute specific commands on a per-machine basis are available. These methods include Access Control Lists, `sudo` and others. Unfortunately, these tools can be very cumbersome to manage on one machine, let alone a network of several machines with varying administrators and differing commands.

ServiceControl Manager provides a secure and robust infrastructure to manage multiple HP-UX servers from a central location. This allows one administrator to manage more machines, from a single point – the Central Management Server – where she may configure and enforce a security policy.

One of the key benefits of ServiceControl Manager is the ability for a ServiceControl Manager Trusted User to partition the Internet data center into groups of machines and groups of users that share an operation or function that is important in the data center – a *rol*e. The ServiceControl Manager also assigns roles to tools, and users are authorized logins on certain managed nodes in the data center. The result is that the security policy defines the tools administrators can execute on a managed node.

This paper is not a description of all aspects of ServiceControl Manager, and it is assumed that the reader is familiar with ServiceControl Manager to the extent that they understand the following primary objects: users (administrators), tools, roles, managed nodes, node groups and authorizations. General ServiceControl Manager concepts are described in “Reducing IT Management Costs Through the Service Control Manager” and an in-depth discussion on tools is presented in “ServiceControl Manager Tools,” both of which appear in these proceedings.

2 Roles

ServiceControl Manager roles allow groupings of administrators and tools along functional, organizational, or any arbitrary criteria important to the requirements of the Internet data center. ServiceControl Manager tools these roles and map administrators to tools they can execute.

Another way to think of a role is as a toolkit. SCM tools are associated with roles. When a trusted user assigns a role to an SCM user on an SCM node, the user may execute any SCM tool associated with the authorized role on the SCM node.

An example of a role is `troubleshooter`. An example use of this role is to allow administrators assigned this role to execute diagnostic or performance tools on nodes in the Internet data center.

2.1 Attributes

The role is a simple object, but its place in the ServiceControl Manager security policy is crucial for effective administration of the data center. The ServiceControl Manager trusted user may modify role attributes using the `mxrole(1M)` command. This command records role modification operations in the ServiceControl Manager central log.

2.1.1 Name

The role name is a unique identifier used to refer to the role. The role name can contain embedded spaces, dashes and underscores, and its length cannot exceed sixteen characters.

2.1.2 Role ID

The role ID is the unique identifier by which the ServiceControl Manager represents roles. The ServiceControl Manager does not expose this attribute is not exposed to the user and uses it internally.

2.1.3 Description

The description provides a field to contain a short line of text describing the role.

2.1.4 Enablement

ServiceControl Manager roles have a state of either enabled or disabled. A tool that assigned a disabled role prevents the ServiceControl manager from executing a tool for a user who has that role on a specified node. An example of a situation where a role could be enabled or disabled is a role that a vendor's field service engineer would use to run tools on machines when they are on site.

2.2 Semantics

The ServiceControl Manager trusted user could assign a ServiceControl Manager role on a prescribed set of nodes to administrators who have similar responsibilities in the Internet data center. For example, The SCM trusted user could assign a "`backup ops`" role to administrators responsible for performing backup and restoration. Then, the SCM trusted user would assign the "`backup ops`" role to all tools that accomplish backup and restoration. The role links the user with the tool.

ServiceControl Manager provides a fixed set of sixteen (16) roles. With the exception of one role, the trusted user may change all role names to provide names that make sense in the environment.

2.2.1 Master Role

The ServiceControl Manager role named `Master Role` is special. Its attributes are not modifiable. Because the SCM automatically assigns the `Master Role` to every SCM tool, the `Master Role` allows a user assigned this role to run any tool on any node assigned this role.

3 Authorizations

An authorization is the association between a user (administrator), role, and node or node group, and is the fundamental element of the security policy. SCM Trusted Users may maintain the authorizations associated with individual nodes with the GUI or the `mxauth(1M)` command. In the current version of SCM, SCM Trusted users must use the `mxauth(1M)` command to maintain authorizations associated with node groups. The SCM records all authorization operations in the ServiceControl Manager central log.

3.1 Attributes

The following fields comprise an SCM authorization.

3.1.1 User Name

The user name identifies the UNIX login name of the user for the authorization. A trusted user must have registered this name as a ServiceControl Manager user.

3.1.2 Role Name

The role name identifies the name of the ServiceControl Manager role for the authorization.

3.1.3 Node Name

The node name identifies the Managed Node for which the user and role combination is valid. An SCM authorization may contain either a node or a node group but not both.

3.1.4 Node Group Name

The node group name identifies the node group for which the user and role combination is valid. A trusted user must have previously defined the node group in the ServiceControl Manager domain. SCM authorization may contain either a node or a node group but not both.

3.1.5 Semantics

ServiceControl Manager uses authorizations to determine if an administrator can execute the ServiceControl Manager tools associated with the specified role on a node or node group . An administrator may execute a tool from the GUI or the command line. To execute the tool, the administrator specifies the name of the tool to execute, along with any parameters for the tool, and the target nodes or node groups on which to execute the tool.

The ServiceControl Manager authorizes a tool invocation using the following steps:

1. Determine what ServiceControl Manager user is attempting to execute the tool
2. Determine which of the tool's roles are enabled
3. Verify that the user is authorized for one of the enabled roles on each target node or node group

Tools can fail to execute for a number of reasons, but failures that occur because they violate the data center's security policy are:

- The user has no authorizations
- The tool has no enabled roles
- There are no enabled roles shared by the tool and the user

- The user is not authorized a tool's enabled role on a target node or node group
- The user is not authorized to run any tools on a target node or node group

Tool authorization fails as soon as the ServiceControl Manager detects a violation of the data center's security policy. The ServiceControl Manager reports the nature of the tool failure and logs it in the ServiceControl Manager central log.

4 Implementing a Security Policy

ServiceControl Manager enables configuration and management of very simple, robust, and flexible, security policies from the Central Management Server. The ServiceControl Manager administrator determines the complexity of the security policy.

After installing and initially configuring the ServiceControl Manager on the CMS, the following steps must take place to configure the security policy for the data center:

- Install the ServiceControl Manager agent software on each managed node
- Use the GUI or the command line to add managed nodes to the ServiceControl Manager repository
- Identify ServiceControl Manager administrators (users) and add them to the ServiceControl Manager with the GUI or the command line
- Add any environment-specific tools to the ServiceControl Manager repository with the GUI or the command line
- Configure node groups, using the GUI or the command line, comprised of nodes with common functionality
- Configure the roles and authorizations

4.1 A Simple Example

Assume that a customer has a data center comprised of a number of HP servers that are responsible for the following functions:

Business processes (payroll, billing, logistics, etc)

E-commerce (web servers)

Database applications for E-commerce

Also, assume that there are operation/organizational roles

Backup/restore operations

HP customer/field support engineer

These may be just a subset of the roles that the trusted user can configure as the security policy. Further, once the trusted user identifies the roles, the administrators responsible for those roles should be identifiable.

4.1.1 Configure Roles

Only the `mxrole(1M)` can modify roles. However, administrators may view them through the GUI. Only ServiceControl Manager administrators with the Trusted User privilege are able to modify roles. The ServiceControl Manager initially configures the following roles:

```
$ mxrole

Master Role
operator
dbadmin
webadmin
lvmadmin
role6
role7
role8
role9
```

```
role10
role11
role12
role13
role14
role15
role16
```

This form of mxrole(1M) simply lists the names of the roles. The Trusted User has determined that the following roles make sense in the data center:

- `operator`
- `bp ops`
- `backup ops`
- `webadmin`
- `dbadmin`
- `HP CE`

The Master Role is not modifiable, and the operator role is a valuable role in this data center. Next, the trusted user modifies the roles for the security policy in the following manner:

```
$ mxrole –m role6         –N “bp ops”
$ mxrole –m “bp ops”      –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”
```

The ServiceControl Manager initially enables all roles. Note that the above steps disabled the HP field engineer role. The ServiceControl manager logs all role modification operations in its central log.

4.1.2 Configure Authorizations

After configuring the roles, the trusted user may create the authorizations, thus defining the security policy for the data center. In this case, the trusted user reasonably assumes that the operator role applies to all nodes in the data center. To configure the authorizations for administrators with this role, the following command is used:

```
$ mxauth –a –u U –R operator –n ‘*’
```

where *U* is the login of the ServiceControl Manager administrator performing `operator` duties on **all** nodes within the data center. Therefore, user *U* on all nodes may execute all tools assigned the `operator` role. The wildcard is a convenience for stating that the user/role combination is to be defined for all the currently defined ServiceControl Manager nodes.

Assume that the names of the nodes running the ERP software are named `erp1 .. erp`N.

Further assume that administrators *U1 .. UN* are to be authorized to execute ERP-related tools on the `erp*` nodes. There may be a large number of authorizations for these nodes and administrators, but `mxauth(1M)` can only create or delete a single authorization on the command line. However, we can use the form of `mxauth(1M)` that enables multiple authorizations to be specified in a file for creation or deletion. The command is:

```
$ mxauth –a –f /var/tmp/erp_auths
```

where each line of `erp_auths` is of the form

```
username:rolename:nodename
```

This colon-delimited syntax fully defines all attributes for the authorization, and is effectively its *name*. The user name, role name and node name must be valid ServiceControl names. The contents of the file specifying authorization for our ERP administrators on the ERP nodes is

```
U1:bp ops:erp1
U1:bp ops:erp2
. . .
. . .
. . .
UN:bp ops:erpN
```

Again, the `mxauth(1M)` command logs a message in the ServiceControl Manager central log for each authorization created. We configure all authorizations in a similar manner. Once the security policy is in place, creating authorizations for new administrators or nodes is straightforward.

4.1.3 Using Node Group Authorizations

When defining the ServiceControl Manager security policy, the ServiceControl Manager trusted user might define authorizations in terms of nodes or node groups. Node group authorizations provide a more dynamic and robust form of authorizations than individual node authorizations.

Node groups are logically related sets of SCM nodes defined by the ServiceControl Manager trusted user using the GUI or the `mxngroup(1M)` command. The ServiceControl Manager trusted user could add or remove nodes from an SCM node group as needed.

When a ServiceControl Manager trusted user authorizes a node group to an SCM user, the SCM user is authorized the specified role on all nodes defined in the node group. As the ServiceControl Manager trusted user changes the membership of the node group, the ServiceControl Manager dynamically updates the node group authorization to stay current with the node group membership.

To create a node group authorization using the `mxauth(1M)` command, the ServiceControl Manager administrator uses the following command form:

```
$ mxauth –a –u U –R operator –g group1
```

Note that the trusted user must have previously defined the node group “group1” in the SCM domain before creating the node group authorization.

If the ServiceControl Manager trusted user ever removes the node group from the SCM domain, the ServiceControl Manager automatically removes all authorizations associated with the node group.

5 Conclusion

ServiceControl Manager allows administrators to manage the use and configuration of their machines by enforcing an easily configurable and very flexible security policy for their data center. The ServiceControl Manager allows administrators to distribute and execute tools on authorized machines based on the roles in the data center. Therefore, ServiceControl Manager allows a Internet data center administrator to configure and enforce a security policy for all ServiceControl Manager tools and administrators for all managed nodes in the data center.

An audit trail tracing the configuration of the security for the ServiceControl Manager is available in the ServiceControl Manager log file. All authorization creation and deletion, as well as role modifications appear in the log.