
# *Role-Based Access Control In Network Vulnerability Management*

## Introduction

All large organizations are run on business processes and policies that define roles and responsibilities. An enterprise security solution needs technology that effectively simplifies the distribution and enforcement of the security policy in order to manage and administer the system. STAT Guardian™ Vulnerability Management Suite (VMS) by Harris Corporation offers this technology.

STAT Guardian VMS is used by enterprise customers around the world. It is comprised of a scan engine (STAT® Scanner), a remediation engine (STAT® Patch and Remediation), a centralized reporting functionality (STAT® Report Center) and an enterprise distributed management functionality (STAT® Command Center).

In enterprise deployments, multiple Vulnerability Management (VM) engines (a scan engine and a remediation engine) may be deployed across the enterprise - reporting to one or more hierarchical reporting levels, as shown in *Figure 1*.

STAT Command Center, the STAT Guardian VMS enterprise distributed management component, provides for the distribution and enforcement of security policies via Role-Based Access Control (RBAC). This paper outlines how RBAC intuitively models daily security policy task requirements, reduces administrative overhead and adapts to fit any network architecture.

## Large Enterprise Deployment Security Challenges

One of the challenges for enterprise deployments is managing the business processes and policies and maintaining uniformity in a widely distributed

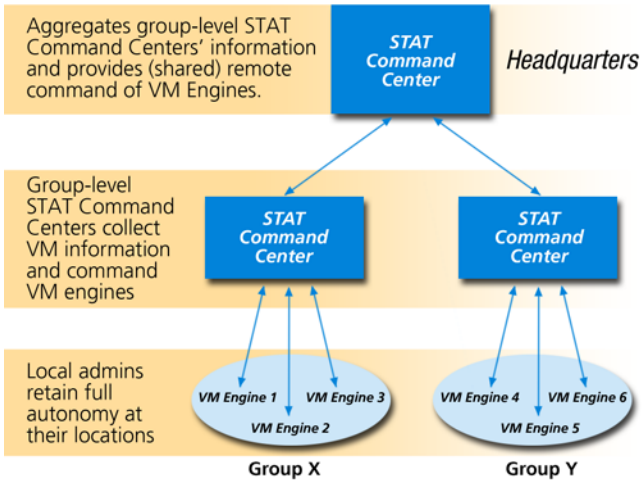


***Figure 1. Harris Corporation's STAT Guardian VMS supports a distributed enterprise deployment***

environment. Harris Corporation's STAT Guardian VMS provides the mechanisms for the effective management of security policies over enterprise deployments via the Role-Based Access Control (RBAC) functionality of STAT Command Center.

RBAC supports the traditional security principles of "least privilege," "separation of duties," "data abstraction," and the security tenet of "need to know" as referenced in *Figure 2*. Security officials can custom-define enterprise-specific roles that are natural parallels to each position of the organization. Administrators can then implement security policy and procedures by assigning users to roles based upon their positions.

Users' privileges are determined by the role(s) to which they are assigned.

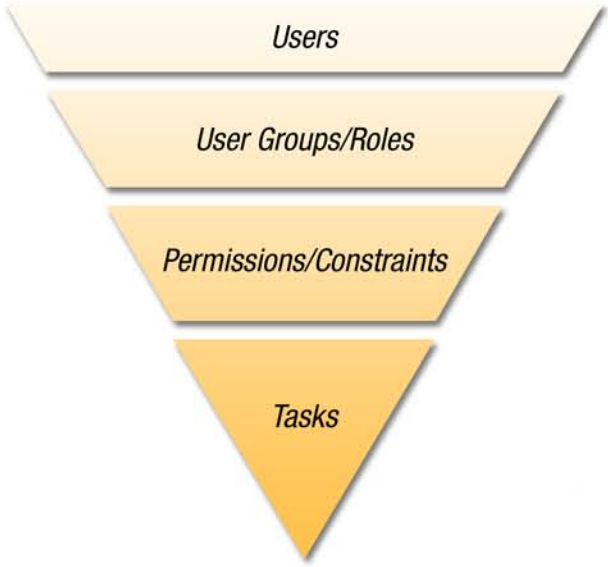


*Figure 2. STAT Guardian RBAC supports the "least privilege" and "separation of duties" concepts*


*Figure 3. Global policy can be created and enforced from a central location*

Users are added and removed from roles as their job assignments change. As users transition between roles, their membership in user groups can easily be created or revoked; role assignments can be modified without the need to update the privileges for every user on an individual basis. The role definitions themselves are typically stable over time, but the group memberships tend to be dynamic. STAT Command Center can even create roles that have a different set of privileges associated with each VM engine in the interface.

## Centralized RBAC Management for a Distributed Architecture

Many organizations lose time and money because users may not know where one function ends and another begins. Cost savings are realized with STAT Command Center RBAC because there is no ambiguity over job responsibilities. STAT Command Center RBAC provides default roles, but new roles can be created that are tailored to each organization's business processes and security policies. Tailoring may be for job functions, geographic boundaries, political boundaries or all of these. Once an RBAC framework is defined and implemented, it will scale across the enterprise. The framework may be centrally deployed and managed, as shown in *Figure 3*.

STAT Command Center RBAC allows for both top-down and distributed network administration. In a distributed architecture, network administrators at a given subnetwork may choose to provide the STAT Command Center account with any subset of privileges they choose. For example, this account may be given full privileges to scan the entire network, but remediation privileges may be limited or denied altogether.

## Practical Application of STAT Command Center RBAC

The use of STAT Command Center RBAC reduces the administrative tasks associated with managing a security policy by creating STAT Guardian VMS users and granting privileges to use the tool suite. Since users inherit their privileges from the user groups of which they are members – and most organizations will have a limited number of roles—changing privileges for all users requires few changes.

Users can be assigned to as many roles as necessary to describe their various functions. If every user in a particular organization has a certain base level of privileges, it would be inefficient and redundant to administer if those privileges were granted to every role. Instead, separate roles can be created to cover these general privileges, and all users should be placed in this role as well as any other roles necessary to perform their jobs. Then, by modifying the base role, the general set of privileges for every user in the organization can be modified in a matter of seconds.

In most organizations, there are differences between the vulnerability management needs of a helpdesk operator and a systems administrator. A helpdesk operator may only require the ability to create scans, whereas a systems administrator can also be required to remediate any vulnerabilities that are found. In addition, some helpdesk operators may only be allowed to scan for vulnerabilities on certain machines—such as workstations—leaving servers for other personnel. With STAT Command Center RBAC, this scenario and much more complex environments are possible. Simply create a role called "Helpdesk Users," grant the ability to perform scans (limiting the scope to only workstations if needed), and add and remove users as the staff grows and changes. Do the same for other positions in the organization and suddenly you have a simple and intuitive system that parallels your organizational structure.

STAT Command Center is also capable of creating roles with unique privileges associated with each unique VM Engine, such as creating roles that mask certain VM engines. If applying privileges at the "Scanner" (or VM engine) level is too granular, try applying privileges at the Group level instead, as shown in *Figure 4*. The RBAC framework easily allows security policy administrators to get as broad or as specific as needed, as shown in *Figure 5*.

## Default Roles

STAT Command Center's default roles are preconfigured to suit most existing security policies. These ready-to-use roles provide a quick, easy set-up right out of the box for a wide range of users: Scan users, Advanced Scan users, Remediate users, Advanced Remediate users, Report users, Managers and Administrators. For more complex environments, STAT Command Center also allows for any number of custom roles to be created in minutes.

Once the roles for the organization have been established, the only administrative tasks that remain are to assign users and move them into and out of roles. Each privilege listed in *Figure 6* is described in detail in the Privilege Descriptions section.

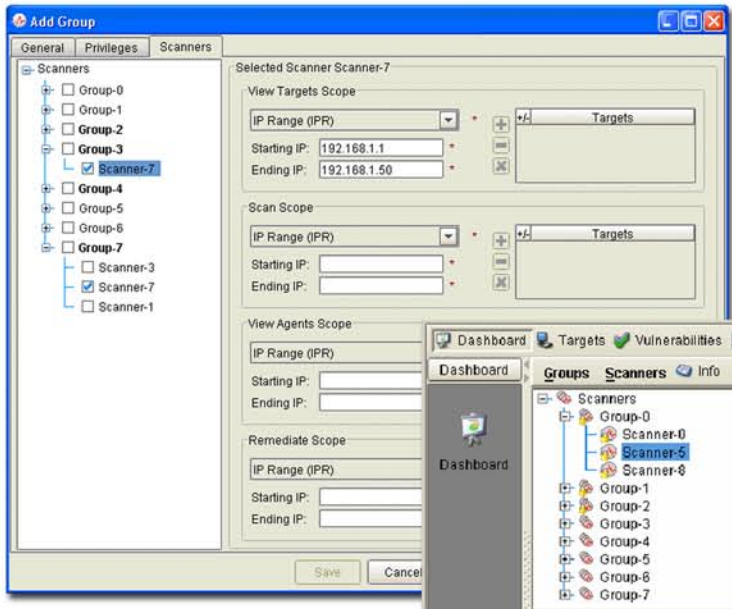


*Figure 4. STAT Command Center RBAC provides the power and versatility needed to implement your security business process.*

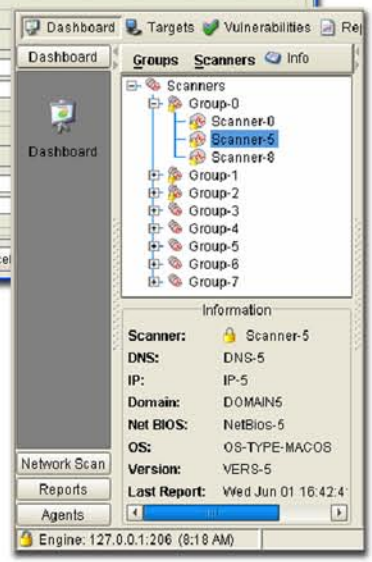


*Figure 5. STAT Command Center RBAC provides a management dashboard to provide immediate status*

## STAT Command Center—Default Roles

| Privilege | Roles | | | | | | |
|---|---|---|---|---|---|---|---|
| | *Scan* | *Advanced Scan* | *Remediate* | *Advanced Remediate* | *Report* | *Manager* | *Administrator* |
| Remediate | | | * | * | | * | * |
| View Agents | | * | * | * | * | * | * |
| Send Agent Data | | * | | * | * | * | * |
| View Targets | * | * | | | * | * | * |
| Scan | * | * | | | | * | * |
| Send Job Data | | * | | | * | * | * |
| Add Port/Vulnerability/Credential Sets | * | * | | | | * | * |
| Delete/Modify Jobs | | | | | | | |
| – Change OS of a Target/Delete Target | | * | | | | * | * |
| Modify Vulnerabilities | | | | | | | |
| – Change update schedule/Update now/Update file | | * | | | | * | * |
| Modify Port/Vulnerability/Credential Sets | | | | | | | |
| – Modify = Change/Delete | | * | | | | * | * |
| Modify License | | | | | | | * |
| Add and Modify Users and Groups | | | | | | | * |
| Modify Agent Groups | | | | | | | |
| – Modify = Change/Delete | | | | * | | * | * |
| Modify Scanners and Scanner Groups | | | | | | | |
| – Modify = Change/Delete | | | | | | | * |
| View Scanners Scope | | | | | | | |
| – Defaults to the "All" scanner group | * | * | * | * | * | * | * |
| Restart PatchLink Service | | | * | * | | * | * |
| Perform Agent-Based Scan | | * | * | * | | * | * |

*Figure 6. For a quick and easy set-up, use STAT Command Center's default roles right out of the box*

## Privilege Descriptions

- **Remediate**—Remediate on any Agent with an IP address in the range of the Remediate Scope (*.*.*.* by default).
- **View Agents**—View all Agents with an IP address in the range of the View Agents Scope (*.*.*.* by default).
- **Send Agent Data**—Send any agent data that can be seen via the View Agents Scope to a STAT Report Center or STAT Command Center.
- **View Targets**—View targets of network scan jobs that have IP addresses that fall in the range of the View Targets Scope (*.*.*.* by default).
- **Scan**—Perform a network-based scan on any device with an IP address that falls in the range of the Scan Scope (*.*.*.* by default).
- **Send Job Data**—Send any job data that can be seen via the View Targets Scope to a STAT Report Center or STAT Command and Control Center.
- **Add Port/Vulnerability/Credential Sets**—Create new port sets, vulnerability sets, and credential sets, but cannot modify or delete existing sets.
- **Delete/Modify Jobs**—Pause, resume, cancel, or delete any active, scheduled, or running job. Also change the Operating System of target(s) or delete target(s) found in a job.
- **Modify Vulnerabilities**—Change the vulnerability update schedule, perform update now, and update from file.
- **Modify Port/Vulnerability/Credential Sets**—Delete or change the contents of any existing port, vulnerability, or credential sets that are not read-only (i.e., defined and maintained by STAT).
- **Modify License**—Modify the license serial ID and key.
- **Add and Modify Users and Groups**—Create, modify, and delete users and groups. This privilege should only be given to administrators because it allows users to elevate their own privileges to that of an administrator.
- **Modify Agent Groups**—Create and modify (change/delete) any agent group's properties and add or delete agents to or from any agent groups. This excludes read-only agent groups.
- **Modify Scanners and Scanner Groups**—Create and modify (change/delete) any scanner group's properties and add or delete scanners to or from any scanner groups. This excludes read-only scanner groups, and only exists on STAT Report Center and STAT Command Center. This privilege should only be granted to administrators because users with this privilege could elevate their privileges by moving a scanner from a group from which they have less privileges to one in which they have more.
- **View Scanners Scope**—This is the only scope that is not defined via IP range. The scanners and scanner groups that are included in this scope are the scanners that are visible when users log in to the STAT Report Center or STAT Command Center. If a scanner group is included, then all scanners in the group are visible (this changes dynamically when scanners are added or removed from the scanner group). For each scanner or scanner group included, the scopes that apply to this scanner group or scanner are inherited from the global scope (unless a specific scope is defined). If a specific scope is defined, this scope overrides global or group setting. The rule of thumb is that the scope applied at the lowest level has precedence. This privilege only exists on STAT Report Center and STAT Command Center.
- **Restart PatchLink Service**—Restart the PatchLink service on any agent that can be seen via the View Agents Scope.
- **Perform Agent-Based Scan**—Perform PatchLink agent-based scans on any agent that can be seen via the View Agents Scope.

## Summary

One of the biggest process challenges facing today's complex enterprise is ensuring that diverse user groups can leverage IT investments effectively. This is especially true when dealing with security-related assets and information and the policies that manage them. Efficiently accommodating many roles and access levels across vulnerability management users is paramount to executing effective security policies. Harris Corporation's STAT Guardian VMS easily delivers this required flexibility without creating excessive management overhead for security policy administrators.

## References

David Ferraiolo and Rick Kuhn, NIST, "An Introduction to Role-Based Access Control," *NIST/ITL Bulletin,* December 1995

Trey Guerin and Richard Lord, *ComputerWorld*, "How role-based access control can provide security and business benefits," November 6, 2003

Ravi Sandhu and Edward Coyne, *IEEE Computer*, "Role-Based Access Control Models," February 1996

HARRIS assuredcommunications™

STAT

www.stat.Harris.com | Copyright © 2006 | Harris Corporation | P.O. Box 8300 | Melbourne, FL USA 32902
888-725-7828 | 321-726-1478 | stat@Harris.com | PL-T-SVM-06-0327-G | 03/06 511018 SEC