Global Information Assurance Certification Paper

Role-Based Administration for Windows 2000

Author: Jane E. Murley

Date: July 26, 2001

Table of Contents

Abstract

Microsoft® Windows® 2000 has a significantly more complex security structure than previous versions of Microsoft operating systems. This paper looks at simplifying the management of security for Windows 2000 by discussing role-based administration in Windows 2000 and a product that provides role-based administration capabilities for Windows 2000.

Introduction

Security administration has continued to become more complex as environments have become more distributed, employee turnover increases, the number of objects to be secured increases, and security intrusions have risen. To meet some of these security challenges, security administration must encompass the enterprise instead of a single server. With the business need to either contract or outsource different functions, non-employees are now exposed to business critical systems and information, which further complicates security administration. All of these factors add to the increased complexity of administering security in the work environment, computer scientists have been looking at ways to simplify the complex task of security administration.

In 1991, a group of computer scientists proposed a new approach to security administration, called role-based administration (RBA), which is scalable, less error prone, and more easily audited than previous security administration approaches. Role-based administration is also known as role-based access control (RBAC) and role-based authorization. Under role-based administration, users are combined into groups, similar to the more classical administration models. Resources and access privileges or permissions are grouped into roles, which represent the various business functions. Roles are assigned to groups. Groups can be assigned multiple roles, based on the functions performed by the members of any specific group.[1]

As with other operating environments, Microsoft® Windows® 2000 presents a significantly more complex security model for controlling authentication and authorization in a Windows 2000 enterprise than previous versions of Microsoft operating systems. For example, in an effort to provide a more granular security model, Windows 2000 Group Policy has 100 security-related settings and over 450 registry-based settings compared with 72 System Policy settings in Windows NT 4.0.[2] While the Windows 2000 security service allows administrators the ability to more granularly apply security settings, security administration in a Windows 2000 enterprise has become more complex than Windows NT 4.0.

In this paper, we will discuss role-based administration - how it works, and its benefits, Windows 2000 security, and a tool that exists in the marketplace for managing Windows 2000 using role-based administration.

---

[1] Byrnes, p. 1-2.

[2] Microsoft, "Group Policy", p 27.

Role-Based Administration

Computer scientists, government agencies, and security conferences have been examining role-based administration for about 10 years because RBA is considered a promising technique for simplifying security administration and more easily auditable than previous methods of administering complex security environments. The National Institute of Standards and Technology (NIST) funded research on role-based access control (RBAC).[3] The Defense Advanced Research Projects Agency (DARPA) has also funded work on role-based access control.[4] Conferences are now including sessions devoted to role-based administration. What makes role-based administration better than existing security administration methods?

Role-based administration is comprised of users and groups, roles, permissions, and resources. Users typically are assigned to groups, based on their functions within the organization. For example, financial analysts would be placed in a different group than administrative assistants because their job functions are different. Roles are also created based on the requirements of different job functions within an organization. Permissions are associated with roles. Roles assign permissions to perform a particular task, access a specific application, etc. Permissions are the ability to perform specific tasks utilizing specific resources. Some examples of resources are applications, files in a directory, databases, printers, and workstations. For example, a computer operator requires access to servers and their tape drives to back up the data on the servers, while a financial analyst does not have that requirement. Decisions on the permissions assigned to a particular role are typically based on the organizational function performed by that role. Defining a comprehensive set of roles within an organization is critical to the success of role-based administration, if roles are to be an effective method of managing access to resources within that organization.[5]

Using role-based administration improves security practices within an organization. Security "Best Practices" dictate that organizations write and maintain security policies that clearly outline the security roles and responsibilities for an organization. Role-based administration facilitates an organization's ability to create security policies by building security policies around the organizational roles. RBA allows for separation of duties. Security administrators determine the

[3] "Role Based Access Control."

[4] Thomsen, p. 1.

[5] "An Introduction", p 1 – 2.

set of permissions required for each role, which can be a complex process. Delegated local administrators have the much simpler task of applying the roles to individual users and groups, based on the users' or groups' job function. A security administrator converts a particular role into a list of resource permissions necessary for the users to perform a job function. As a user's function changes in the organization, the user can be moved to a different group and/or roles can be added or removed from the user's account. As requirements for a role change, permissions can be added or removed from the role to reflect the change without changing permissions for each and every user and group assigned to that role. By simplifying the administration tasks and eliminating the need for manually assigning and re-assigning permissions for individual users, role-based administration enhances security in user environments.

Windows 2000 Security[6]

Windows 2000 security is comprised of a number of different components. This section describes, at a high level, the complexity of the security services within Windows 2000 to serve as a basis for discussing how a role-based administration tool can simplify the security administration process. The components discussed in this section are Active Directory, Access Control Entries, Group Policy Objects, and various tools to manage Windows 2000 security.

Windows 2000 is a directory-based operating system. The directory, Active Directory is used to store user, security, application, and configuration information. Active Directory follows a hierarchical database model, similar to X.500. Active Directory is comprised of a forest, with one or more trees. Each tree has one or more domains, similar to Windows NT domains. Each domain has its own instantiation of the directory database, containing objects that belong to that specific domain and possibly a subset of information about objects in other domains. A domain can be further broken out into Organizational Units (OU). The domain forms the top-level organizational unit within the domain, while all other organizational units within the domain are subordinate to the top-level domain OU. Since Active Directory is the repository for some security information, it is one focus for security administration. Active Directory utilizes a multi-master replication model, where updates can be applied to any instance of a specific directory database and are replicated to other instances of the same domain database.

Access Control Entry (ACE) defines the permissions a user or group has been

[6] Microsoft, Windows 2000 Advanced Server.

granted for a specific file or object. Many objects within Windows 2000 have the Security tab on their Properties page, which is where access control entries are defined. A set of permissions for the object is assigned to a specific user or security group within Windows 2000, forming an access control entry. The set of all access control entries for a specific object form the access control list (ACL) for that object. Different objects have different available permissions. For example, a file has Full Control, Modify, Read & Execute, Read, and Write basic permissions. A Group Policy Object has Full Control, Read, Write, Create All Child Objects, Delete All Child Objects, and Apply Group Policy basic permissions. ACEs provide the foundation for securing Windows 2000 files and other objects. Generally, the default permissions for files and shared folders in Windows 2000 permit *Everyone* Full Control access. ACLs need to be applied to secure these files and shared folders. ACEs can be assigned in Windows Explorer or using other tools specifically designed to administer that specific object.

"Group Policy is a Windows 2000 administrator's primary tool for defining and controlling how programs, network resources, and the operating system behave for users and computers in an organization. Group Policy allows you to specify a desired computer configuration one time, and then to rely on the Windows 2000 environment to enforce that desired configuration on all affected client computers until you want it to change. After you set Group Policy, the system maintains the state of computers without further intervention."[7] Group Policy Objects contain the settings that are applied to specific objects. Group Policy Objects can be applied to sites, domains, and organizational units.

Windows 2000 comes with various tools for configuring and administering security. Security Configuration and Analysis Microsoft Management Console (MMC) snap-in enables the administrator to compare the current security settings for account policies, local policies, event log, restricted groups, system services, registry, and file system against a stored configuration. Only those security attributes contained in the template are analyzed. The analysis indicates whether settings are the same with a green check mark, different with a red X, or not tested with no indicator. The analysis is performed on one system at a time unless a script is used to automate the process for multiple systems.

Security attributes can be set on each system manually via the Domain Security Policy program or through the use of a security template in the Security Templates MMC snap-in. Both methods affect account policies, local policies, restricted groups, registry, file system, and system services. The security templates are pre-

[7] Microsoft, "Group Policy", p. 1.

defined security templates that collect the security attributes in a single place and assign values to them. Templates have been defined for various levels of security – default, secure, and highly secure – and for different levels of systems – domain controller, server, and workstation. These templates can also be imported into a Group Policy Object and used to apply that security profile to a single computer or many computers.

Active Directory Users and Computers MMC snap-in administers user accounts, groups, computer accounts, and contacts. Users and Computers snap-in is also used to delegate administrative control over domains and organizational units. ACEs can be used to secure Group Policies from the Active Directory Users and Computers MMC snap-in.

Windows 2000 is much more complex than Windows NT. Many different tools are required to secure different aspects of the Windows 2000 environment. While most of these tools exist as Microsoft Management Console snap-ins, the administrator needs to determine which tool will produce the required results. While the Windows 2000 security model allows an administrator to create security groups and assign permissions to those groups, the tools do not facilitate auditing the access permissions assigned to a particular group. The Windows 2000 tools allow for delegation of administration of organizational units and domains, but the tools offer no simple view of the rights relationships within the Windows 2000 environment.

Role-Based Administration Tools

Several vendors have role-based administration tools for Windows 2000. This section will describe the BindView bv-Admin product and its role-based administration implementation. This document does not make any recommendations for or against bv-Admin, but merely presents information on the role-based administration offered by this product. Information about the product was gathered using the product and its help files.

BindView bv-Admin™ for Windows 2000[8]

BindView's bv-Admin™ is a suite of products used to manage users and their resources in a single or multiple platform environment. "A comprehensive, integrated directory management solution, bv-Admin streamlines the administration of resources across Microsoft Windows® 2000, Windows NT® 4.0,

[8] BindView, bv-Admin.

Exchange® 5.5 and Exchange 2000, and Novell® NDS®."[9] bv-Admin for Windows 2000 was developed specifically for Windows 2000 and uses the Active Directory Service Interfaces (ADSI) to access Active Directory. bv-Admin does not require software on each Active Directory server. bv-Admin uses Microsoft interfaces, like DCOM and ADSI to interface with Windows 2000. bv-Admin does have a server piece of software that creates a data cache that stores information about roles and activity logs of bv-Admin actions, both successful and unsuccessful. This data cache can be either an Access or SQL database.

bv-Admin offers a number of different functions, one of which is to delegate administrative tasks for Windows 2000, where bv-Admin allows role-based delegation of tasks. Administrative tasks are delegated in bv-Admin by assigning a role to an individual or group. Roles assign specific administrative responsibilities. bv-Admin has included pre-defined 18 administrative roles. Additional roles can be created to better meet organizational requirements. Roles can be assigned to users and groups. Some examples or roles are:

- Account Manager allows a user or group to manage user accounts.
- Organizational Unit Manager allows a user or group to manage an Organizational Unit.
- Printer Manager allows a user or group to manage a printer

Roles can be created at any level in the tree and are available to the whole organization.

Each role is comprised of tasks, where a task is a single administrative action that can be assigned to a user or group of users. bv-Admin offers no capabilities to create additional tasks. bv-Admin has about 180 defined tasks. bv-Admin offers no capabilities to create additional tasks. Some examples of tasks are:

- CanAddPrinter allows the user or group to install a printer on a computer.
- CanCreateFile allows the user or group to create a file on the share or in the folder.
- CanManagePrinterDocuments allows the user or group to perform administrative tasks on print jobs.

Tasks are descriptive with further details in their description to make their functions easy to understand. Tasks equate to access control entries for different

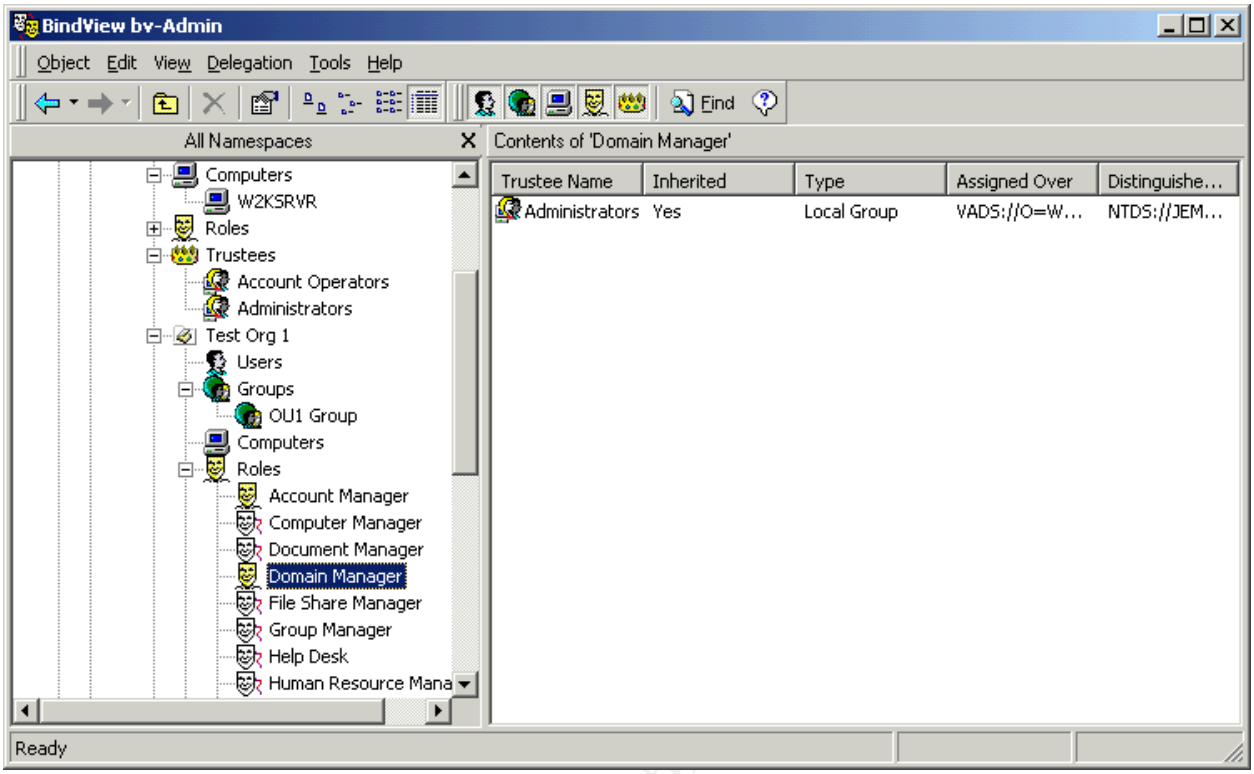
[9] BindView, "bv-Admin Evaluator Guide", p. 1.

objects, such as printers, files, groups, and users.

bv-Admin offers two clients, the bv-Admin Client for Windows 2000 and a browser version of the client. Both clients offer administration of Windows 2000, as well as Windows NT and Microsoft Exchange. The client interface is divided into two sections; the tree view can be shown on the left and the actual contents are on the right. Both client interfaces provide graphical user interfaces, where the user can click to drill down in the tree to get to the desired object. Figure 1 - bv-Admin Screen displays the bv-Admin client for Windows 2000 window. As with other Windows interfaces, the user can right click on an object to get a list of operations that can be performed on that object and to view the properties of the object. For example, right clicking on *Test Org 1* allows the administrator to chose operations such as moving the organizational unit to another portion of the tree, creating organizational units (OU), users, groups, computers, and roles within *Test Org 1*, deleting the OU, renaming the OU, and viewing the properties.

The bv-Admin client for Windows 2000 provides access to additional Windows 2000 administration capabilities. The bv-Admin client provides access to the domain's account policy and account lockout as well as the local computer's account policy, account lockout, auditing, and rights. Additionally, local groups can be administered from the bv-Admin client. When operating in a heterogeneous operating environment, the bv-Admin client can be used to administer both Windows 2000 and Windows NT 4.0 environments, allowing the administrator to enter the user information once and allowing bv-Admin to update the information in the two environments.

Figure 1 - bv-Admin Screen



Contact BindView via phone at 800-813-5869, via email at sales@bindview.com, or via the web at http://www.bindview.com for additional information and an evaluation copy of bv-Admin.

Conclusions

Role-based administration is critical for managing complex Windows 2000 security environments. Using role-based administration simplifies the security administration of the organization, eases auditing, eases troubleshooting security problems, simplifies implementation of the organization's security policies, and permits for separation of duties. Given the complexity of managing resources within Windows 2000, using a role-based administration tool is recommended to simplify security administration and reduce the time required to maintain security on the various Windows 2000 objects. Tools such as BindView's bv-Control should be evaluated for suitability in providing role-based security administration in any organization's environment. Vendors offer evaluation copies of the product. Each organization considering implementing Windows 2000 should evaluate these products in their Windows 2000 lab environment to determine which product is better suited to the operational environment.

References

Aberdeen Group, Inc. "Kick-Starting a Directory-Enabled IT Infrastructure: Delegation Rights Management in Active Directory – An Executive White Paper." December 2000. URL: http://www.quest.com/whitepapers/Aberdeen-Group.pdf (3 Jul. 2001).

BindView. bv-Admin for Windows 2000 version 4.1.121. June 6, 2001. bv-Admin for Windows 2000. BindView, 2001. BindView. Windows 2000 Server or Advanced, 20 MB, CD-ROM.

BindView. bv-Admin for Windows 2000 version 4.1 Evaluator Guide. May 2001.

BindView. "Managing Group Policy Objects." WP-0011 0301. URL: http://www.bindview.com/downloads/public/WhitePapers/GroupPolicyObjectsWP32001.pdf (3 Jul. 2001).

Bragg, Roberta. Windows 2000 Security. Indianapolis: New Riders Publishing, 2001. 216 – 249, 422 – 439.

Byrnes, Christian. "Role Based Authorization: What and Why?" Tivoli Analyst Reports. 13 Jun. 1997. URL: http://www.tivoli.com/news/press/analyst/body_rolebased.html (18 Jul. 2001).

Hurwitz Group. "Management Controls: Security Impact of IT Administration." November 2000. URL: http://www.bindview.com/downloads/public/whitePapers/ImpactofItAdministration.pdf (20 Jul. 2001).

"An Introduction to Role-Based Access Control." http://csrc.nist.gov/publications/nistbul/csl95-12.txt (24 Jul. 2001).

Microsoft Corporation. "Change and Configuration Management Deployment Guide - Chapter 4 – How Group Policy Works." Microsoft TechNet. July 2001 (2000): 1 – 28.

Microsoft Corporation. Windows 2000 Advanced Server. Version 5.0.2195 Build 2195. Windows 2000 Advanced Server operating system. Microsoft, 2000. Microsoft.

Quest Software. "FastLane ActiveRoles™ Release 3.0 – A Guide to Reviewing FastLane ActiveRoles™." URL:

http://www.quest.com/fastlane/activeroles/pdfs/ActiveRoles_Rev_Guide_0401.pdf (22 Jul. 2001).

Quest Software. "Plan, Deploy, and Manage Windows 2000." URL: http://www.quest.com/whitepapers/Aberdeen-Group.pdf (3 Jul. 2001).

"Role Based Access Control." 9 April 2001. http://csrc.nist.gov/rbac/ (24 Jul. 2001).

Thomsen, Dan, O'Brien, Dick, and Bogle, Jessica. "Role Based Access Control Framework for Network Enterprises." URL: http://www.ktsi.com/carlos/papers/98/87890050.pdf (20 Jul. 2001).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS