WHITE PAPER: ENTERPRISE SECURITY MANAGEMENT

User and Group Entitlement Reporting

White Paper: Enterprise Security Management

User and Group Entitlement Reporting

Contents

Introduction

Understanding User and Group Entitlement Reporting

When securing a network, even when limiting the scope to the Microsoft portion of the network, there are numerous elements to address. These areas include, but are not limited to:

- Account Management
- Separation of Duties
- Patch Management
- Configuration Reporting
- Vulnerability Assessment and Remediation
- User and Group Entitlement

Although Symantec's products, specifically bv-Control® for Windows®, are used to address many of these security-related issues, the purpose of this document is to understand and address one of the most significant and challenging aspects of security: User and Group Entitlement.

Defining User and Group Entitlement

Many customers' needs fall into the category of Group and User Entitlement Reporting, but generally they involve the ability to answer the following questions:

Where in our network does John Doe have access?
What type of access is it?

The answer to this question identifies the Risk Exposure that an employee constitutes. This question is often asked when an employee leaves the company and is suspected of compromising information, or if the employee is being terminated.

Where in our network do members of this Group have access?
What is that access?

Adding a user to a group is a relatively simple process. More importantly, understanding the complete set of access controls granted to a user when they are placed in a group is a requirement of diligent security auditing.

Who has access to this data?

What type of access is it?

When all is said and done, the complete list of users that can read/write/modify specific data should be reviewed on a regular basis by both the data owner and the security auditor. This report is the foundation for that review.

Who validates that access grants are appropriate?

It is no longer enough to merely implement a strong security model. Due to regulations such as Sarbanes-Oxley, organizations are increasingly asked to provide proof of their ongoing review of access controls. In order for management to conduct periodic reviews of permissions grants, organizations must be able to associate critical data with appropriate business data owners who are able to validate the grants.

The Requirements and Limitations of Evaluating User And Group Entitlement

The associated challenges are two-fold. First, and most significant, all of the data "John Doe" has access to should not be the target of an entitlement report, since all of the "public" areas of the network will be included in such a report. Inclusion of this public data will conceal the significant data by burying it within thousands or hundreds of thousands or possibly even millions of extraneous records. Sensitive data should be segregated from public-access data, not only by direct controls, but by location—server/volume/root—directory. Failure to identify and overcome this challenge manifests itself in a number of ways. Examining and reporting huge volumes of data will take inordinate amounts of time and will dilute meaningful data to the point of uselessness.

The second challenge is to identify the accuracy boundaries of the data. Although it is imperative to understand this issue in the context of risk assessment, it is a relatively technical issue and is often misunderstood or ignored. The initial reaction is almost certainly, "Well, there is only one answer—the 100% accurate one. "While philosophically this is true, in the real world everything has its price—including accuracy. In this context, the variables associated with identifying effective permissions modify both the accuracy boundaries and the "cost" (time to results) of the entitlement report.

Let's examine the variables that impact the accuracy boundaries and understand the costs associated with them:

The parameters that affect the accuracy boundaries fall into two general categories:

1) file system permissions

2) machine-based rights

NTFS Permissions

File or Directory

We must first determine if there is a need to identify the permissions set at the individual file level or at the directory level. Most users and auditors assume that the directory is the access control point. In reality, each individual file has its own Access Control List. In most thorough audits, permissions should be examined at the file level; however, the cost of reporting at the file level, both in volume of data and in evaluation time, is prohibitively expensive. The ratio of files to directories is routinely 200:1000 or more per directory. To put this in perspective, examining access control at the file level rather than at the directory level changes a procedure that could be accomplished weekly into one that could take months. This is a prime example of the cost outweighing the value, unless employed with extreme caution.

Interpreting the DACL

When determining directory access, the first location to examine is the Access Control List associated with the directory, called the Discretionary Access Control List (DACL). There are many utilities that will dump this list into a file for further examination. However, a DACL contains multiple types of entries: those for User, and those for Groups, each being either Allow or Deny, and each identifying the specific permissions such as Read, Write, Modify or Take Ownership. An individual Access Control Entry (ACE) in a directory DACL, when taken out of context of the entire DACL, is at significant risk of being inaccurate. Without considering the Deny entries associated with a user, either directly or through group membership within the same Access Control List, the individual ACE is quite possibly an inaccurate reflection of a user's permissions.

For example, the Accounting group can be granted Allow Read and Write permissions to a directory. By contrast, the Accounts Payable group has the Deny right specified for the same directory. A user that is a member of both Groups would have Read permissions only, a result that is not reflected in either of the individual Access Control Entries (ACE). In summary, the DACL must be examined as a whole, since interpreting individual entries out of context or even out of order will often be wrong.

Users or Groups

Because the operating system algorithm uses the Access Control List to control access, the entire DACL must be considered as described above. As part of this algorithm, users' group memberships must be considered. In the Windows NT® environment, group membership is relatively simple. At its most complex, a user could be a member of a Domain Group that was a member of a Local Group granted/denied permissions.

With the advent of Native Mode AD, groups may be nested in far deeper structures. Before a user's effective directory permissions can be identified, every ACE must be examined for Allow and Deny, and every group ACE must be expanded to its constituents to include any nesting, so it can be determined if the ACE applies to the User or Group in question. Determining effective group membership is not a trivial task; yet, it is a foundation for user or group entitlement reporting.

For a reasonably accurate interpretation of NTFS permissions on both the Group and User level, reporting must take into consideration the Complete DACL, interpreting both Allow and Deny, as well as completely accurate effective group membership reporting. Anything less is simply wasting paper. As we will see, there are additional considerations, depending on the accuracy boundaries defined.

Rights Analysis

Further Restrictions: Network or Local Access

After examining the NTFS permissions on the file system, we must determine how a user can access the data. So that users that have effective NTFS permissions to actually access the data, they must be able to access the data. For example, before a user can reach a point at which the DACL on the directory is examined, they must be able to access the machine. There are two choices: either local access or access via the network. For a user to access a machine locally,

they must effectively have the Logon Locally machine right. As with other Microsoft access controls, this is also a calculated field that must consider multiple machine rights and effective group membership when identifying who has these rights. With a combination of an effective Logon Locally right and an appropriate DACL, they can now access the data.

With most networks, the point is to share the data from the network. For remote users to access the data, they must effectively have the machine right, Access this computer from the Network? As with the Logon Locally machine right, there are multiple rights to be considered, as well as effective group membership. If a user is allowed network access, there must also be a Network Share that enables access to the target directory, and the user must have permissions on that share to access the data. An individual's effective permission to a directory is the intersection of the share permissions and the NTFS permissions, whichever is lower.

The Bypass Traverse Network Checking right comes into play here as well. This right allows a user to traverse a directory for which they do not have permission (use it as part of a file path), resulting in the ability to access a child directory where they do have permissions. If this permission is granted to specific groups, it must be expanded to determine membership. By default, Microsoft grants both EVERYONE and USERS this right. While EVERYONE is a well-known group that cannot be modified, USERS can be changed to include or exclude users and groups, and as such, it must be expanded to determine the impact when calculating effective permissions.

Accuracy boundaries play a role in determining the need for this analysis. The share permissions and Network/Local access rights discussed above cannot add users to a file or directory; they can only shorten the list. If an entitlement report is based solely on NTFS permissions, it would show users that have access based on NTFS permissions, but in reality the share permissions or the machine-based rights mentioned above could prohibit some of these users from accessing the data. This type of inaccuracy would be classified as a false positive—often considered a reasonable accuracy boundary.

Other Machine-Based Rights

Based on the NTFS permissions and Network/Local access controls, both have examined the ways to identify users and groups that have file system permissions. Unfortunately, this is not the complete list of users that have File System Access. Without considering malicious code,

hacking utilities, etc., there are basic machine rights that also allow a user to access the File System without an associated entry in the DACL. Three specific machine-based rights that grant access to the file system are Backup files and directories, Restore files and directories, and Take Ownership of files or other objects.

A user with any of these rights can read any object in the file system on that machine. Although these rights are usually reserved for administrative tasks, they are sometimes granted to others. In order to be completely accurate, an entitlement report should consider these rights when listing users that have access to the file system.

Data And Performance Considerations Of The Entire Process

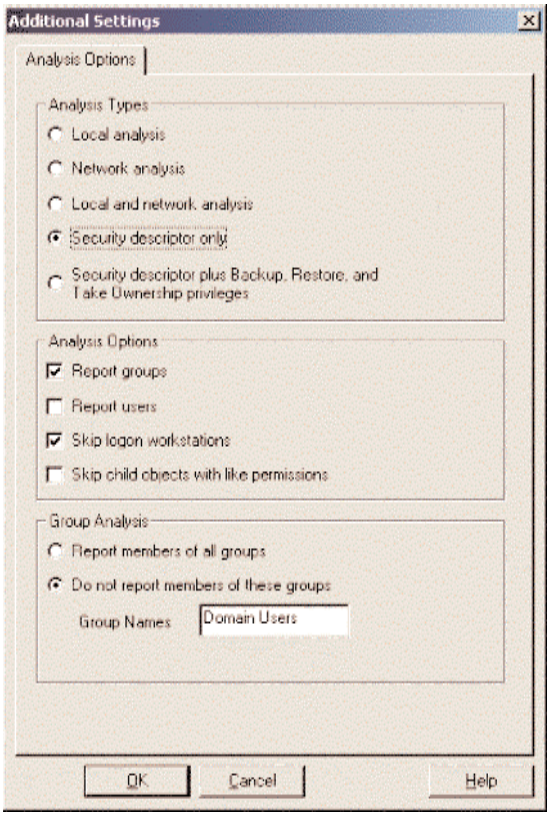
The following points should be considered when undertaking such an extensive task as User and Group Entitlement Reporting in an enterprise-class corporate environment.

- The entire DACL must be analyzed to determine the effective permissions of one user. A vast majority of the work required for identifying every user's access to a file or directory has already been done. Filtering results for just one user is an inefficient use of this type of data.
- If the directories examined include public areas, the volume of data returned will be tremendous. Even if constrained (as it should be) to examine just the "Crown Jewels," millions of records returned in a moderate-sized network are to be expected. Data this large does not lend itself to printing, exporting to Excel, viewing on a Web page or the like. This volume of data is only usable when shepherded into a database to be used for ad hoc queries.
- Every additional degree of accuracy has associated costs in the complexity and calculation time. When analyzing tens of thousands of directories, and if the number of analysis calculations can be reduced from billions to merely millions, these compromises must be weighed if the time to results is a factor.

How Symantec Reporting Can Be Configured To Work With These Constraints

With bv-Control for Windows Version 8.0, Symantec introduced a new data source, Security: File System (Effective), to specifically address the group and user entitlement issue. In addition to the standard scoping options available for all of Symantec's File and Directory reporting, this new data source includes a specific Analysis Options Scoping page (updated with SP2).

By selecting various options as illustrated, a user can determine within reason the Accuracy Boundaries for the entitlement reporting options. There is no option to ignore a user's group membership or to ignore Deny ACEs, since this would put the accuracy boundaries beyond the scope of reason.



The top option button, Local analysis, sets the analysis to consider possible restrictions from a user's effective right to Logon locally when calculating effective permissions. Because these are effective rights calculations, eliminating this calculation has a positive impact on overall performance.

The second option button, Network analysis, sets the analysis to consider possible restrictions from the Access from Network right, Network Share existence and permissions, as well as the impact of the Bypass Traverse Checking right. Since these are effective rights calculations, selecting this calculation will have significant impact on overall performance.

The third option button, Local and network analysis, considers all rights, permissions and share paths. This will be the most time-consuming analysis option, but includes the tightest accuracy boundaries.

The fourth option, Security descriptor only, considers NTFS Permissions, Owner and effective group membership of Groups within the DACL. This will be the fastest option, but with the loosest accuracy boundaries.

The final option in this grouping, Security descriptor plus Backup, Restore, and Take Ownership privileges, is the best compromise between accuracy boundaries and performance. When this option is selected, all rights and permissions that can expand the permissions of groups and users are being considered; therefore, the results will never exclude a user or group with permissions, but may include users or groups whose access is restricted further via other controls.

The next grouping configures how data is presented. If only the Report groups check box is selected, Groups and their Nested Groups will be returned. If only the Report users check box is selected, all groups will be expanded to their effective members, and all directly assigned users will be included. In this case, the only groups that will appear in the results are those groups identified in the Do not report members of these groups section. If both options are selected, the results will include all users, including those derived from group membership and all groups, except those explicitly excluded with the Do not report members of these groups: Group Name field.

The option to Skip child objects with like permissions configures the analysis to compare the DACL (as a whole, ignoring inheritance tags) and Owner of a child file or directory with its parent. If the two are identical, the results for this file or directory are not returned in the result set.

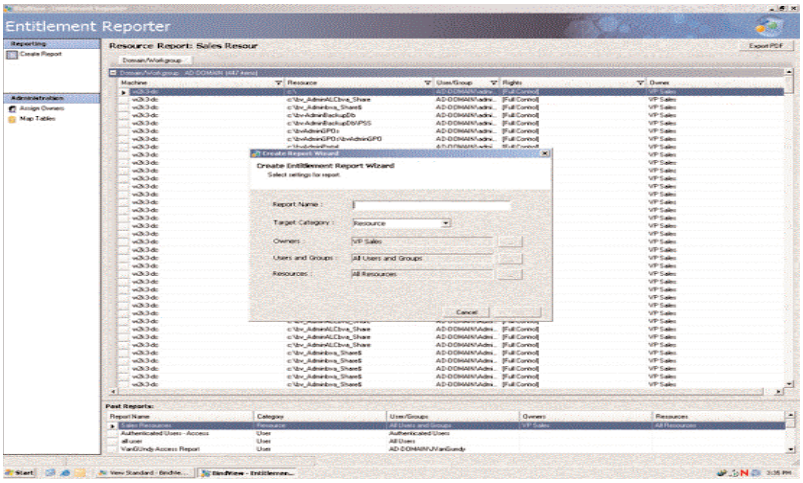
When the result set is sorted by user or group, this may produce somewhat confusing results. While an individual's permission to a directory may not be different, if any user or group's effective permissions for the directory are different, permission records will be returned to the report. This allows a report sorted by users to display parent and child directories with identical permissions for *that* user, to still appear in the results.

Once appropriate configurations have defined the level of analysis to be performed, the data can be collected using bv-Control. Given the large amount of data to be analyzed, organizations require an entitlements-focused interface to manage the information. Symantec

developed the Entitlement Reporter extension to bv-Control for Windows for this reason. This interface sits on top of a SQL Server database populated on a scheduled basis with the effective permissions information being gathered by bv-Control for Windows.

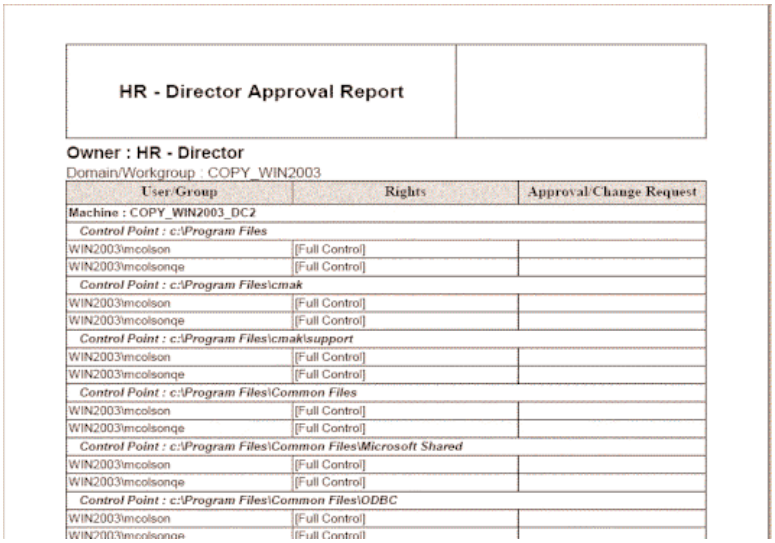
The Entitlement Reporter extension benefits:

1. Provides a drag-and-drop interface to sort the collected data and reduce the dataset to manageable levels.



2. Provides a database backend that allows organizations to incrementally scan their environment at non-peak hours, reducing production environment impact. At the same time, users can rapidly run reports on entitlements because all data is already collected and stored in the database.

3. Provides the ability to associate business owners to critical data. This greatly facilitates periodic process reviews of permissions grants by associating the appropriate control points for access to the business owners best able to validate these grants. These reports can be printed and signed-off on by the appropriate owners. The resulting documentation can be retained as evidence of a periodic review for compliance with regulations such as Sarbanes-Oxley or the Payment Card Industry Data Security Standard (PCI Standard).



HR - Director Approval Report

Owner : HR - Director

Domain/Workgroup : COPY_WIN2003

User/Group	Rights	Approval/Change Request
Machine : COPY_WIN2003_DC2		
Control Point : c:\Program Files		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	
Control Point : c:\Program Files\cmak		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	
Control Point : c:\Program Files\cmak\support		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	
Control Point : c:\Program Files\Common Files		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	
Control Point : c:\Program Files\Common Files\Microsoft Shared		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	
Control Point : c:\Program Files\Common Files\ODBC		
WIN2003\mcolson	[Full Control]	
WIN2003\mcolsonqe	[Full Control]	

Key Parameters To Consider When Evaluating Performance Of Large Number Of Domain Users

In an environment where there are 12,000 users (even when the user has selected not to list names in "Domain Users"), if a DACL or a machine-based right contains Domain Users the group's membership must be examined. In a large environment, enumerating Domain Users group membership takes time. Even if there are only a few directories, the report will pay an up-front time cost for gathering this information. Additional directories on that target requiring this information will not add to this "cost." The information is cached by the agent on a target machine basis.

Large Groups

If there are groups in the DACL with a large number of members, there is an additional cost with enumerating membership of these groups.

Deep Group Nesting

This factor can become convoluted since nested groups can have large memberships again which increase the cost for enumeration of its members.

Large Number of ACEs in DACL

Analyzing a DACL with many entries is another costly endeavor, not only due to the membership enumerations, but also because of the analysis of permissions and rights assignments for each ACE.

Number of Files and/or Directories

This factor will increase the cost of analysis, particularly when the permissions are different from parent directory to child directory, or if the option to Skip child objects with like permissions is not set, since every directory's DACL will be analyzed.

Rights Assignments

This factor can also increase processing time, since each group must be checked for its rights assignments in order to calculate accurate, effective permissions. It is unknown whether the number of rights assigned to a user or group will have an impact on processing.

Other Parameters To Consider In Performance Testing

Agent Memory Consumption

If there are a large number of groups, groups with many members, or directories with Domain Users granted access, the memory footprint of each agent will be large. In large environments (30,000 users), this footprint can be 40 MB or more per agent. In a much larger environment (100,000 users), this footprint can be more than 100 MB per agent. Unlike any other report, a single default, 6 DCA QE, can consume more than 500 MB of memory if asked to generate a report with a poorly defined scope. If the installation has been tuned to allow 15 agents per QE, or perhaps 30, as is often the case, a poorly defined query in a very large environment can drive a QE to consume 3 gigabytes of memory.

CPU Utilization on the QE

There are no other queries that even remotely require the CPU agent calculations of effective permissions. As you can tell from the details involved above, the CPU has its work cut out for it. If you have a large number of agents configured for a QE and an entitlement report is run against many targets, a QE will become severely stressed—even if it's a quad-processor box.

Availability of the Target Server

The ability of the target server to respond to requests in a timely fashion may be another performance factor. If the server or domain controller is too busy to handle the requests in a timely fashion, data collection could be delayed.

Scope And License Considerations

Scoping

Throughout this document, scoping (exclusively targeting specific directories and machines) has been utilized as a method to increase performance and prevent information overload. Additionally, the user's ability to restrict the scope of the analysis (eliminating analysis of certain rights, etc.) has also been discussed as another methodology for increasing performance.

Sample Based Reporting is another scoping-related method for performance improvement and workload reduction often used by the auditing community. bv-Control allows the user to do Sample Based Reporting by scoping to a sample of the target machines. Sampling auditing involves taking a random sample of some percentage (20%, 30%, etc.) of the network machines, auditing those in detail, and extrapolating the results to the whole.

License Considerations

While scoping is intended to increase performance and limit extraneous data, it is not intended to circumvent the need for complete bv-Control license coverage. Symantec target licenses are not based on a single report scope or concurrent reporting scope; they are based on aggregate use.

Specifically, bv-Control licenses are required for every machine and every user that could or will be reported on. As an example, it is beyond the scope of the licenses to report on a sample of 100 servers this quarter and a different sample of 100 servers next quarter, unless all 200 servers are licensed. Servers that are never reported against, such as test servers and utility servers that could pose no threat to the environment, can certainly be excluded from license requirements.

In addition to bv-Control for Windows licenses, organizations using the Entitlement Reporter extension will require a short, Professional Services engagement. This engagement cost will be based on the scope of work to be accomplished and will be charged on a time-and-materials basis. The Entitlement Reporter software is a free extension to bv-Control for Windows. The professional services requirement exists only to help customers appropriately query and gather the right permissions information to be stored within Entitlement Reporter. As outlined in this white paper, the considerations surrounding the defininition of configurations for reporting on effective permissions are complex. History has demonstrated that customers benefit greatly from a short duration services engagement, during which time Symantec consultants work with the customer to define the information to be collected and optimize the collection process.

Understanding Data Source Licenses

bv-Control for Windows is licensed with two basic target licenses: MACHINE and USER. Each of the 20+ Symantec reporting data sources targets either information from Active Directory® (or a Legacy NT SAM) or a machine. The Symantec reporting specifically discussed in this document is based on the four Security data sources, all of which are licensed on a MACHINE target basis. While these reports do identify specific users and groups with directory and file access, the primary targets of these reports are machines and directories. Other data sources are required to specifically list user and group properties, such as reporting effective group membership and user last login dates. In order to use bv-Control for Windows to report on specific properties of users and groups in AD and Legacy NT environments, USER licenses are required.

As another example, in the Services data source the primary target is a machine and the services installed on it. Although there may be an AD account associated with a service, because this data source is machine-based, machine licenses (either Server or Workstation, depending on the OS running on the machine) are required. Other data sources that utilize machine licenses include Services, Volumes, Shares, Directories, Files and Event Logs.

About Symantec

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, California, Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517-8000
1 (800) 721-3934
www.symantec.com

10526866