BINDVIEW® Insight at Work

Evaluation Guide

bv-Control® for NDS® eDirectory™

Policy Compliance | Vulnerability Management | Directory Administration & Migration

bv-Control®
for NDS® eDirectory™ v8.00

Evaluation Guide

BindView Corporation · 5151 San Felipe, Suite 2500 · Houston, TX 77056

COPYRIGHT

TRADEMARK NOTES

July 2004

Contents

Introduction 9
Features Overview 10
Identifying and Closing Security Holes: Using Pre-Defined Reports 11
Scenario 1 Retrieving DirXML Information 11
Scenario 2 User Security 13
Auditing and Documenting Compliance: Evaluating Standards 18
Scenario 3 Intruder Detection 18
Simplifying Data Analysis: Extending Reporting Capabilities 20
Scenario 4 Hidden Objects 20
Conclusion 22
Contacting BindView 23

Introduction

bv-Control® for NDS® eDirectory™ is a comprehensive solution for proactively assessing, securing, and managing your NDS eDirectory environment. As part of the BindView Vulnerability Management family of solutions, it provides in-depth reporting as well as closed-loop problem identification and remediation. Using bv-Control for NDS eDirectory, you can audit and document compliance of corporate policies, identify and close security holes, perform configuration management, and assess NDS Trustee assignments. You can also view and manage trees, containers, groups, users and other objects in NDS eDirectory.

About This Guide

This bv-Control for NDS eDirectory Evaluation Guide is designed to guide you through an evaluation process that demonstrates key features of this product. After installing and configuring bv-Control for NDS eDirectory, you can proceed through scenarios that are intended to give you a brief, hands-on tour of specific functionality highlights.

Features Overview

The following chart provides a quick overview of the key features of bv-Control for NDS eDirectory and how they can help you administer and secure your NDS eDirectory environment:

Features	Benefits
	Identify and Close Security Holes
Pre-Defined Reports	Using the many out-of-the-box reports, you can identify conditions that threaten the security of your enterprise, and increase productivity by reducing the IT administrator's learning curve.
Custom Reports	The query-based interface allows you to easily build custom queries that are specific to particular corporate policies and procedures.
Effective Rights Analysis	You can identify who has access to data and how it was obtained, perform enterprise-wide effective rights analysis on NDS objects, provide critical information about hidden objects, locate and delete stale accounts, and find and eliminate password problems.
Easy-to-view Reports	Simplify Problem resolution by making changes to eDirectory from within a report. This feature enables you to enforce fast and efficient changes across a diverse IT environment.
	Audit and Document Compliance
Site Standards	Create Gold standards for group membership, security equivalencies, account restrictions, password restrictions and log-time restrictions. You can then compare the entire enterprise against those standards to help ensure compliance.
	Perform Configuration Management
Disk Space Analysis	Identify how much space is available and how much is in use for all volumes, find stale or unused user accounts and delete them, and find and delete inappropriate files in users' home directories.
	Simplify Documentation and Data Analysis
Discrepancy Analysis	View the enterprise from a historical perspective for future planning.
Extended Auditing and Reporting Capabilities	Audit and report in DirXML and iManager RBS roles and tasks. This capability increases NDS eDirectory efficiency and quickens enterprise-wide system compatibility.

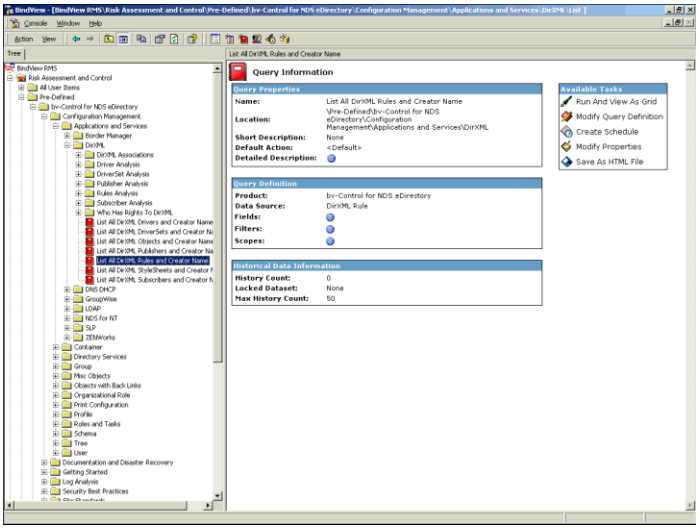
Identifying and Closing Security Holes: Using Pre-Defined Reports

Scenario 1: Retrieving DirXML Information

Disaster recovery documentation may include the DirXML implementation and configuration. This type of information should be collected periodically and placed in an accessible location should a disaster occur and disaster recovery be initiated. bv-Control provides the ability to present this information in hardcopy or electronic format, which can be printed or exported in any of twenty-four formats. This scenario illustrates how to execute a pre-defined query and print the results.

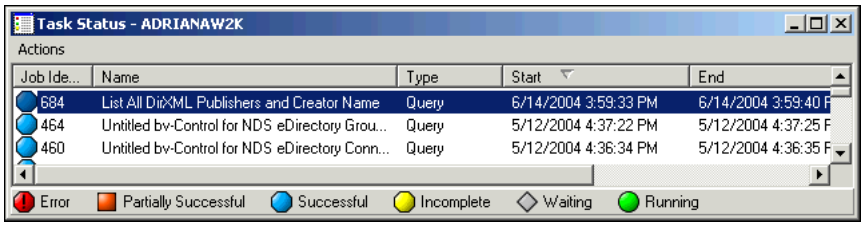
▶ ***To execute a query***

1 Navigate to the **List All DirXML Rules and Creator Name** pre-defined query in the **BindView RMS** folder by using the following path: **BindView RMS>Risk Assessment and Control>Pre-Defined>bv-Control for NDS eDirectory>Configuration Management>Applications and Services>DirXML>List All DirXML Rules and Creator Name**.

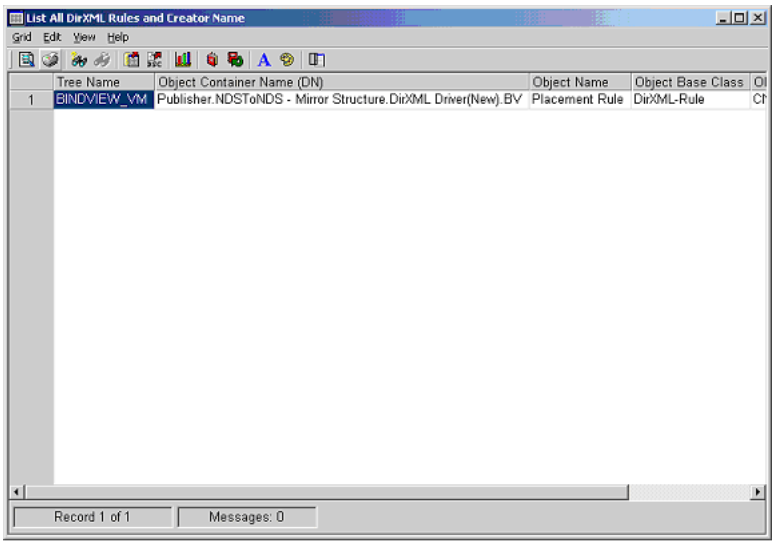


2 Right-click **List All DirXML Rules and Creator Name** in the **Tree** pane and select **Run>And View as Grid** to execute the query. Alternatively, you can click **Run And View As Grid** from the **Available Tasks** pane of the left-hand console window.

The **Task Status** window appears and shows the status of any queries currently being executed and any which have been previously executed without saving the dataset to the query binder.



When the query has successfully executed, the dataset is displayed.

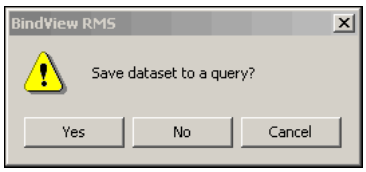


▶ *To print a dataset*

3 Select the printer  icon from the toolbar of the dataset.

4 Review the settings in the printer dialog that appears and click **OK** to print the dataset.

5 Close the dataset window and click **No** in response to the **Save dataset** dialog.



Selecting **No** will keep the query you have run in the **Task Status** window for future reference and allows you to review the dataset at anytime without re-running the query. To review a non-saved dataset, double-click any previously run query in the **Task Status** window.

Selecting **Yes** removes the query from the **Task Status** window and places the historical data in the query binder. From the query binder, you can access historical data by right-clicking on the query and selecting **Manage>Historical Data** from the sub-menu.

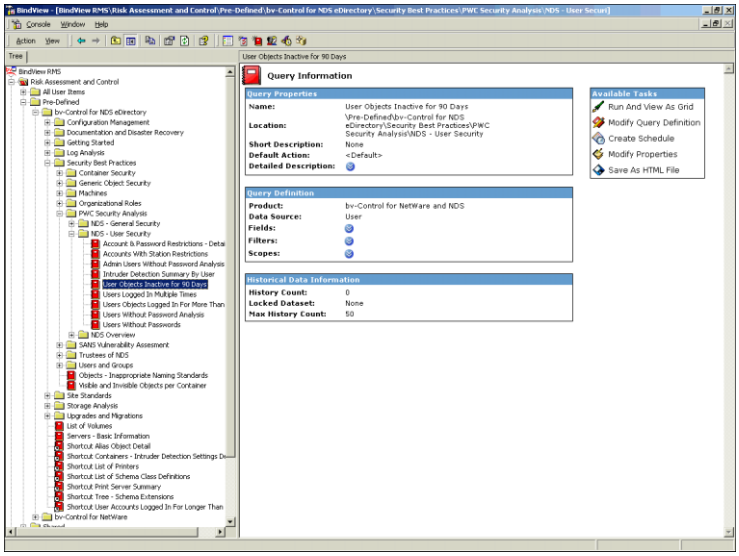
For more information on managing historical data and the options available, see the *bv-Control for NDS eDirectory User Guide.*

Scenario 2: User Security

A variety of user security parameters exist that should be verified to ensure security and compliance with best practices. These include such password settings as minimum password length and expiration frequency, as well as identifying accounts which have not been used within a given time frame. This scenario illustrates how to modify a pre-defined query to meet your specific needs and how to save the changes for future use. You will then make a change to the enterprise and utilize the baseline feature to illustrate the changes made.

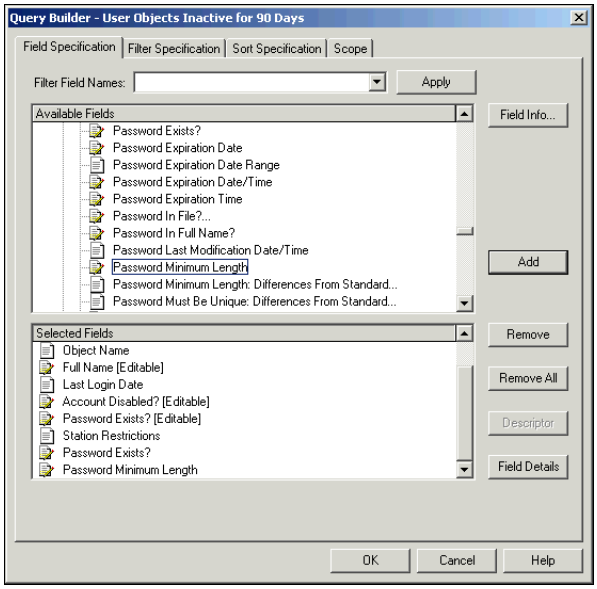
▶ *To modify a pre-defined query*

1 Navigate to the **User Objects Inactive for 90 Days** pre-defined query in the **BindView RMS** folder by using the following path: **BindView RMS>Risk Assessment and Control>Pre-Defined>bv-Control for NDS eDirectory>Security Best Practices>PWC Security Analysis>NDS-User Security>User Objects Inactive for 90 Days**.



2 Right-click the query to access the sub-menu and select **Settings>Query Definition**.

The **Query Builder** dialog appears.



3 Click the **Field Specification** tab.

4 Expand the **All Fields** folder and select the **Password Exists?** and **Password Minimum Length** fields.

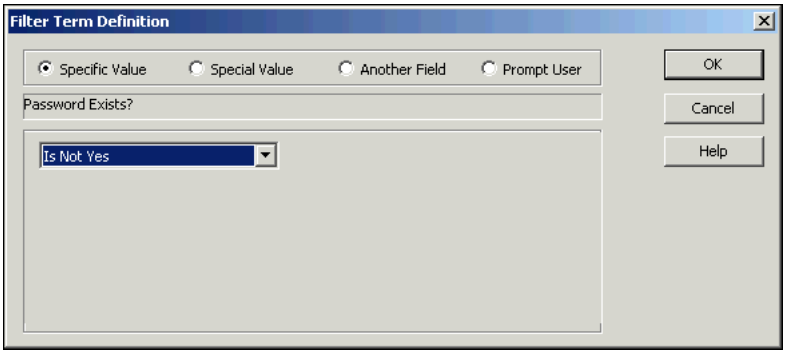
5 Click **Add**.

6 Click the **Filter Specification** tab to modify the criteria used for selecting which records will appear on the report.

7 Expand the **All Fields** folder and select the **Password Exists?** field.

8 Click **Add**.

The **Filter Term Definition** dialog appears.



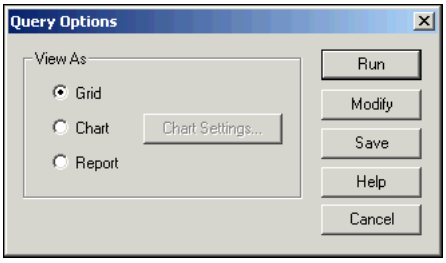
9 Select **Is Not Yes** from the drop-down box.

10 Click **OK**.

The new criteria is displayed in the lower pane of the **Query Builder** dialog on the **Filter Specification** tab.

11 Click **OK**.

The **Query Options** dialog appears.



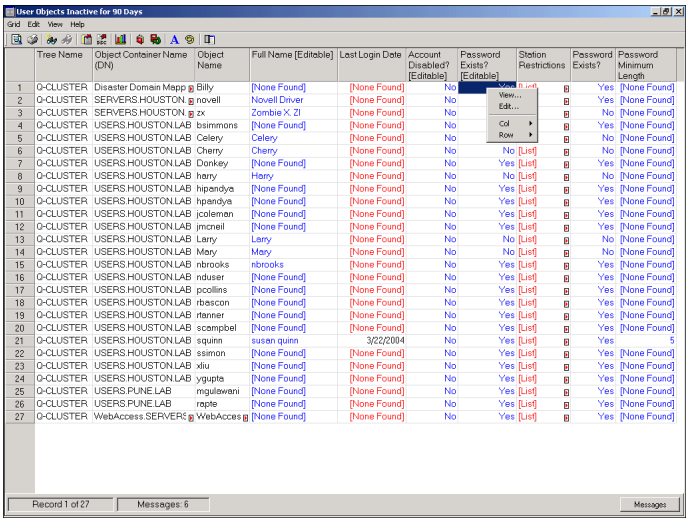
12 Click **Save** and save the modified query in the **My Items** folder with a name of your choosing.

A copy of the modified query is saved for future reference and use.

▶ *To perform and review enterprise changes within a dataset*

13 From the **Query Options** dialog, click **Run** with **View As Grid** selected.

A dataset appears listing all users whose accounts are either inactive or have no password.

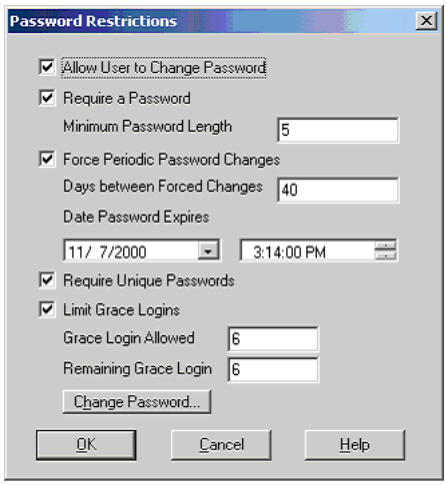


14 Choose a user from the list whose account you can safely modify and click the **Password Minimum Length** cell which corresponds to that user.

15 Right-click on the cell and select **Edit** from the sub-menu to open the **Password Restrictions** dialog.

The **Password Restrictions** dialog appears, allowing you to make changes to your enterprise from within the bv-Control dataset.

If you receive a message stating that information needs to be queried, click **Yes**.

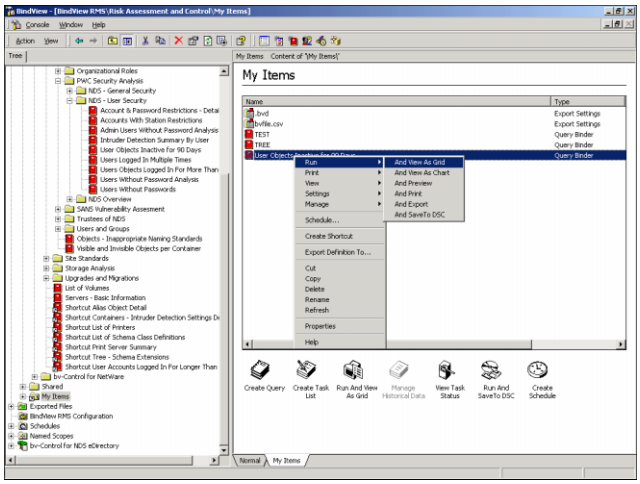


16 Change the default value in the **Minimum Password Length** text box to 4 and click **OK**.

17 Click **Yes**.

An administrative job is initiated which writes the change you have made to NDS. While you are changing only a single user in this scenario, it is possible to select multiple users or all users appearing on the report, and make changes to each simultaneously.

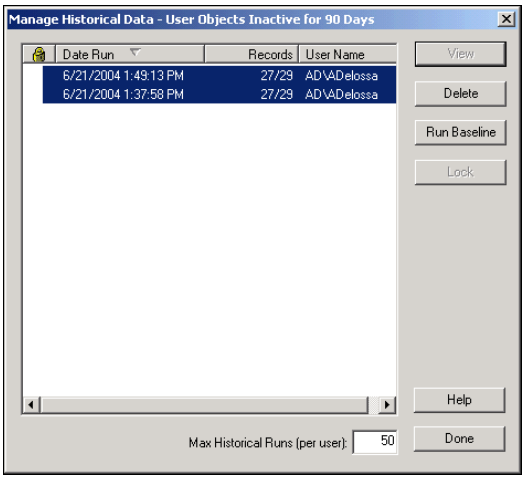
18 When the administrative job is completed, re-run the query by right-clicking the query you saved to the **My Items** folder in step 12 and selecting **Run>And View as Grid** from the sub-menu.



19 Close both queries and click **Yes** to save the datasets to the query binder.

20 Right-click the saved query and select **Manage>Historical Data** from the sub-menu.

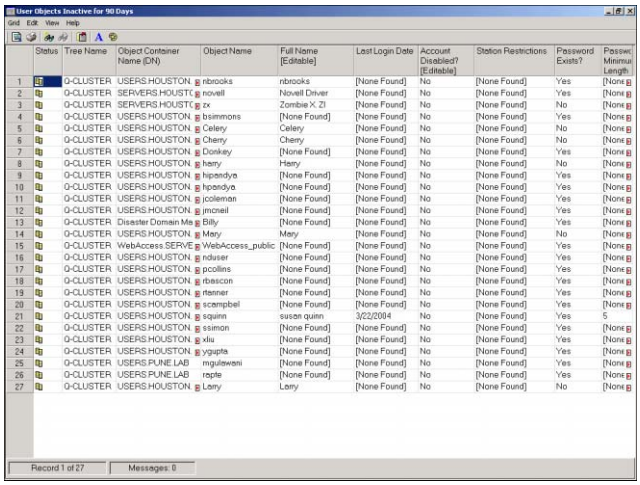
The **Manage Historical Data** dialog appears.



21 Select both queries and click **Run Baseline**.

22 Accept the default options, and click **OK**.

The baseline dataset appears.



23 Pause the mouse cursor over the red arrow that appears in the **Password Minimum Length** field.

The old and new values are displayed for review, allowing you to determine changes to the enterprise at a glance.

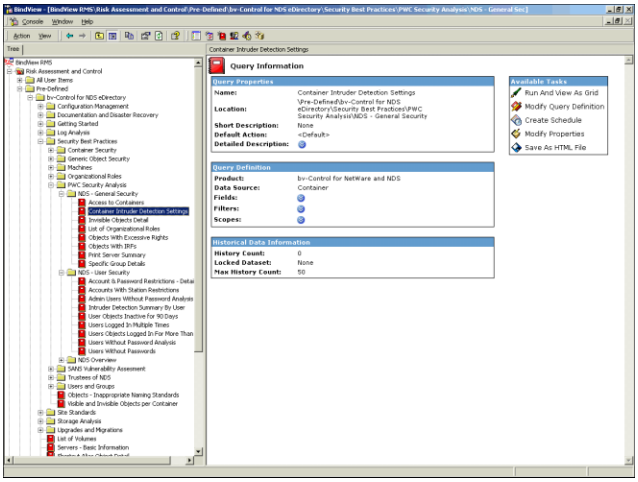
Auditing and Documenting Compliance: Evaluating Standards

Scenario 3: Intruder Detection

Intruder Detection settings are an important aspect of NDS security. They allow administrators to place restrictions on the number of incorrect attempts a user may perform when entering a password. Once the number of incorrect attempts has been exceeded the account is locked. bv-Control for NDS eDirectory offers not only the ability to report on these settings, but also a method for modifying the settings on multiple containers simultaneously.

▶ ***To customize the scope of an existing query***

1 Navigate to the **Container Intruder Detection Settings** pre-defined query in the **BindView RMS** folder by using the following path: **BindView RMS>Risk Assessment and Control>Pre-Defined>bv-Control for NDS eDirectory>Security Best Practices>PWC Security Analysis>NDS-General Security>Container Intruder Detection Settings**.

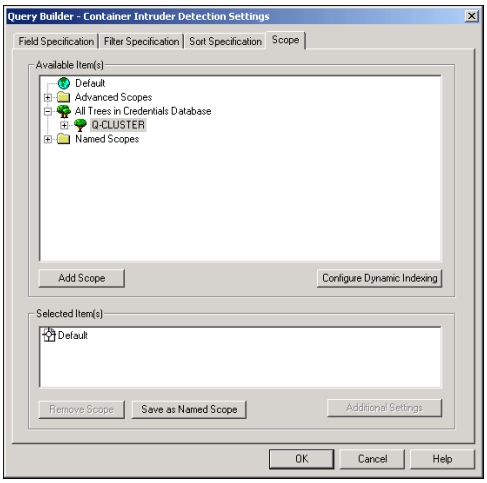


2 Right-click the query and select **Settings>Query Definition** from the sub-menu.

3 The **Query Builder** dialog appears.

4 Click the **Scope** tab.

5 Select a location on which to execute the query.



6 Click **OK**.

The **Query Options** dialog appears.

7 Click **Run** with the **View As Grid** option selected.

The **Container Intruder Detection Settings** dataset appears.

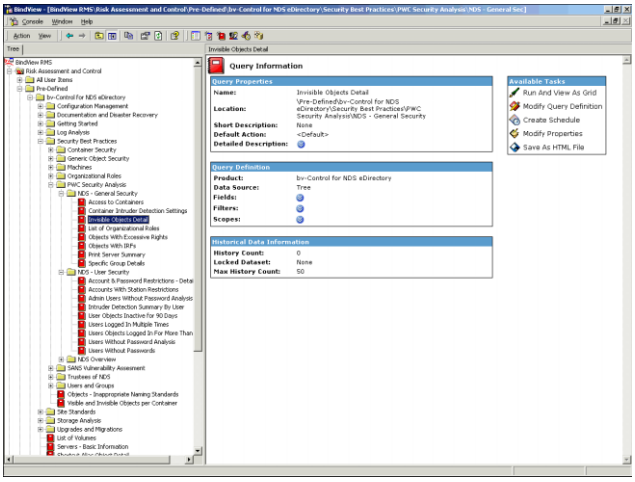
8 Close the dataset without saving the information.

Simplifying Data Analysis: Extending Reporting Capabilities

Scenario 4: Hidden Objects

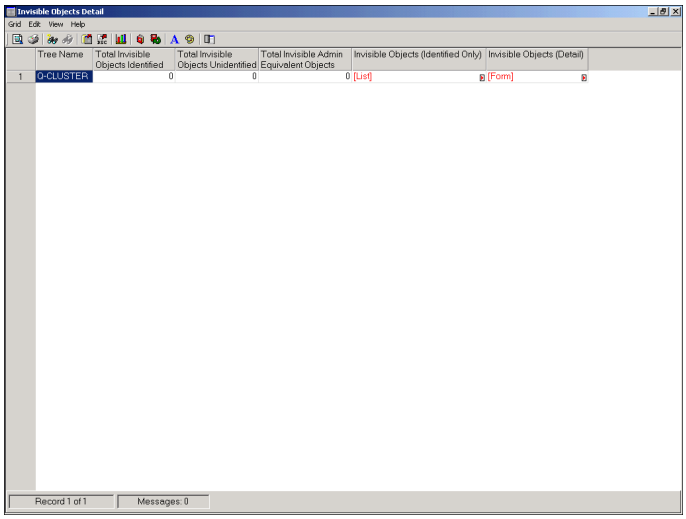
Hidden objects may represent serious security issues with your network and are often used by hackers as a means of creating a backdoor for future possible exploitation. These objects are created in such a way as to be inaccessible to other users. Although these objects are often vulnerabilities, there are other reasons objects may be invisible. The main purpose of this query is to bring awareness to the administrators of the existence of objects which have escaped administration.

1 Navigate to the **Invisible Objects Detail** pre-defined query in the **BindView RMS** folder by using the following path: **BindView RMS>Risk Assessment and Control>Pre-Defined>bv-Control for NDS eDirectory>Security Best Practices>PWC Security Analysis>NDS-General Security>Invisible Objects Detail**.

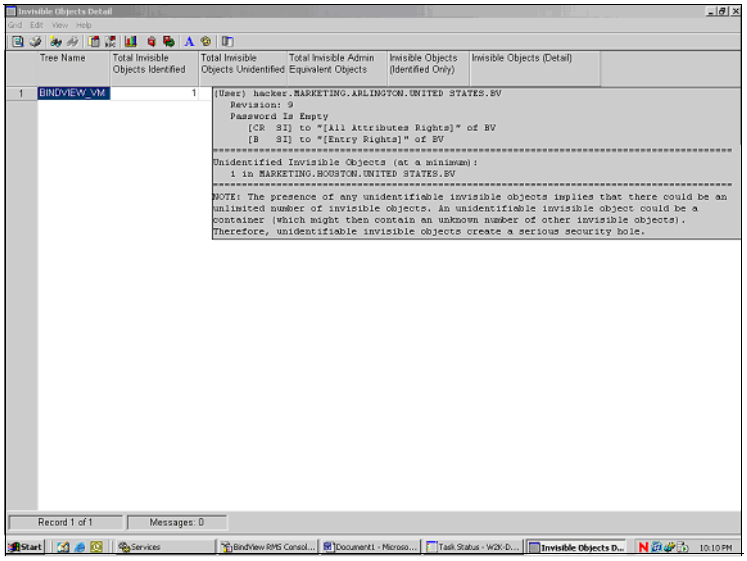


2 Right-click **Invisible Objects Detail** in the **Tree** pane and select **Run>And View as Grid** to execute the query. Alternatively, you can click **Run And View As Grid** from the **Available Tasks** pane of the right-hand console window.

The **Invisible Objects Detail** dataset appears.



3 Pause the mouse cursor over the red arrow in the **Invisible Objects (Detail)** column to view the field details.



From the dataset, you can view expanded information on the selected User object. In this case, the password is empty and the rights assigned to the user over NDS objects are detailed.

4 Close the dataset without saving the information.

Conclusion

The information provided in this Evaluation Guide covers only a few of the features of bv-Control for NDS eDirectory. However, the scenarios give you an idea of how bv-Control for NDS eDirectory can help you assess, secure and manage your NDS eDirectory environment. As part of the BindView Vulnerability Management solutions family, bv-Control for NDS eDirectory assists organizations in properly configuring and protecting the NDS eDirectory environment, avoiding unplanned downtime and realizing a desired return on IT investments.

Contacting BindView

BindView has sales and support offices around the world. For information on contacting BindView, please refer to the information below or to the BindView Web site: ***www.bindview.com***

For Technical Support: ***www.bindview.com/support***

Technical Support is available Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Time. Normal working hours for all other departments are 9:00 a.m. to 6:00 p.m.

Phone		
Sales and Customer Service	U.S. and Canada	800-813-5869
	Outside N. America	713-561-4000
Technical Support	U.S. and Canada	800-813-5867
	Outside N. America	713-561-4000
Training/Professional Service	U.S. and Canada	800-749-8439
	Outside N. America	713-561-4000

Fax	All Areas	713-561-1000

E-mail	
Sales	sales@bindview.com
Training	edu@bindview.com
Documentation	docs@bindview.com

Other	
FTP Site	ftp://ftp.bindview.com
Internet	www.bindview.com
Postal Mail	BindView 5151 San Felipe, Suite 2500 Houston, TX 77056