

Symantec bv-Control[®] for NDS[®] eDirectory[™] 10.0 Getting Started Guide



Symantec bv-Control for NDS eDirectory 10.0 Getting Started Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 10.0

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, BindView, and bv-Control are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID, SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights” and DFARS 227.7202, “Rights in Commercial Computer Software or Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- n A range of support options that give you the flexibility to select the right amount of service for any size organization
- n Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- n Upgrade assurance that delivers software upgrades
- n Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- n Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- n Product release level

- n Hardware information
- n Available memory, disk space, NIC information
- n Operating system
- n Version and patch level
- n Network topology
- n Router, gateway, and IP address information
- n Problem description:
 - n Error messages and log files
 - n Troubleshooting that was performed before contacting Symantec
 - n Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- n Questions regarding product licensing or serialization
- n Product registration updates, such as address or name changes
- n General product information (features, language availability, local dealers)
- n Latest information about product updates and upgrades
- n Information about upgrade assurance and support contracts
- n Information about the Symantec Buying Programs
- n Advice about Symantec's technical support options
- n Nontechnical presales questions
- n Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customer care_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Symantec Corporation Software License Agreement

SYMANTEC CORPORATION AND/OR ITS AFFILIATES (“SYMANTEC”) IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT (“LICENSE AGREEMENT”). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED SOFTWARE PACKAGE, BREAKING THE LICENSED SOFTWARE SEAL, CLICKING THE “I AGREE” OR “YES” BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE LICENSED SOFTWARE OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE “I DO NOT AGREE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE LICENSED SOFTWARE. UNLESS OTHERWISE DEFINED HEREIN, CAPITALIZED TERMS WILL HAVE THE MEANING GIVEN IN THE “DEFINITIONS” SECTION OF THIS LICENSE AGREEMENT AND SUCH CAPITALIZED TERMS MAY BE USED IN THE SINGULAR OR IN THE PLURAL, AS THE CONTEXT REQUIRES.

1. Definitions:

“Content Updates” means content used by certain Symantec products which is updated from time to time, including but not limited to: updated anti-spyware definitions for anti-spyware products; updated antispam rules for antispam products; updated virus definitions for antivirus and crimeware products; updated URL lists for content filtering and antiphishing products; updated firewall rules for firewall products; updated intrusion detection data for intrusion detection products; updated lists of authenticated web pages for website authentication products; updated policy compliance rules for policy compliance products; and updated vulnerability signatures for vulnerability assessment products.

“Documentation” means the user documentation Symantec provides with the Licensed Software.

“License Instrument” means one or more of the following applicable documents which further defines Your license rights to the Licensed Software: a Symantec license certificate or a similar license document issued by Symantec, or a written agreement between You and Symantec, that accompanies,

precedes or follows this License Agreement.

“Licensed Software” means the Symantec software product, in object code form, accompanying this License Agreement, including any Documentation included in, or provided for use with, such software or that accompanies this License Agreement.

“Support Certificate” means the certificate sent by Symantec confirming Your purchase of the applicable Symantec maintenance/support for the Licensed Software.

“Upgrade” means any version of the Licensed Software that has been released to the public and which replaces the prior version of the Licensed Software on Symantec’s price list pursuant to Symantec’s then-current upgrade policies.

“Use Level” means the license use meter or model (which may include operating system, hardware system, application or machine tier limitations, if applicable) by which Symantec measures, prices and licenses the right to use the Licensed Software, in effect at the time an order is placed for such Licensed Software, as indicated in this License Agreement and the applicable License Instrument.

2. License Grant:

Subject to Your compliance with the terms and conditions of this License Agreement, Symantec grants to You the following rights: (i) a non-exclusive, non-transferable (except as stated otherwise in Section 16.1) license to use the Licensed Software solely in support of Your internal business operations in the quantities and at the Use Levels described in this License Agreement and the applicable License Instrument; and (ii) the right to make a single uninstalled copy of the Licensed Software for archival purposes which You may use and install for disaster-recovery purposes (i.e. where the primary installation of the Licensed Software becomes unavailable for use).

2.1. Term:

The term of the Licensed Software license granted under this License Agreement shall be perpetual (subject to Section 14) unless stated otherwise in Section 17 or unless You have obtained the Licensed Software on a non-perpetual basis, such as, under a subscription or term-based license for the period of time indicated on the applicable License Instrument. If You have obtained the Licensed Software on a non-perpetual basis, Your rights to use such Licensed Software shall end on the applicable end date as indicated on the applicable License Instrument and You shall cease use of the Licensed Software as of such applicable end date.

3. License Restrictions:

You may not, without Symantec's prior written consent, conduct, cause or permit the: (I) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software except as expressly provided in this License Agreement; (ii) creation of any derivative works based on the Licensed Software; (iii) reverse engineering, disassembly, or decompiling of the Licensed Software (except that You may decompile the Licensed Software for the purposes of interoperability only to the extent permitted by and subject to strict compliance under applicable law); (iv) use of the Licensed Software in connection with service bureau, facility management, timeshare, service provider or like activity whereby You operate or use the Licensed Software for the benefit of a third party; (v) use of the Licensed Software by any party other than You; (vi) use of a later version of the Licensed Software other than the version that accompanies this License Agreement unless You have separately acquired the right to use such later version through a License Instrument or Support Certificate; nor (vii) use of the Licensed Software above the quantity and Use Level that have been licensed to You under this License Agreement or the applicable License Instrument.

4. Ownership/Title:

The Licensed Software is the proprietary property of Symantec or its licensors and is protected by copyright law. Symantec and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Your rights to use the Licensed Software shall be limited to those expressly granted in this License Agreement. All rights not expressly granted to You are retained by Symantec and/or its licensors.

5. Content Updates:

If You purchase a Symantec maintenance/support offering consisting of or including Content Updates, as indicated on Your Support Certificate, You are granted the right to use, as part of the Licensed Software, such Content Updates as and when they are made generally available to Symantec's end user customers who have purchased such maintenance/support offering and for such period of time as indicated on the face of the applicable Support Certificate. This License Agreement does not otherwise permit You to obtain and use Content Updates.

6. Upgrades/Cross-Grades:

Symantec reserves the right to require that any upgrades (if any) of the Licensed Software may only be obtained in a quantity equal to the number indicated

on the applicable License Instrument. An upgrade to an existing license shall not be deemed to increase the number of licenses which You are authorized to use. Additionally, if You upgrade a Licensed Software license, or purchase a Licensed Software license listed on the applicable License Instrument to cross-grade an existing license (i.e. to increase its functionality, and/or transfer it to a new operating system, hardware tier or licensing meter), then Symantec issues the applicable Licensed Instrument based on the understanding that You agree to cease using the original license. Any such license upgrade or cross-grade is provided under Symantec's policies in effect at the time of order. This License Agreement does not separately license You for additional licenses beyond those which You have purchased, and which have been authorized by Symantec as indicated on the applicable License Instrument.

7. Limited Warranty:

7.1. Media Warranty:

If Symantec provides the Licensed Software to You on tangible media, Symantec warrants that the magnetic media upon which the Licensed Software is recorded will not be defective under normal use, for a period of ninety (90) days from delivery. Symantec will replace any defective media returned to Symantec within the warranty period at no charge to You. The above warranty is inapplicable in the event the Licensed Software media becomes defective due to unauthorized use of the Licensed Software. **THE FOREGOING IS YOUR SOLE AND EXCLUSIVE REMEDY FOR SYMANTEC'S BREACH OF THIS WARRANTY.**

7.2. Performance Warranty:

Symantec warrants that the Licensed Software, as delivered by Symantec and when used in accordance with the Documentation, will substantially conform to the Documentation for a period of ninety (90) days from delivery. If the Licensed Software does not comply with this warranty and such non-compliance is reported by You to Symantec within the ninety (90) day warranty period, Symantec will do one of the following, selected at Symantec's reasonable discretion: either (I) repair the Licensed Software, (ii) replace the Licensed Software with software of substantially the same functionality, or (iii) terminate this License Agreement and refund the relevant license fees paid for such non-compliant Licensed Software. The above warranty specifically excludes defects resulting from accident, abuse, unauthorized repair, modifications or enhancements, or misapplication. **THE FOREGOING IS YOUR SOLE AND EXCLUSIVE**

REMEDY FOR SYMANTEC'S BREACH OF THIS WARRANTY.

8. Warranty Disclaimers:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE WARRANTIES SET FORTH IN SECTIONS 7.1 AND 7.2 ARE YOUR EXCLUSIVE WARRANTIES AND ARE IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. SYMANTEC MAKES NO WARRANTIES OR REPRESENTATIONS THAT THE LICENSED SOFTWARE, CONTENT UPDATES OR UPGRADES WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OR USE OF THE LICENSED SOFTWARE, CONTENT UPDATES, AND UPGRADES WILL BE UNINTERRUPTED OR ERROR-FREE. YOU MAY HAVE OTHER WARRANTY RIGHTS, WHICH MAY VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

9. Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS, RESELLERS, SUPPLIERS OR AGENTS BE LIABLE TO YOU FOR (I) ANY COSTS OF PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS AND SERVICES, LOSS OF PROFITS, LOSS OF USE, LOSS OF OR CORRUPTION TO DATA, BUSINESS INTERRUPTION, LOSS OF PRODUCTION, LOSS OF REVENUES, LOSS OF CONTRACTS, LOSS OF GOODWILL, OR ANTICIPATED SAVINGS OR WASTED MANAGEMENT AND STAFF TIME; OR (ii) ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES WHETHER ARISING DIRECTLY OR INDIRECTLY OUT OF THIS LICENSE AGREEMENT, EVEN IF SYMANTEC OR ITS LICENSORS, RESELLERS, SUPPLIERS OR AGENTS HAS BEEN ADVISED SUCH DAMAGES MIGHT OCCUR. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE FEES YOU PAID FOR THE LICENSED SOFTWARE GIVING RISE TO THE CLAIM. NOTHING IN THIS AGREEMENT SHALL OPERATE SO AS TO EXCLUDE OR LIMIT SYMANTEC'S LIABILITY TO YOU FOR DEATH OR PERSONAL INJURY ARISING OUT OF NEGLIGENCE OR FOR ANY OTHER LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED BY LAW. THE DISCLAIMERS AND LIMITATIONS SET FORTH ABOVE WILL APPLY REGARDLESS OF WHETHER OR NOT YOU ACCEPT THE LICENSED SOFTWARE, CONTENT UPDATES OR UPGRADES.

10. Maintenance/Support:

Symantec has no obligation under this License Agreement to provide maintenance/support for the Licensed Software. Any maintenance/support purchased for the Licensed Software is subject to Symantec's then-current maintenance/support policies.

11. Software Evaluation:

If the Licensed Software is provided to You for evaluation purposes and You have an evaluation agreement with Symantec for the Licensed Software, Your rights to evaluate the Licensed Software will be pursuant to the terms of such evaluation agreement. If You do not have an evaluation agreement with Symantec for the Licensed Software and if You are provided the Licensed Software for evaluation purposes, the following terms and conditions shall apply. Symantec grants to You a nonexclusive, temporary, royalty-free, non-assignable license to use the Licensed Software solely for internal non-production evaluation. Such evaluation license shall terminate (I) on the end date of the pre-determined evaluation period, if an evaluation period is pre-determined in the Licensed Software or (ii) sixty (60) days from the date of Your initial installation of the Licensed Software, if no such evaluation period is pre-determined in the Licensed Software ("Evaluation Period"). The Licensed Software may not be transferred and is provided "AS IS" without warranty of any kind. You are solely responsible to take appropriate measures to back up Your system and take other measures to prevent any loss of files or data. The Licensed Software may contain an automatic disabling mechanism that prevents its use after a certain period of time. Upon expiration of the Licensed Software Evaluation Period, You will cease use of the Licensed Software and destroy all copies of the Licensed Software. All other terms and conditions of this License Agreement shall otherwise apply to Your evaluation of the Licensed Software as permitted herein.

12. U.S. Government Restricted Rights:

The Licensed Software is deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Licensed Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Licensed Software or Commercial Computer Licensed Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software by the U.S. Government shall be

solely in accordance with the terms of this License Agreement.

13. Export Regulation:

You acknowledge that the Licensed Software and related technical data and services (collectively "Controlled Technology") are subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. You agree to comply with all relevant laws and will not to export any Controlled Technology in contravention to U.S. law nor to any prohibited country, entity, or person for which an export license or other governmental approval is required. All Symantec products, including the Controlled Technology are prohibited for export or re-export to Cuba, North Korea, Iran, Syria and Sudan and to any country subject to relevant trade sanctions. You hereby agree that You will not export or sell any Controlled Technology for use in connection with chemical, biological, or nuclear weapons, or missiles, drones or space launch vehicles capable of delivering such weapons.

14. Termination:

This License Agreement shall terminate upon Your breach of any term contained herein. Upon termination, You shall immediately stop using and destroy all copies of the Licensed Software.

15. Survival:

The following provisions of this License Agreement survive termination of this License Agreement: Definitions, License Restrictions and any other restrictions on use of intellectual property, Ownership/Title, Warranty Disclaimers, Limitation of Liability, U.S. Government Restricted Rights, Export Regulation, Survival, and General.

16. General:

16.1. Assignment:

You may not assign the rights granted hereunder or this License Agreement, in whole or in part and whether by operation of contract, law or otherwise, without Symantec's prior express written consent.

16.2. Compliance With Applicable Law:

You are solely responsible for Your compliance with, and You agree to comply with, all applicable laws, rules, and regulations in connection with Your use of the Licensed Software.

16.3. Audit:

An auditor, selected by Symantec and reasonably acceptable to You, may, upon reasonable notice and during normal business hours, but not more often than once each year, inspect Your records and deployment in order to confirm that Your use of the Licensed Software complies with this License Agreement and the applicable License Instrument. Symantec shall bear the costs of any such audit, except where the audit demonstrates that the Manufacturer's Suggested Reseller Price (MSRP) value of Your non-compliant usage exceeds five percent (5%) of the MSRP value of Your compliant deployments. In such case, in addition to purchasing appropriate licenses for any over-deployed Licensed Software, You shall reimburse Symantec for the auditor's reasonable actual fees for such audit.

16.4. Governing Law; Severability; Waiver:

If You are located in North America or Latin America, this License Agreement will be governed by the laws of the State of California, United States of America. If you are located in China, this License Agreement will be governed by the laws of the Peoples Republic of China. Otherwise, this License Agreement will be governed by the laws of England. Such governing laws are exclusive of any provisions of the United Nations Convention on Contracts for Sale of Goods, including any amendments thereto, and without regard to principles of conflicts of law. If any provision of this License Agreement is found partly or wholly illegal or unenforceable, such provision shall be enforced to the maximum extent permissible, and remaining provisions of this License Agreement shall remain in full force and effect. A waiver of any breach or default under this License Agreement shall not constitute a waiver of any other subsequent breach or default.

16.5. Third Party Programs:

This Licensed Software may contain third party software programs ("Third Party Programs") that are available under open source or free software licenses. This License Agreement does not alter any rights or obligations You may have under those open source or free software licenses. Notwithstanding anything to the contrary contained in such licenses, the disclaimer of warranties and the limitation of liability provisions in this License Agreement shall apply to such Third Party Programs.

16.6. Customer Service:

Should You have any questions concerning this License Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Enterprise Customer Care, 555 International Way, Springfield, Oregon 97477, U.S.A., (ii) Symantec

Enterprise Customer Care Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Enterprise Customer Care, 1 Julius Ave, North Ryde, NSW 2113, Australia.

16.7. Entire Agreement:

This License Agreement and any related License Instrument are the complete and exclusive agreement between You and Symantec relating to the Licensed Software and supersede any previous or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter. This License Agreement prevails over any conflicting or additional terms of any purchase order, ordering document, acknowledgment or confirmation or other document issued by You, even if signed and returned. This License Agreement may only be modified by a License Instrument that accompanies or follows this License Agreement.

Contents

Technical Support

Chapter 1 Overview

Introduction	11
RMS Console	11
bv-Control for NDS eDirectory	12
ActiveAdmin	13
Site standards	13
Auditing (Auditcon)	13
User management	14
bv-Count for NDS eDirectory	15

Chapter 2 Planning for Deployment

Introduction	17
Dependency on RMS Console	17
Architecture	18
Query processing	19
WAN link case study	20
Deployment strategies	20
Local strategy	21
Remote strategy	22
Network design factors affecting deployment decisions	23
Centralized environment without multiple NDS partitions	23
Centralized environment with multiple NDS partitions	24
Distributed environment with multiple NDS partitions	25
Deployment	25
WAN locations	26
Novell Directory Services server locations	26
Credential databases	26
Defining a deployment strategy	27
Create a table of potential users	28
Diagram the logical organization of the enterprise	28
Diagram the physical organization of the enterprise	29
Diagram the probable reporting areas for each user	29
Perform preliminary testing	29

	Estimate disk space requirements	30
	Develop an Information Server deployment strategy	31
	Estimate the size of each bv-Control computer	31
	Estimate the projected volume of use for each bv-Control computer	31
	Finalize the Information Server deployment strategy	31
	Select hardware	32
Chapter 3	Installing, Configuring, and Uninstalling the Product	
	System requirements	33
	bv-Control for NDS eDirectory	34
	Preinstallation considerations	34
	Installing bv-Control for NDS eDirectory	34
	Configuring the Console	35
	Configuring bv-Control for NDS eDirectory	35
	To manually configure bv-Control for NDS eDirectory	37
	Advanced configuration	37
	Uninstalling bv-Control for NDS eDirectory	38
Chapter 4	Evaluating the Product	
	Overview of the features	39
	Managing ZENworks	41
	Configuring the server	41
	Configuring the workstation	42
	Configuration information	43
	Configuring the product for Nsure Audit	43
	Specifying your data store	43
	Configuring the secure logging server	44
	Changes to security equivalence	45
	Closing security holes	46
	Retrieving DirXML information	46
	User security	47
	Evaluating standards	48
	Detecting intrusion	49
	Extending reporting capabilities	49
	Hidden objects	49
	Conclusion	50
Chapter 5	Troubleshooting	
	Symptoms and solutions	51
Appendix A	RMS Console Windows Groups	

	Administrator and user rights	55
Appendix B	Installing on a Secondary Windows 2000 Domain Controller with Active Directory Replicated	
	Replication	57
	Verifying replication	58
	Forcing replication	58
Appendix C	bv-Count for NDS eDirectory Utility	
	Counting NetWare servers	59
Glossary		
Index		

Overview

This chapter includes the following topics:

- [Introduction](#)
- [bv-Control for NDS eDirectory](#)

Introduction

This chapter provides an overview of the Symantec bv-Control® for NDS® eDirectory™ product. The bv-Control for NDS eDirectory product is a Snap-in to the RMS Console. The RMS Console and bv-Control for NDS eDirectory product lets you view and manage your NDS eDirectory environment.

The RMS Console provides the interface through which you access the bv-Control for NDS eDirectory product.

RMS Console

The RMS Console hosts bv-Control for NDS eDirectory and can also host other RMS Console products, giving you an integrated view of your network resources.

The RMS Console product installs as a Snap-in to the Microsoft Management Console (MMC). The MMC is a host application that provides a common interface for management snap-ins, such as the RMS Console.

For detailed information about how to use and configure the MMC, consult Help Topics from the MMC Help menu, or consult the MMC home page at www.microsoft.com.

The RMS Console provides a platform and the essential services for the bv-Control for NDS eDirectory product.

You use the RMS Console to create a query to collect information about your NDS environment. After query processing and the collection of information

from your NDS environment, the RMS Console can display the information. The information can be displayed in a grid, chart, or report.

bv-Control for NDS eDirectory

The bv-Control for NDS eDirectory product is a query-based addition to the RMS Console that installs into the RMS Console, extending the console's capabilities. With the bv-Control for NDS eDirectory module, the RMS Console can access information from NDS trees on your enterprise network. Using bv-Control for NDS eDirectory, you can view and manage the trees, containers, groups, users, and other objects in NDS. You can use the query tools that the RMS Console supplies to select and filter items in grids, charts, and the reports that are based on conditions you specify. In addition, bv-Control for NDS eDirectory provides the ability to enforce Site Standards. Together with other modules, bv-Control for NDS eDirectory and the RMS Console provide a comprehensive administration solution across disparate platforms.

The release of bv-Control for NDS eDirectory provides additional data sources, greater scalability, and improved speed of queries in certain data sources.

In addition to the standard features that the RMS Console provides, bv-Control for NDS eDirectory lets you do the following:

- View the ZENworks® Desktop Management policies in effect for all or for selected users, workstations, and servers using a single query.
- View the configuration details of ZENworks Desktop Management policies in effect for all or for selected users, workstations, and servers using a single query.
- Identify the ZENworks Desktop Management user who has created or modified the Policy Package and when the user takes an action.
- View configuration and audited information for Novell® Nsure® Audit 1.0.1, 1.0.2, 1.0.3, 2.0.0, and 2.0.1. Event information that the Secure Logging Server logs in the MySQL, Microsoft SQL Server, and Oracle database is reported.
- Edit the contents of fields in the grids that a Query generates and have those values change on the server (ActiveAdmin).
- Generate audit logs to review changes made using ActiveAdmin.
- Compare users on your network to selected attributes of a standard user.

ActiveAdmin

With ActiveAdmin®, you can make changes to user properties from within the RMS Console.

The following features are available to help you make changes to the user properties:

- Icons signifying editable fields in the list of available data sources
- Editable (ActiveAdmin) fields grouped in Available Fields lists
- A command that opens editors when you right-click in a grid
- ActiveAdmin editors that are associated with specific types of results, which appear in a grid
- Dialog boxes for error messages that NDS generates if attempts to update NDS settings fail due to inadequate permissions
- ActiveAdmin permission settings in the Enter User Account Information dialog box
- An audit database and related fields that retain log information on all changes made using ActiveAdmin

Site standards

Site Standards allow you to set up a model for users on your network. After the model is set, they determine how closely the attributes of standard users adhere to the ideal you created.

The bv-Control for NDS eDirectory product provides the following features to help you create and use Site Standards:

- Ability to configure multiple, independent Site Standards
- Site Standards fields in the list of available data sources
- Ability to select which Site Standard to conform to from a dialog box

Auditing (Auditcon)

In addition to support for NDS features, bv-Control for NDS eDirectory provides the auditing functionality that uses an approach similar to Novell's Auditcon. Using the bv-Control for NDS eDirectory Auditing feature, you can enable, configure, and run auditing queries.

Auditors using the reporting feature of bv-Control for NDS eDirectory can generate reports against data sources.

Reports can be generated from the following Audit File Types:

- Current audit log file
- Newest history audit log file
- Oldest history audit log file
- All history audit log files

These audit log files list the selected NDS object audit events that occur during an audit.

Audit administrators configure the NDS objects using the ActiveAdmin features in bv-Control for NDS eDirectory. Typically, auditing is enabled for a container or volume, then specific audit events are enabled. Once the audit is enabled, audit events are recorded in the current log file. The bv-Control for NDS eDirectory product provides reporting for container auditing only.

Each container being audited has its own set of audit files. Each set of files is kept in an audit file archive. The audit administrator administers these archives.

For more information on reporting on the event information of Novell® Nsure® Audit, see the *bv-Control for NDS eDirectory Help*.

User management

The bv-Control for NDS eDirectory product includes the features that let you manage the users on your NDS network.

Novell application launcher support

The bv-Control for NDS eDirectory product supports managing and reporting on Novell Application Launcher (NAL) objects. NAL is Novell's method of distributing applications to end users and controlling which applications they are allowed to see and use.

User template object support

The bv-Control for NDS eDirectory product supports managing and reporting on the User Template NDS object type that is provided on NetWare 4.11 servers. User templates are used to create new users with certain settings already defined in the template object. NetWare 4.2, 5, and 6 provide for a template object to create new objects with certain predefined settings.

GroupWise analysis

The bv-Control for NDS eDirectory product supports reporting on the basic aspects of user information for GroupWise® management tool v5.2 and later.

User attributes in site standards

User attributes are incorporated into each Site Standard. The fields that check these attributes have corresponding ActiveAdmin editors.

The following User Attributes are now defined on individual panels in the Site Standard Setup dialog box:

- Account Restrictions
- Password Restrictions
- Groups Belonged To
- Security Equivalences
- Login Time Restrictions

bv-Count for NDS eDirectory

The bv-Control for NDS eDirectory product includes the bv-Count® for NDS® eDirectory™ utility. This utility counts the number of objects in your NDS tree.

See “[Counting NetWare servers](#)” on page 59.

Planning for Deployment

This chapter includes the following topics:

- [Introduction](#)
- [Architecture](#)
- [Query processing](#)
- [Deployment strategies](#)
- [Network design factors affecting deployment decisions](#)
- [Deployment](#)
- [Defining a deployment strategy](#)

Introduction

This chapter provides the information that is required to help administrators make informed decisions about the deployment of bv-Control for NDS eDirectory. For more information, see the *Console and Information Server Getting Started Guide*.

Dependency on RMS Console

The bv-Control for NDS product depends on the Information Server component of the RMS Console and Information Server (also referred to as the infrastructure) to do all data collection.

The RMS Console must be installed before bv-Control for NDS can be used. If you install the RMS Console products for the first time, you should plan your bv-Control for NDS installation with your RMS Console installation planning.

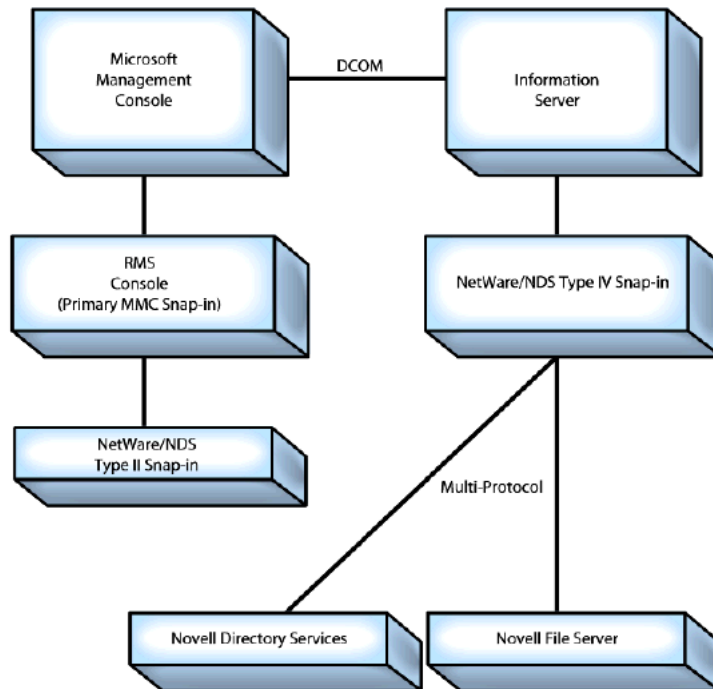
After deployment of RMS Console

After you deploy the RMS Console, you should identify the bv-Control for NDS installation options available in your current RMS Console. You also need to consider the possible modifications to your infrastructure can afford, that can further optimize its performance.

Architecture

Figure 2-1 shows the bv-Control for NDS eDirectory architecture.

Figure 2-1 bv-Control for NDS eDirectory architecture



Query processing

The bv-Control product suite includes two products that are designed to work together to report on Novell enterprises.

Each product is designed for the following functions:

- bv-Control for NetWare is used to perform queries on file data that is stored on Novell file servers and queries on the configuration of the servers themselves.
- bv-Control for NDS eDirectory is used to perform queries on object and object-attribute data that is stored in NDS replicas.

The bv-Control for NDS eDirectory product depends on the Information Server for query processing tasks. When a user submits a query using bv-Control for NDS eDirectory, the RMS Console passes the query to the Information Server, which makes the API calls that are required for retrieving the requested data.

bv-Control for NDS eDirectory API calls

API calls from the Information Server are handled in the following sequence for bv-Control for NDS eDirectory:

- The Information Server submits the API call to NDS.
- NDS directs the API call to the preferred server, or if none has been defined, to the first server that responds containing a replica of the requested information.
- NDS attempts to authenticate the bv-Control user against the rights and permissions that are required for server access.
- If the server is able to authenticate the bv-Control user, access is granted, and the Information Server retrieves the requested data. If no server authenticates the bv-Control user, the query fails.
- If NDS locates a server that is able to authenticate the bv-Control user, access is granted, and the Information Server retrieves the requested data.
- When the API call has returned and all data has been retrieved, the RMS Console pulls the dataset into virtual memory and displays the data.

Note: The computers on which the RMS Console and the Information Server are installed must have enough free disk space to hold the returned dataset. If either computer does not have enough free disk space to hold the dataset, the query fails.

Factors that affect NDS query processing response times

Response times for the queries that are submitted by bv-Control for NDS eDirectory are dependent on the number of objects in the NDS tree the query must report against. NDS directs all API calls made by the Information Server. In distributed enterprise environments, WAN link speed may affect the response time of bv-Control for NDS eDirectory in unexpected ways.

WAN link case study

A company has a main office in New York and a branch office in Tokyo. The company has deployed a Novell network with the WAN links that are relatively slow. On this network, administrators in each location have created organizational units (OU) based on departments. Each OU has been assigned its own NDS partition. One server in each city holds a full replica of the entire network, and each location has at least two servers containing replicas of OU data for that location.

An administrator in New York submits a query using an Information Server that is located at the main office in New York. The query requests data on network resources for an OU that is located in New York. This data is contained on the replica at the New York office. However, when the administrator submits this query, NDS directs the API call to the first server that responds. In this instance, the first server to respond is the server located at the office in Tokyo. When bv-Control for NDS eDirectory responds slowly, the administrator checks the Task Status window and determines that the Information Server is connected to a server in Tokyo, and assumes there has been a software error.

The following actions are required for NDS eDirectory to direct the API calls to the wanted server:

- Define a preferred server
- Deploy the Information Server in the same general location
- Optimize the replica ring

Deployment strategies

The following strategies can be employed to deploy bv-Control for NDS eDirectory:

- [Local strategy](#)
- [Remote strategy](#)

Each deployment type has advantages and disadvantages. Administrators should consider the advantages and disadvantages of each type of deployment.

Local strategy

The local strategy includes the use of an Information Server and local RMS Console. The strategy applies to single-user bv-Control networks or for multiple-user bv-Control networks where users do not need to share files.

Advantages of a local strategy

The advantages of deploying the Information Server with a local RMS Console are as follows:

- The software can be deployed on the user's normal workstation that has enough RAM, virtual memory, and free disk space. Enough RAM, virtual memory, and free disk space lets the workstation handle query data from both the RMS Console and the Information Server.
- The actions of other bv-Control users does not affect product response times unless other RMS Console users use the Information Server remotely.
- Network traffic between the Information server and the Console is eliminated.
- Administrators only need to select suitable hardware, and do not need to be concerned with other infrastructure deployment issues.

Note: If deployment on the user's normal workstation is not feasible, the software can still be deployed on a dedicated workstation.

Disadvantages of a local strategy

The disadvantages of deploying the Information Server with a local RMS Console are as follows:

- Central repository for query definitions or historical datasets is absent. Users cannot share queries, and information may be duplicated across computers.
- Simultaneous use of bv-Control products and other memory-intensive software that is installed on a computer limit the response time of all software in use. It may be impractical to use the computer to run other software while bv-Control queries are running.

Remote strategy

The remote strategy includes remote installation of the Information Server and deployment of RMS Consoles on multiple-user bv-Control networks where users must share files.

Advantages of a remote strategy

The advantages of deploying the Information Server with a remote RMS Console or Consoles are the following:

- Central repository for queries and historical datasets is present. Users can share queries.
- The RMS Console can be deployed on the user's normal workstation without affecting the performance of other software that is installed on the computer.
- If the volume of use is low, server response times may be significantly faster than workstation response times.

Disadvantages of a remote strategy

The disadvantages of deploying the Information Server with a remote RMS Console or Consoles are the following:

- Communication between the Information Server and the Consoles consumes network bandwidth.
- The actions of other bv-Control users may affect product response times. The bv-Control infrastructure is designed for multiple users, but on any computer, no matter how powerful, a point is reached where each additional user that connects to the Information Server affects the response times for all users. To determine the point at which the response times for all users are affected is difficult. Response times are dependent on a number of variables.

The variables include the following:

- Total amount of CPU power
- Amount of CPU power that is consumed by other software that is installed on the server
- Total amount of RAM
- Amount of RAM that is consumed by other software that is installed on the server
- Number of concurrent bv-Control users
- Type of queries submitted

Note: Use the information that is provided in this guide to make deployment decisions that improve performance.

Administrators who adopt an incremental deployment strategy should deploy the product in logical stages. At each stage, administrators should attempt to determine an optimal deployment scenario for their environment. After physical deployment is complete, administrators should monitor overall bv-Control product performance and modify the original deployment decisions as required.

Network design factors affecting deployment decisions

On Novell network enterprises, the response time for bv-Control for NDS eDirectory depends primarily on the tree replication state. The response time depends to a lesser degree on the design of the RMS Console.

When you plan for deployment, give consideration to the following:

- The amount and type of use users require of bv-Control for NDS eDirectory
- The organization of the NDS tree which include the containers within the tree and the partition scheme that is used for the tree

The types of NDS partition schemes are follows:

- Centralized environment without multiple NDS partitions
- Centralized environment with multiple NDS partitions
- Distributed environment with multiple NDS partitions

Centralized environment without multiple NDS partitions

The administrators can deploy local installations of the Information Server and RMS Console in centralized environments without multiple NDS partitions. They can also deploy remote installations of the Information Server with multiple connecting Consoles. The remote installation environment is usually small, with no more than 10 servers or 3000 NDS tree objects. In a remote installation environment, the total size of bv-Control for NDS eDirectory network is usually small with no more than 3-7 users.

Administrators who deploy a remote installation of the Information Server with multiple connecting Consoles should obtain satisfactory results with a single Information Server. The Information Server should be installed on a dedicated Windows server if simultaneous queries are run constantly against the NetWare

file system. Administrators can deploy a remote installation of multiple Information Servers.

Multiple Information Servers can be deployed with multiple connecting Consoles on a bv-Control network with more than seven simultaneous bv-Control users.

Centralized environment with multiple NDS partitions

In a centralized environment with multiple domains, administrators can deploy either multiple Information Servers with local RMS Consoles, or one or more Information Servers with multiple connecting Consoles. Deployment issues that are related to remote installations of Information Server or Servers is covered in more detail in the *Console and Information Server Getting Started Guide*.

Consider the following factors while planning to deploy remote installations of Information Server or Servers:

- [Size of the bv-Control network](#)
- [Departmental or group deployment strategies](#)
- [Auditing groups](#)

Size of the bv-Control network

If the size of the bv-Control network is ten concurrent users or greater, and administrators want to deploy a single Information Server, the Information Server should be deployed on a dedicated server to prevent possibly slower response times for both bv-Control and other software that might be installed on the same computer. If the number of users is seven or greater, administrators should consider deploying multiple Information Servers to maximize bv-Control reporting speed.

Departmental or group deployment strategies

In large bv-Control networks, some administrators prefer to deploy multiple Information Servers on a departmental or group basis. This type of deployment strategy lets administrators optimize deployment for each department or reporting area, and is effective under most conditions.

Auditing groups

If queries are run on a periodic basis by the auditing groups, deploy a separate Information Server for these users. The administrators can plan the rest of the deployment separately. Separate deployment of the Information Server optimizes the deployment strategy for daily users.

Distributed environment with multiple NDS partitions

In distributed network environments with multiple locations, we recommend that administrators deploy at least one bv-Control infrastructure for each geographical location. At each location, administrators should consider deploying multiple bv-Control computers that are based on the organization of the enterprise.

See [“Centralized environment with multiple NDS partitions”](#) on page 24.

Queries against enterprise-wide data

Administrators intending to deploy bv-Control for NDS eDirectory in a distributed environment must consider both the normal and potential reporting areas for each user. Since WAN links are slow, query response time is slow. If numerous simultaneous queries are submitted over a WAN link, response time may suffer.

Administrators should consider deploying an Information Server that is dedicated for using bv-Control for NDS eDirectory queries across the WAN to minimize the effects of the bv-Control for NDS eDirectory queries on the overall response time.

The bv-Control for NDS eDirectory queries do not perform efficiently, if the following conditions exist:

- The projected volume of use of bv-Control for NDS eDirectory is high to very high.
- Users submit numerous simultaneous queries against file systems outside the local LAN.

Deploying an Information Server that is dedicated for the use for bv-Control for NDS eDirectory queries across a WAN should be considered as a stage in incremental deployment, and should be considered only if cross-WAN queries seem to affect the overall response of the bv-Control network.

Deployment

After you have deployed your RMS Console, you can deploy bv-Control for NDS eDirectory.

The following items in your Enterprise network affect how you should deploy these bv-Control products:

- [WAN locations](#)
- [Novell Directory Services server locations](#)

- [Credential databases](#)

WAN locations

If your tree covers multiple geographic areas, each separated by a WAN, we recommend deploying at least one Console and Information Server in each area. If you connect your Console to a remote Information Server across a WAN, your task processing time increases.

Novell Directory Services server locations

When you run a query, the Information Server sends an API call to the Novell Directory Services server. After Novell Directory Services recognizes and accepts the API call, the specified resource objects are queried for the requested information. NDS then sends this information to the Information Server and it can be displayed as a dataset on the user's Console.

Since the amount of time that is required to retrieve a dataset is directly dependent on NDS, we recommend deploying your Information Servers in the same locations as the Novell Directory Services servers.

Before you select the Information Server to process your query, you should consider the following characteristics about your NDS server:

- Speed
- Usage level
- Maintenance schedule

Select an Information Server in an area that has the fastest possible NDS server with the lowest possible usage level. If an NDS server is currently down for maintenance, use an Information Server that is located in an area that has another Novell Directory Services server.

Credential databases

The person who installs the Information Server is automatically the RMS Console administrator of the Information Server. We recommend that the RMS Console administrator completely configure the Information Server with all credential databases required for the deployed by-Control for NDS eDirectory users. The credential databases uses NDS security to allow users access to the tree. It is very important to properly use credential databases to protect the integrity of the NDS security.

The RMS Console administrator should create one credential database per RMS Console user. They should only add credentials to the credential database for the

resource objects that they want the specific user to be able to query. Since the RMS Console administrators create the credential database, only they know the password for it and be able to assign it to the user.

The credential administrator protects the NDS security in the following ways:

- The user can only query the specific resource objects whose credentials reside in their assigned credential database, this lets the RMS Console administrator restrict the user's ability to retrieve information about specific resource objects.
- Since each user has their own credential database that only provides access to specific areas of the NDS tree, the RMS Console administrator easily tracks who made specific changes to the tree.

See [“Administrator and user rights”](#) on page 55.

Defining a deployment strategy

No single deployment strategy is valid for all enterprises.

The administrators can consider the following factors as an aid for developing a general deployment strategy:

- [Create a table of potential users](#)
- [Diagram the logical organization of the enterprise](#)
- [Diagram the physical organization of the enterprise](#)
- [Diagram the probable reporting areas for each user](#)
- [Perform preliminary testing](#)
- [Estimate disk space requirements](#)
- [Develop an Information Server deployment strategy](#)
- [Estimate the size of each bv-Control computer](#)
- [Estimate the projected volume of use for each bv-Control computer](#)
- [Finalize the Information Sever deployment strategy](#)
- [Select hardware](#)

Create a table of potential users

Create a table that includes the name and location of each potential user of bv-Control for NDS eDirectory.

At a minimum, the table should contain the following information:

- User name
- Group or location
- Product or products used
- Frequency of use (daily or periodic)
- Comments

Comments can be used to include user rights, position, projected volume of use, or other information about the user that might affect deployment decisions

[Table 2-1](#) is a sample user table only. Administrators should design the table to include whatever information is relevant to their network environment.

Table 2-1 Sample user table

User	Group Location	NetWare	NDS	Daily	Periodic	Comments
name 1	location 1	Y	Y	Y		
name 2	location 2	Y	Y	Y		
name 3	location 4	Y	Y		Weekly	
name 4	location 4	Y	N		Monthly	

Diagram the logical organization of the enterprise

Diagram the logical organization of the enterprise, based on the company organization chart. Do not include individuals. Use this diagram as a visual aid when making bv-Control deployment decisions. For distributed network enterprises with multiple geographical locations, consider creating one diagram for the network as a whole. Then create separate diagrams that contain detailed information for each geographical location. Administrators should be thoroughly familiar with the logical organization of the current enterprise network configuration before attempting to make the decisions that are related to deployment of the bv-Control network.

Diagram the physical organization of the enterprise

Diagram the physical organization of the enterprise. Include information on both the NDS tree structure and the location of Novell file servers. Use this diagram as a visual aid when making bv-Control infrastructure deployment decisions. For distributed network enterprises with multiple geographical locations, consider creating one diagram representing the NDS tree structure of the network as a whole. Then creating separate diagrams that contain detailed information for each geographical location. Administrators should be thoroughly familiar with the physical organization of the current enterprise network configuration before attempting to make the decisions that are related to deployment of the bv-Control network.

Diagram the probable reporting areas for each user

First determine the probable normal and potential reporting area for each user, based on both the logical and physical organization of the enterprise. After you determine the normal and potential reporting areas for each user, map these reporting areas to both the logical and physical enterprise organization diagrams created earlier. No matter how large or complicated is the enterprise, mapping probable reporting areas to the enterprise network configuration helps the administrators. It lets them visualize how the reporting area of each user overlaps. Administrators can work backward from these overlapping reporting areas to determine where to deploy different bv-Control computers. For example, if the normal reporting areas of six bv-Control users logically overlap in Sales, administrators should consider deploying a bv-Control computer for Sales.

Perform preliminary testing

Before the administrators make any decisions that are related to actual deployment or hardware selection, they should perform a few preliminary tests.

Note: This information, considered together with the users' probable pattern of use of bv-Control for NDS eDirectory, can be used to estimate both the projected use of bv-Control and the general hardware requirements.

Perform preliminary testing by doing the following:

- Deploy a local installation of the RMS Console and the Information Server on an available workstation, and install bv-Control for NDS eDirectory.
- After the software is installed, the administrators should select predefined queries from the RMS Console Pre-Defined Queries folder that can be used

to represent typical and worst-case queries for each user. A worst-case query is a query that is likely to either force NDS to direct multiple API calls for bv-Control for NDS eDirectory (for example, a query that must search data on multiple partitions).

- Administrators may find it helpful to involve future users in this process, and let the users select and run the queries.
- Record the size (in bytes) of the dataset for a typical query by each user for bv-Control for NDS eDirectory.
- Record the size (in bytes) of the dataset for a worst-case query by each user for bv-Control for NDS eDirectory.
- Record the duration of the typical query by each user for bv-Control for NDS eDirectory.
- Record the duration of a worst-case query by each user for bv-Control for NDS eDirectory.

Estimate disk space requirements

The administrators should always overestimate, rather than underestimate, when estimating disk space requirements.

The figures that are obtained by executing the actions can be used as a guide for estimating minimum requirements only. These figures should not be considered actual measurements of requirements.

Estimate hardware requirements by doing the following:

- Using the data that is collected during preliminary testing, round the size of the dataset for each user's worst-case query result to the next 100 MB, then multiply by six. (Six is the default maximum number of queries each user can run before the queries are queued.) Multiply the result by two to provide a margin of error. This figure provides a rough estimate of the minimum amount of virtual memory and free disk space that the user's RMS Console may require for dataset display.
- Estimate the number of historical datasets each user may need to save. Multiply the result by six to provide a margin of error. Multiply this figure by the result that is obtained in the first bullet point. This figure provides a rough estimate of the minimum amount of disk space each user may require for historical dataset storage.
- Administrators who deploy a remote Information Server and multiple RMS Consoles should add the totals that are obtained in the first bullet point. This step should be executed for the users of each Information Server. Multiply the result by two to provide a margin of error. This figure provides

a rough estimate of the minimum free disk space that the Information Server may require for data storage.

- Administrators who deploy a remote Information Server and multiple RMS Consoles should add the totals that are obtained in the second bullet point. This step should be executed for the users of each Information Server. Multiply the result by three to provide a margin of error. This figure provides a rough estimate of the minimum amount of disk space that should be allotted for historical dataset storage.

Develop an Information Server deployment strategy

Administrators should develop an Information Server deployment strategy that meets the needs of their environment. The administrators should consider the problem in terms of logical bv-Control computers when attempting to develop the best strategy for a particular environment. The administrators should not consider the problem in terms of physical Infrastructure deployment.

See [“Defining a deployment strategy”](#) on page 27.

To develop a deployment strategy, do the following:

- Select an Information Server deployment strategy using local or remote RMS Consoles.
- Determine the number of Information Servers to deploy.
- Determine the reporting areas for each Information Server.
- Determine the potential users of each Information Server.

Estimate the size of each bv-Control computer

Estimate the size of each bv-Control computer that is deployed, based on normal and potential reporting areas of each Information Server.

Estimate the projected volume of use for each bv-Control computer

Estimate the projected volume of use of each bv-Control computer that is deployed. As an alternative, add the number of RMS Consoles in the potential reporting area of the computer.

Finalize the Information Server deployment strategy

Before the administrators finalize the Information Server deployment strategy, they should review the deployment strategy and modify the strategy as required, based on size and projected volume of use estimations.

Select hardware

Administrators should base hardware selection decisions for both the Information Server and the RMS Console on the earlier estimations of disk space requirements.

See [“System requirements”](#) on page 33.

Installing, Configuring, and Uninstalling the Product

This chapter includes the following topics:

- [System requirements](#)
- [Preinstallation considerations](#)
- [Installing bv-Control for NDS eDirectory](#)
- [Configuring the Console](#)
- [Configuring bv-Control for NDS eDirectory](#)
- [Advanced configuration](#)
- [Uninstalling bv-Control for NDS eDirectory](#)

System requirements

This section describes the hardware and software requirements for using bv-Control for NDS eDirectory.

For general system requirements for the RMS Console and Information Server, see the *Control Compliance Suite Installation Guide*.

bv-Control for NDS eDirectory

In order to use bv-Control for NDS eDirectory with the RMS Console, your computer must meet the following system requirements:

- RMS Console and Information Server 10.0
- Novell Client™ 4.8 or later (Information Server computer only)
- File and Printer sharing for Microsoft Network enabled
- Server Services installed
- Admin Shares enabled

Preinstallation considerations

bv-Control for NDS eDirectory requires a Console and Information Server to function. Before you install bv-Control for NDS eDirectory, you must install the RMS Console and Information Server.

During the Console installation process, you must choose the Information Server for the Console you intend to install. You can choose to install a local Information Server, or you can connect the Console to an existing Information Server. The Information Server you install or connect to is the default Information Server for the Console.

For more information on installing the RMS Console and Information Server, see the *Control Compliance Suite Installation Guide*.

Installing bv-Control for NDS eDirectory

The bv-Control for NDS eDirectory product is shipped on a product disc. The product disc must be available from either a local or remotely mounted product disc drive. If you do not have access to a product disc drive, contact Symantec Technical Support for assistance.

See [“Technical Support”](#) on page 3.

See [“Replication”](#) on page 57.

See [“System requirements”](#) on page 33.

Before you install the product, we recommend that you review the Release Notes for the RMS Console and bv-Control for NDS eDirectory.

For more information on installing and upgrading, see the *Control Compliance Suite Installation Guide*.

Configuring the Console

Before using bv-Control for NDS eDirectory, you must configure the RMS Console.

For more information, see the *RMS Console and Information Server Getting Started Guide*.

Configuring bv-Control for NDS eDirectory

bv-Control for NDS eDirectory must be configured properly before using. You use the bv-Control for NDS eDirectory Configuration Wizard to configure the product with the required items.

You can also use the bv-Control for NDS eDirectory configuration feature to custom-configure the product.

The bv-Control for NDS eDirectory Configuration Wizard guides you through the following tasks:

- Create a credential database
- Associate a credential database
- Assign a credential database to a user
- Link credentials from bv-Control for NetWare

To launch the bv-Control for NDS eDirectory Configuration Wizard

- 1 From the Console Tree, select the **bv-Control for NDS eDirectory** container.
- 2 In the Details Pane, double-click **Configuration Wizard**.
- 3 In the Welcome panel, click **Next**.

To create a credential database

- 1 In the Add Credential Databases panel, click **Click and edit here to add new credential database**.
- 2 Enter a name for the credential database in the text box.
- 3 Click **Next**.
- 4 In the Create New Database dialog box, enter a password and then verify the password by re-entering it.
- 5 Click **OK**.
The credential database appears on the Add Credential Databases panel.
- 6 In the Add Credential Databases panel, click **Next**.

To associate a credential database with bv-Control for NDS eDirectory

- 1 In the Select Credentials panel, under Products, select **bv-Control for NDS eDirectory** from the dropdown list.
- 2 Under Credential Database, select that database to which you want to add resource object credentials.
- 3 From the Resource Objects box, select the tree you want to add credentials to and click >>. In the Credentials - Tree Credential dialog box, enter the Context for the tree, as well as a User Name, Password, and Server name combination which is valid for that context, and click **OK**. To specify an unlisted tree, select **Specify Unlisted Tree** and click >>. In the Additional Settings - Tree Credentials dialog box, enter the Context for the tree, as well as a User Name, Password, and Server name combination which is valid for that context, and click **OK**.
Specifying the Server name is optional while the other text boxes are required.
- 4 Click **Next**.

To assign a credential database to each user

- 1 Select a user under User Name.
- 2 Select the database to be assigned to the user from the Credential Database dropdown list. If the database is password protected, enter the password and click **OK**.
You can assign only one credential database to a user.
- 3 Click **Next**.

To link credentials from bv-Control for NetWare

- 1 In the Set Credential Link panel, select the **Link Credentials from bv-Control for NetWare** check box to link the existing credentials from bv-Control for NetWare to bv-Control for NDS eDirectory.
- 2 Click **Next**.
- 3 Review the summary information in the bv-Control for NDS eDirectory Product Settings Summary panel and click **Finish** to save your settings or click **Back** to modify your settings.

To manually configure bv-Control for NDS eDirectory

In addition to configuring the RMS Console for bv-Control for NDS eDirectory with the configuration wizard, you can also manually configure bv-Control for NDS eDirectory.

The bv-Control for NDS eDirectory product lets you do the following:

- Manually configure the settings for default scopes
- Add one or more advanced scopes
- Link existing configured credentials
- Control some of the syntax of queries
- Control the ways that the Information Server processes queries
- Control how Auditing queries are processed

To manually configure bv-Control for NDS eDirectory

- ◆ From the details pane of the RMS Console, click **Configuration** to configure the settings for bv-Control for NDS eDirectory.
The Settings, Export Advanced Scopes, and Link Credentials containers are displayed.

Warning: Auditing in NetWare has changed with the release of NetWare 6.0, which uses NAAS, not the API calls that were used in previous versions. The bv-Control for NetWare product uses the API calls that are supported in NetWare 4.x and 5.x. Do not attempt to configure NetWare 6.0 or later with these API calls as adverse results may occur. We advise that NDS auditing not be enabled through bv-Control for NDS eDirectory environments where NetWare 6.0 holds replicas of the partitions being audited, and that volume auditing not be configured on NetWare 6.5 servers through bv-Control for NDS eDirectory.

Note: To audit NetWare 6.x servers or later, you can use Novell's Nsure Audit which the bv-Control for NDS eDirectory product supports. Currently, the event information that is logged in the MySQL, Microsoft SQL Server, and Oracle database is reported.

Advanced configuration

After you complete the bv-Control for NDS eDirectory Configuration Wizard, you can further configure your bv-Control for NDS eDirectory snap-in.

With bv-Control for NDS eDirectory, you can configure the following:

- Scoping
- Auditing
- Query settings

- LDAP connection settings
- Exporting advanced scopes
- Linking credentials from bv-Control for NetWare to bv-Control for NDS eDirectory

In the Console tree, you double-click Configuration in the bv-Control for NDS eDirectory container to access the various configuration options.

For additional information, see the About advanced configuration options topic in the *bv-Control for NDS eDirectory Help*.

Uninstalling bv-Control for NDS eDirectory

You can uninstall bv-Control for NDS eDirectory from your computer by using the recommended process of removing programs through the Add/Remove Programs dialog box.

For more information on uninstalling, see the *Control Compliance Suite Installation Guide*.

Evaluating the Product

This chapter includes the following topics:

- [Overview of the features](#)
- [Managing ZENworks](#)
- [Configuring the product for Nsure Audit](#)
- [Closing security holes](#)
- [Evaluating standards](#)
- [Extending reporting capabilities](#)
- [Conclusion](#)

Overview of the features

This section 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.

bv-Control for NDS eDirectory product lets you efficiently protect and manage your ZENworks environment.

Server Configuration	You can get important information about ZENworks for Desktop Management that Novell native tools cannot provide, such as server names, services and their versions, and middle-tier configuration.
----------------------	--

Policy Configuration	You can view configuration details of all policies in a single view, which is not possible using Novell native tools.
----------------------	---

Effective Policies You can view the policies in effect for all or for selected users, workstations, and servers using a single query. With Novell native tools, selection and checking of all policy objects individually is a time-consuming and error-prone process.

Custom Reports Use out-of-the-box custom reports to efficiently identify the conditions that threaten the security of ZENworks for Desktop Management environment.

bv-Control for NDS eDirectory lets you report on Novell Nsure Audit information:

Configuration Information Using the support for Novell's Nsure Audit, you can report on the configuration information of your auditing environment in a single view.

Audited Information Using the support for Novell's Nsure Audit, you can report on the audited information that is logged by the Secure Logging Server in the MySQL, Microsoft SQL Server, and Oracle database. Event information for eDirectory and Nsure Instrumentation applications can be reported.

bv-Control for NDS eDirectory lets you identify and close security holes:

Predefined 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 lets you easily build custom queries that are specific to particular corporate policies and procedures.

Effective Rights Analysis Using Effective Rights Analysis you can do the following:

- Identify who has access to data and how it was obtained
- Perform enterprise-wide effective rights analyses on NDS objects
- Provide critical information about hidden objects
- Locate and delete stale accounts
- Find and eliminate password problems

Easy-to-view Reports	Simplify Problem resolution by making changes to eDirectory from within a report. This feature lets you enforce fast and efficient changes across a diverse IT environment.
----------------------	---

bv-Control for NDS eDirectory lets you 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.
----------------	--

bv-Control for NDS eDirectory lets you 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.
---------------------	--

bv-Control for NDS eDirectory lets you 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 computer compatibility.

Managing ZENworks

The bv-Control for NDS eDirectory product lets you get the information you require quickly.

Configuring the server

It is sometimes essential to access server configuration information that Novell native tools cannot currently provide, such as server names, services and their versions, and middle-tier configuration. The bv-Control for NDS product provides the ability to collect and view this information with a single query.

To execute the query

- 1 Double-click the **New Query** icon on the toolbar.
- 2 Double-click **bv-Control for NDS eDirectory** on the Select Data Source dialog box.
- 3 Select **Server Object** and click **OK**.
- 4 On the Query Builder dialog box, select the **Field Specification** tab.
- 5 From the All Fields list, select the **Effective Policies** field and click **Add**.
- 6 Click **OK**.
- 7 On the Query Options dialog box, click **Run**.
- 8 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 console window.

Configuring the workstation

It is sometimes essential to access workstation configuration information that Novell native tools cannot currently provide, such as workstations and the policies that affect them. The bv-Control for NDS product provides the ability to collect and view this information with a single query.

To execute the query

- 1 Double-click the **New Query** icon on the toolbar.
- 2 Double-click **bv-Control for NDS eDirectory** on the Select Data Source dialog box.
- 3 Select **Workstation** and click **OK**.
- 4 On the Query Builder dialog box, select the **Field Specification** tab.
- 5 From the All Fields list, select the **Effective Policies** field and click **Add**.
- 6 Click **OK**.
- 7 On the Query Options dialog box, click **Run**.
- 8 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 console window.

Configuration information

It is sometimes essential to access policy configuration information that Novell native tools cannot currently provide, such as when the policies were created, last modified, and by whom. The bv-Control for NDS product provides the ability to collect and view this information with a single query.

To execute the query

- 1 Double-click the **New Query** icon on the toolbar.
- 2 Double-click **bv-Control for NDS eDirectory** on the Select Data Source dialog box.
- 3 Select User and click **OK**.
- 4 On the Query Builder dialog box, select the **Field Specification** tab.
- 5 From the All Fields list, select the **Effective Policies** field and click **Add**.
- 6 Click **OK**.
- 7 On the Query Options dialog box, click **Run**.
- 8 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 console window.

Configuring the product for Nsure Audit

The bv-Control for NDS eDirectory product lets you report on event information pertaining to Novell® Nsure® Audit.

Specifying your data store

To report on Novell® Nsure® Audit you need to specify the advanced configuration options after completing the product installation wizard. You can report on event information pertaining to Novell® Nsure® Audit 1.0.1, 1.0.2, 1.0.3, 2.0.0, and 2.0.1 using bv-Control for NDS eDirectory. This snap-in reports on eDirectory Instrumentation and Nsure Instrumentation applications. bv-Control for NDS eDirectory reports the event information that is logged by the Secure Logging Server in an Oracle database and Microsoft SQL Server database.

To configure bv-Control for NDS eDirectory for Nsure Audit

- 1 Select **Configuration** under bv-Control for NDS eDirectory in the Console tree.
- 2 Double-click **Settings** in the Details pane.

- 3 On the Settings dialog box, select the **Nsure Audit Settings** tab.
- 4 On the Nsure Audit Settings tab, click **Add**.
- 5 On the Data Store Credentials dialog box, enter the information about your data store and click **OK**.
If you select Oracle as your Data Store Type then you also have to specify the Connection Type.
- 6 Select the Connection Type from the dropdown box, which displays the following options:

Database Default	The default configuration of the database
Shared Server	A database server that lets many user processes share a few server processes
Dedicated Server	A database server in which each server process is dedicated to only one client connection
- 7 Ensure that the check box in the Selected column for the added data store is checked.
- 8 To add another data store, click **Add**. To report on multiple data stores at a time, ensure that the check box in the Selected column is checked. Similarly, to avoid reporting on a data store, clear the check box under the Selected column.
- 9 Click **OK** on the Settings dialog box.
Assuming that the data store credentials you entered are valid, you can report on event information that is logged by the Secure Logging Server (SLS) in the data store.

Configuring the secure logging server

You can report on configuration settings of the Secure Logging Servers in your NDS environment. You can also report on the configuration settings of the various channel objects being used for auditing purposes.

You can use the predefined queries under Pre-Defined > bv-Control for NDS eDirectory > Log Analysis > Nsure Audit > Configuration for reporting.

To execute the query

- 1 Navigate to the Nsure Audit Secure Logging Server predefined query in the RMS Console folder by using the following path: RMS Console > Risk Assessment and Control > Pre-Defined > bv-Control for NDS eDirectory >

Log Analysis > Nsure Audit > Configuration > Nsure Audit Secure Logging Server.

- 2 Right-click **Nsure Audit Secure Logging Server** in the Tree pane and select **Run > And View as Grid** to execute the query.
It is assumed here that the default scope has been set to root.
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.
- 3 When the query has successfully executed, the dataset is displayed.

Changes to security equivalence

You can report on audited events of eDirectory and Nsure configuration in your NDS environment. The event information that is reported is obtained from the MySQL, Microsoft SQL Server, or Oracle data store that you specified during configuration.

Using bv-Control for NDS eDirectory, you can report on multiple tables at a time (from multiple MySQL, Microsoft SQL Server, or Oracle data stores), which cannot be done using Novell native tools. However, using the bv-Control for NDS eDirectory product, you can also specify a server or multiple servers in the scope by selecting the servers that are enumerated on the Scope tab. Audited information for only those servers is reported.

You can use the predefined queries under Pre-Defined > bv-Control for NDS eDirectory > Log Analysis > Nsure Audit > Reporting for reporting.

Executing the query

- 1 Navigate to the Changes to Security Equivalence in the Past Month predefined query in the RMS Console folder by using the following path: RMS Console > Risk Assessment and Control > Pre-Defined > bv-Control for NDS eDirectory > Log Analysis > Nsure Audit > Reporting > eDirectory Events > Changes to Security Equivalence in the Past Month.
- 2 Right-click **Changes to Security Equivalence in the Past Month** in the Tree pane and select **Run > And View as Grid** to execute the query.
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.
- 3 When the query has successfully executed, the dataset is displayed.

Closing security holes

bv-Control for NDS eDirectory lets you use the predefined reports which also facilitate disaster recovery.

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 for NDS eDirectory provides the ability to present this information in hard copy or electronic format, which can be printed or exported in many formats. This scenario illustrates how to execute a predefined query and print the results.

Executing the query

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

- 1 Select the **Printer** icon from the toolbar of the dataset.
- 2 Review the settings in the printer dialog box and click **OK** to print the dataset.
- 3 Close the dataset window and click **No** in response to the Save dataset dialog box.

Selecting No keeps the query you have run in the Task Status window for future reference and lets you 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.

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 section illustrates how to modify a predefined query to meet your specific needs. It also tells you how to save the changes for future use. You then make a change to the enterprise and use the baseline feature to illustrate the changes made.

Modifying a predefined query

- 1 Navigate to the User Objects Inactive for 90 Days predefined query in the RMS Console folder by using the following path: RMS Console > 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.
- 3 On the Query Builder dialog box, select the **Field Specification** tab.
- 4 In the Available Fields list, expand the All Fields folder and select the **Password Exists?** and **Password Minimum Length** fields and click **Add**.
- 5 Click the **Filter Specification tab** to modify the criteria that is used for selecting which records should appear on the report.
- 6 In the Available Fields list, expand the All Fields folder and select the **Password Exists?** field and click **Add**.
- 7 On the Filter Term Definition dialog box, select **Is Not Yes** from the dropdown box and click **OK**.
The new criteria is displayed in the lower pane of the Query Builder dialog box on the Filter Specification tab.
- 8 On the Query Options dialog box, click **Save** and save the modified query in the My Items folder with a name of your choice.
A copy of the modified query is saved for future reference and use.

To perform and review enterprise changes within a dataset

- 1 From the Query Options dialog box, click **Run** with View As Grid selected. A dataset appears listing all users whose accounts are either inactive or have no password.
- 2 Choose a user from the list whose account you can safely modify and click the Password Minimum Length cell which corresponds to that user.
- 3 Right-click on the cell and select **Edit** from the sub-menu to open the Password Restrictions dialog box.
The Password Restrictions dialog box lets you 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**.
- 4 Change the default value in the Minimum Password Length text box to 4 and click **OK**, then click **Yes**.
An administrative job is initiated, which writes the change you have made to NDS. While you change 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.
- 5 When the administrative job is completed, re-run the query by right-clicking the query you saved to the My Items folder earlier and select **Run > And View as Grid** from the sub-menu.
- 6 Close both queries and click **Yes** to save the datasets to the query binder.
- 7 Right-click the saved query and select **Manage > Historical Data** from the sub-menu.
- 8 On the Manage Historical Data dialog box, select both queries and click **Run Baseline**.
- 9 Accept the default options, and click **OK**.
- 10 On the Baseline Dataset, 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.

Evaluating standards

The bv-Control for NDS eDirectory product lets you monitor user action and evaluate the standards.

Detecting intrusion

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 predefined query in the RMS Console folder by using the following path: RMS Console > 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 On the Query Builder dialog box, click **Scope tab**.
- 4 On the Scope tab, select the location on which you want to execute the query and click **OK**.
- 5 On the Query Options dialog box, click **Run** with the View As Grid option selected.
- 6 On the Container Intruder Detection Settings dataset, close the dataset without saving the information.

Extending reporting capabilities

bv-Control for NDS eDirectory product lets you extend reporting capabilities and thereby simplify data analysis.

Hidden objects

Hidden objects may represent serious security issues with your network as they are used by hackers as a means of creating a back door 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 that have escaped administration.

To get a list of the hidden objects

- 1 Navigate to the Invisible Objects Detail predefined query in the RMS Console folder by using the following path: RMS Console > 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 console window.
- 3 On the Invisible Objects Detail dataset, 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 that are assigned to the user over NDS objects are detailed.
- 4 Close the dataset without saving the information.

Conclusion

The information that is provided in this Evaluation chapter covers only a few of the features of the bv-Control for NDS eDirectory product. The scenarios are intended to give you an idea of how bv-Control for NDS eDirectory can help you administer and secure the safety and reliability of your servers. bv-Control for NDS eDirectory is designed to assist you to properly configure and protect your environment, thus minimizing unplanned downtime and maximizing the return on your IT investment.

Troubleshooting

This chapter includes the following topic:

- [Symptoms and solutions](#)

Symptoms and solutions

This chapter provides information to help you resolve the difficulties that you may encounter installing or using bv-Control for NDS eDirectory.

[Table 5-1](#) contains various issues, the symptoms, and its solutions.

Table 5-1 Symptoms and solutions

Issues	Symptoms	Solutions
Cannot audit an event.	In a mixed operating system environment, cannot audit an event that is visible in the Auditing dialog box.	Certain events cannot be audited in a mixed operating system environment. This is a limitation of auditing for which there is no solution or workaround.
Cannot scope a query.	User receives an NWDSLogin error during the authentication operation for logging into the tree.	Modify the NDS user account information in the credentials database to support login by the active user.
Single NDS tree visible when scoping a query.	A single NDS Tree may be visible when scoping a query, even though multiple Trees are defined in the credentials database.	Verify that there are no extraneous definitions provided in the Product Configuration, Settings, Default Scope, or Tree Tabs.

Table 5-1 Symptoms and solutions

Issues	Symptoms	Solutions
Query fails.	A query fails.	<ul style="list-style-type: none"> ■ Information Server cannot authenticate the bv-Control for NDS for eDirectory user. ■ RMS Console or Information Server does not have enough free disk space to hold the returned dataset.
Query response is slow.	<p>Query response time varies widely in an environment.</p> <p>It varies due to the following reasons:</p> <ul style="list-style-type: none"> ■ WAN links that are relatively slow ■ Organizational units (OU) that are geographically distant, where each OU has its own NDS partitions containing a full replica of the entire network 	<ul style="list-style-type: none"> ■ Deploy Information Servers as close as possible to the environment they query. ■ Avoid bandwidth bottlenecks between the Information Servers and the environments they query. ■ In certain queries, more than one Information Server can acquire the data. When you make such queries, define an Information Server that has a response-time advantage over the other Servers.
Audit query not reporting on all available files.	The bv-Control product Audit query does not report on all available Audit Files.	Select which files are to be used in performing Audit queries on the Auditing Tab by navigating the following path: Product Configuration>Settings>Auditing Tab.

Table 5-1 Symptoms and solutions

Issues	Symptoms	Solutions
<p>NetWare configuration is corrupt.</p>	<p>Configuration of NetWare 6.0 or higher is corrupted after auditing through NDS eDirectory where NetWare holds replicas of the partitions being audited.</p>	<ul style="list-style-type: none"> <li data-bbox="940 321 1236 494">■ Do not use bv-Control for NDS eDirectory to enable NDS auditing where NetWare 6.x and higher holds replicas of the 4.x and 5.x partitions. <li data-bbox="940 494 1236 607">■ Do not use bv-Control for NDS eDirectory to enable Volume auditing on NetWare 6.5 servers.

RMS Console Windows Groups

This chapter includes the following topic:

- [Administrator and user rights](#)

Administrator and user rights

The following are the Windows user groups:

- BV Console Admins
- BV Console Users

[Table A-1](#) lists the rights of the Windows user groups created by the RMS Console along with those required for the Windows administrator.

Table A-1 Administrator and user rights

Right	RMS Console administrator	RMS Console user	Windows administrator
Install a Console or Information Server on a computer			X
Add or remove licenses to or from the Information Server	X		
Add or remove Information Server users	X		X
Add or remove users to or from the BV Console Admins and BV Console Users groups	X		X
Assign RMS Console administrator right	X		
Assign right to create and modify queries	X		

Table A-1 Administrator and user rights

Right	RMS Console administrator	RMS Console user	Windows administrator
Assign right to use ActiveAdmin®	X		
Create and run ActiveAdmin session log queries	X		
Create and run historical dataset queries	X		
Assign a credential database to a user (password required). The credential database lets the user query resource objects for information and delete or edit a resource object using ActiveAdmin.		X	
Modify or delete a credential database (password required)		X	
Assign right to create and modify task lists	X		
Assign right to launch programs on the Information Server computer (Run Program post process command)	X		
Assign right to send export files to directories on the Information Server computer	X		
Modify other users' rights and properties	X		X
Modify your own rights and properties	X	X	X
Modify all named scopes stored on the Information Server	X		
Assign default scopes for all users	X		
Assign default scopes for yourself		X	
Define global report style settings	X		
Define global export style settings	X		
Link to other users' My Items folders	X		
Manage other users' queries	X		
Disable or modify your dynamic index settings		X	

Installing on a Secondary Windows 2000 Domain Controller with Active Directory Replicated

This chapter includes the following topic:

- [Replication](#)

Replication

When you install bv-Control for NDS eDirectory on a secondary Windows® 2000 Domain Controller that has Active Directory replicated to it, a Replication Wait dialog box appears during the installation process because the BV Console Users and BV Console Admin groups are installed on the primary Domain Controller, and the RMS Console cannot be launched on the secondary Domain Controller until these groups are replicated through Active Directory.

If you choose not to click Cancel during the installation process, the dialog box disappears automatically after the groups are replicated. After the replication occurs, the installation process continues and bv-Control for NDS eDirectory is ready for use after installation.

If you choose to click Cancel, the dialog box disappears, and the installation process continues. If you launch the RMS Console before the groups have been replicated, you receive an Initial Failed message in the MMC Console pane and the product becomes unusable. If you receive an Initial Failed message in the MMC Console pane, close the MMC and wait for the groups to replicate. After replication, you can launch the Console.

Verifying replication

You can verify if the groups have been replicated by opening the Properties dialog box.

Observe that the BV Console Users group is already replicated, but the BV Console Admins group is not. The string of numbers and dashes under the BV Console Users group is a placeholder representing the BV Console Admins group waiting to replicate.

To verify replication

- 1 From the computer Desktop, right-click **My Computer**.
- 2 Select **Manage**.
The Computer Management Console is launched.
- 3 Under the Share Folders container, expand the Shares folder.
- 4 From the details pane, right-click the **BindView share**.
- 5 Select **Properties**.
- 6 Select the **Share Permissions** tab on the Properties dialog box.

Forcing replication

Instead of waiting on the Active Directory replication to occur on its own (which can take up to 45 minutes), you can manually force a replication.

To force replication

- 1 From the Windows Start menu, go to Programs.
- 2 Select **Administrative Tools**.
- 3 Select **AD Sites and Service**.
- 4 On the AD Sites and Services Console, navigate to the NTDS Settings on the secondary Domain Controller where bv-Control for NetWare and NDS was installed.
- 5 From the details pane, right-click on the connection object.
- 6 Select **Replicate Now**. You are notified if the replication was successful.

bv-Count for NDS eDirectory Utility

This chapter includes the following topic:

- [Counting NetWare servers](#)

Counting NetWare servers

The bv-Count® for NDS® eDirectory™ utility is provided as a quick method for you to count the number of NetWare servers you select. You can choose to count all servers or servers of a specific type. This utility is an add-on to bv-Control for NDS eDirectory.

To use bv-Count for NDS eDirectory

- 1 Run the RMS Console and open the bv-Control for NDS eDirectory container. Inside it, open the bv-Count for NDS eDirectory container.
- 2 Double-click the **bv-Count for NDS eDirectory Utility** in the details pane.
- 3 Click the browse button on the **bv-Count for NDS eDirectory Utility** dialog box to specify the server that the utility should search for.
- 4 On the Select Container dialog box, double-click items in the list to expand them and show their contents.
- 5 Single-click an item and click **OK** to close the dialog box and select the level below which the utility should search.
- 6 Select the object type that the utility should search for from the Search For list.
- 7 Click **Search** when you are ready for the utility to begin its search.

The utility counts the objects you specified and displays its results in the dialog box.

- 8 For more information about the objects, click the **Details** tab and double-click to expand the containers.
- 9 To save the results, select **Save As** from the File menu and specify a name and location where the file should be saved.
- 10 When you are ready to quit the utility, click **Close** or select **Exit** from the File menu.

Glossary

ActiveAdmin	Feature that lets a user delete resource objects, historical datasets, or session logs; or to modify resource object attributes.
advanced scope	Named collections of scope information that you can create before they are needed and then use later in queries.
attributes	Characteristics of a resource object.
auditing	Reporting feature that lets you generate reports against data sources.
audit log file	Lists the selected object audit events that occur during an audit.
container	Item appearing in the a tree that holds objects or other containers.
credential database	Collection of information stored on the Information Server that provides access rights to resource objects.
data source	Group of fields related to resource objects with similar attributes, or properties.
default scope	A scope that ensures that only relevant objects are queried.
eDirectory	Novell directory service that stores and manages objects such as users, applications, network devices, and data.
field	Attributes, or properties, of the selected data source.
named scope	Group of saved scope items associated with a specific data source and Information Server.
NDS	Novell Directory Services is an information name service that organizes network resources—users, groups, printers, servers, volumes, and other physical network devices—into a hierarchical tree structure.
query	Request for information from selected resource objects.
query binder	Item used to store and manage query-related information.
scope	Part of the query definition that narrows the range of possible resource objects to be queried, thereby reducing the run time of the query.
server	Physical hardware device or computer that runs the network operating system.

site standards

Comparison of users against a standard user configuration.

Index

A

- ActiveAdmin 13
- administrator rights 55
- API calls 19
- architecture 18
- auditing 13, 41
- authentication 19

B

- BV Console Admins 55
- BV Console Users 55
- bv-Control for NDS eDirectory, description 12
- bv-Control for NetWare 19
- bv-Count for NDS eDirectory 15, 59, 60

C

- configuration
 - Nsure information 44, 45
- configuration reports
 - policy 43
 - server 41, 42

D

- deployment
 - across WAN 25
 - disk space requirements 30
 - hardware selection 31
 - incremental strategy 23
 - Information Server strategy 31
 - Information Servers 20
 - logical organization 28
 - NDS server characteristics 26
 - Novell Directory Services server locations 26
 - physical organization 29
 - preliminary testing 29
 - probable reporting areas by user 29
 - projected use 31
 - size of bv-Control computers 31
 - strategies 20, 27

- table of potential users 28
 - WAN considerations 26
- disk space 19
 - query failure 19
- domain controller replication 58

F

- features and benefits 39

G

- GroupWise support 15

H

- hidden objects, scenario 49

I

- Information Server
 - deployment strategy 31
 - preferred server specification 20
- installing 34
 - Active Directory replication 57
- intruder detection, scenario 49

L

- local deployment 20

M

- managing users 14
- Microsoft Management Console (MMC) 11

N

- NDS partition schemes 23, 24, 25
- Novell Application Launcher support 14
- Novell Directory Services server locations 26
- Novell Nsure Audit 12
 - reporting 44, 45
- Novell, limitations of native tools 41, 42, 43

O

optimizing replica ring 20

P

partition schemes 23, 24, 25

performance 25

 across WAN link 20

policy configuration report 43

predefined reports 40

preinstallation requirements 34

Q

query

 failure 19

 Novell Nsure Audit 44, 45

 processing 19

 response time 20, 25

 ZENworks for Desktop Management 41, 42, 43

R

remote deployment 20, 22

replication of domain controller 58

reporting

 Nsure Audit configuration information 44, 45

reports 41

 policy configuration 43

 server configuration 41, 42

requirements

 preinstallation 34

response time 20, 25

retrieving DirXML information, scenario 46

rights

 user and administrator 55

RMS Console 11

RMS Console, dependency on 17

S

scenario

 configuration information 44, 45

 hidden objects 49

 intruder detection 49

 policy configuration 43

 retrieving DirXML information 46

 server configuration 41, 42

 user security 47

secondary domain controllers 57

server configuration report 41, 42

Site Standards 13, 15

T

template support 14

troubleshooting 19, 51

U

user

 attributes 15

 management 14

 rights 55

 security scenario 47

 template support 14

W

WAN

 deployment considerations 25, 26

 impact on response time 20

Z

ZENworks Desktop Management 12, 39, 41