White Paper

Managing the Migration to Exchange 2000:

Leveraging Microsoft's Active Directory Connector (ADC)

BINDVIEW™

Integrity. IT Matters.™

BindView Corporation, 5151 San Felipe, Suite 2100, Houston, Texas 77056 USA ▪ Phone: 800-749-8439, 713-561-4000 ▪ Fax: 713-561-1000
World Wide Web: http://www.bindview.com ▪ Email: info@bindview.com ▪ If calling from outside North America, please call: +1-713-561-4000
Copyright © 2001 BindView Corporation. All rights reserved. BindView, the BindView logo, and the BindView product names used in this document are trademarks of BindView Corporation and may be registered in one or more jurisdictions. The names of products of other companies mentioned in this document, if any, may be the registered or unregistered trademarks of the owners of the products.

© 2000, 2001 BindView Development Corporation. All rights reserved.

The information contained in this document represents the current view of BindView Development Corporation, on the issues discussed as of the date of publication. Because BindView must respond to changing market conditions, it should not be interpreted to be a commitment on the part of BindView, and BindView cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. BINDVIEW MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

BindView, the BindView logo, and the BindView product names used in this document are trademarks of BindView Corporation and may be registered in one or more jurisdictions.

The names of products of other companies mentioned in this document, if any, may be the registered or unregistered trademarks of the owners of the products.

BindView Corporation • 5151 San Felipe • Suite 2100 • Houston, Texas77056 • USA

Table of Contents

Introduction

bv-Admin™ Migration Benefits for Exchange Migrations:

- Allows you to leverage and take advantage of Microsoft migration tools and strategies
- Eliminates duplicate Active Directory Accounts
- Resolves conflicting account properties between NT SAM and Exchange 5.5
- Prevents AD store bloat from tombstone records
- Automatically moves new accounts to their proper destination OU
- Ensures that users retain access to un-migrated Exchange 5.5 directory objects

Microsoft® Exchange 2000 is the first major Microsoft .NET enterprise server application to fully exploit Active Directory™— the directory service integrated with Windows® 2000. In fact, the integration between Exchange 2000 and Active Directory is one of most compelling features of Exchange 2000, and one of its most complex. Active Directory is the engine behind several Exchange 2000 services, including name resolution, security and a unified enterprise directory.

As the leader in directory administration, assessment, and security, BindView provides complete solutions for managing the transition to Exchange 2000. This document provides an overview of how BindView's bv-Admin for Windows 2000 Migration can ensure a successful migration of Exchange 5.5 and Windows NT objects to Exchange 2000/Active Directory, utilizing the Exchange Active Directory Connector.

What is the Exchange Active Directory Connector?

Microsoft's Active Directory Connector (ADC) is included in both Exchange 2000 and Windows 2000, and provides an automated means to replicate a hierarchy of directory objects from Exchange 5.5 to Active Directory. According to Microsoft, the Active Directory Connector is a key element in a flexible migration and upgrade path to Exchange 2000. The key features of the Active Directory Connector include:

- Fast, one-stop population of Active Directory with the directory information stored in the Exchange 5.5 directory.
- Bidirectional replication between Exchange 5.5 and Active Directory. Only changes are replicated between the directories, reducing network bandwidth utilization.
- Bulk import and export from Active Directory using a text file format.
- Flexible object matching rules for connecting objects in the Exchange 5.5 directory and Active Directory, resulting in fewer conflicts and enabling greater flexibility in how Active Directory is populated from Exchange 5.5.
- Use of connection agreements that allow administrators to fine-tune the replication schedule, the authentication parameters, and the format of the replication schema.

When Should You Move Exchange 5.5 Data to Active Directory?

Migration is not an event—it's a process. This philosophy also applies to Exchange migration. There are many critical planning questions you need to answer before you begin the process. These questions include:

- ☑ At what point in your migration plan should you move Exchange 5.5 data to Active Directory?
- ☑ Is it best to move it in the beginning to take advantage of the depth of information available?
- ☑ Or, is it more advantageous to wait and move your Exchange data after your Active Directory migration is complete?

Each organization will ultimately determine what is best for them, but for many organizations, moving Exchange 5.5 data to Active Directory in the early stages of their Windows 2000 migration is the preferred approach for the following reasons:

- **Exchange 5.5 is a real directory,** unlike the Windows NT SAM. Exchange 5.5 contains significantly more user information attributes than the Windows NT SAM, such as title, phone number, fax number, first name, last name, middle initial, address, company, department, office, e-mail and address.
- **Eliminates the need to manually add** or import the extra data values into Active Directory after the Windows NT SAM accounts have been migrated to Active Directory.
- By merging Exchange 5.5 and the Windows NT SAM up front, you **reduce the risk of data conflicts** causing user and resource access problems after you've moved Active Directory into production.

E-mail and messaging have become a mission-critical application for a majority of Global 2000 organizations, and as such, the data contained in an Exchange 5.5 directory represents a valuable corporate asset. This asset is one in which corporations have a sizable investment in creating and maintaining. It only stands to reason that corporations want to move this data to Exchange 2000. Therein lies the major reason for utilizing the ADC as a key component in a migration to Exchange 2000.

Challenges of Moving Exchange 5.5 Data to Exchange 2000

As with any complex process, moving Exchange 5.5 data to Active Directory requires planning. One of the biggest challenges of moving to Exchange 2000 is the consolidation of Windows NT 4.0 SAM information and Exchange 5.5 Directory Service information into Active Directory (AD). Binding these two data sources together and guaranteeing the integrity of directory information is absolutely critical. Best practices suggest assessing and cleaning up your Exchange 5.5 data prior to running the ADC. Otherwise, you run the risk of creating mail-enabled Windows 2000 user accounts and distribution groups for users and distribution lists that no longer exist or are needed. Other ramifications of using the ADC include:

☑ *Duplicate Active Directory (AD) accounts*

The ADC creates a mail-enabled Windows 2000 account, independent of the Windows 2000 account created by migrating the Windows NT SAM user account to Active Directory. In addition to creating administrative havoc, duplicate accounts will cause problems with Exchange 2000. Unlike Exchange 5.5, Exchange 2000 and Active Directory allow only one mailbox per user account. Therefore, in order for each user account to receive e-mail, duplicate accounts must be cleaned up. Microsoft's and other vendors' solution to this problem is to run a cleanup utility (AD Clean) that finds and merges duplicate accounts.

☑ *Conflicting account properties*

In many organizations, user account information in Exchange 5.5 may not match exactly the user account information in the Windows NT SAM. This results from either inaccurate data or different standards applied by different administrators in creating the accounts. Additionally, the ADC creates accounts based on the Exchange Alias, which may or may not match the Windows NT account name. Either way, as the data is merged into Active Directory, decisions need to be made about which source field will be used to prevent large amounts of account cleanup after the ADC is run.

☑ *AD store bloat from tombstone accounts*

Duplicate account creation results in a bloated Active Directory. AD Clean merges the duplicate accounts into one, but you are still left with tombstone records tying up disk space and possibly affecting AD performance.

☑ *Placement of accounts in proper AD container or OU*

The ADC enables you to specify the destination container (OU) in AD where the mail-enabled accounts will be created. This all-or-nothing approach provides little flexibility in placing user accounts in the proper OU container in AD.

☑ *Access to Exchange 5.5 resources during the transition to Exchange 2000*

The primary goal of any migration is to eliminate any impact on end users. As you transition to Exchange 2000, users will still need full access to their Exchange 5.5 mailboxes, distribution lists, calendars, and public folders.

All of these issues can be avoided by using bv-Admin for Windows 2000 Migration.

How Can BindView Help?

Clean up NT and Exchange 5.5 Directory Data

Before the migration to Active Directory begins, the preparation must be complete. This important "cleanup" step includes eliminating duplicate and stale users, groups, mailboxes and distribution lists. It is also a good strategy to determine which Windows NT accounts are associated with multiple Exchange 5.5 mailboxes, as well as to determine if Exchange aliases map to Windows NT SAM user names.

BindView's unique "find and fix" feature in bv-Admin for Windows 2000 Migration, and in bv-Control for Microsoft Exchange, allows you to quickly and effectively scrub the Windows NT SAMs and the Exchange 5.5 Global Address Lists. Servers can be consolidated before the move, to reduce the number of objects involved.

The benefit that BindView's Exchange migration solution delivers is found when:

- only those objects that need to be migrated are migrated.
- the "right" Windows 2000 user account is associated with the "right" Exchange 2000 mailbox.
- Exchange 5.5 directory information is complete and accurate, so that the correct associations are made.
- the entire migration process is simplified and expedited.

Consolidate NT SAM & Exchange 5.5 into Active Directory

Once you make sure that your source data is in good shape, you need to consider how you are going to consolidate these two data sources into Active Directory. Microsoft provides the foundation to accomplish this integration. If you are planning to deploy Exchange 2000 with your existing Exchange 5.5 mailbox and directory information, Microsoft requires that you establish Microsoft's Active Directory Connector (ADC) connection agreements between Active Directory and all Exchange 5.5 sites. ADC prepares your Active Directory environment for Exchange 2000. Additionally, ADC allows all users in the enterprise, whether on Active Directory or Exchange 5.5, to share a single Global Address List. The ADC synchronizes the Exchange directory information with Active Directory.

When you initially set up the ADC, you create a connection agreement in which you specify what recipients' containers to copy to AD and where (the container or organizational unit (OU)) you want to

copy it. You can copy account information from your Exchange 5.5 recipient containers (every mailbox account in a recipient container will be copied over, although you can choose to not bring over custom recipients and public folder mailboxes). All accounts in a connection agreement are copied into the same destination container or OU, and you cannot have more than one connection agreement for the same container. In addition, each connection agreement supports a single Exchange site, so if you have a multi-site Exchange organization, you will need to create multiple connection agreements. You can also specify whether or not ongoing changes made in Exchange 5.5 are to be applied to AD (one-way replication) or have the option for any changes made in AD to be applied to the Exchange 5.5 directory (two-way replication). ADC creates accounts using the Exchange alias, which may or may not match your Windows NT 4.0 account names.

Before you can establish a connection agreement, the ADC must extend the Active Directory schema (i.e., it makes 430+ schema changes!) to support the replication between Exchange 5.5 and Active Directory. This process also creates new AD user accounts, populates the extended attributes with information from the Exchange 5.5 mailbox, mail-enables the AD user account, and (optionally) disables the new AD user account.

bv-Admin for Windows 2000 Migration is ADC Aware

The next logical step in your migration process is to move all of your Windows NT 4.0 user accounts to the new AD environment. This is where BindView's bv-Admin for Windows 2000 Migration software can save you a lot of trouble, because it is the only "ADC-Aware" migration software available.

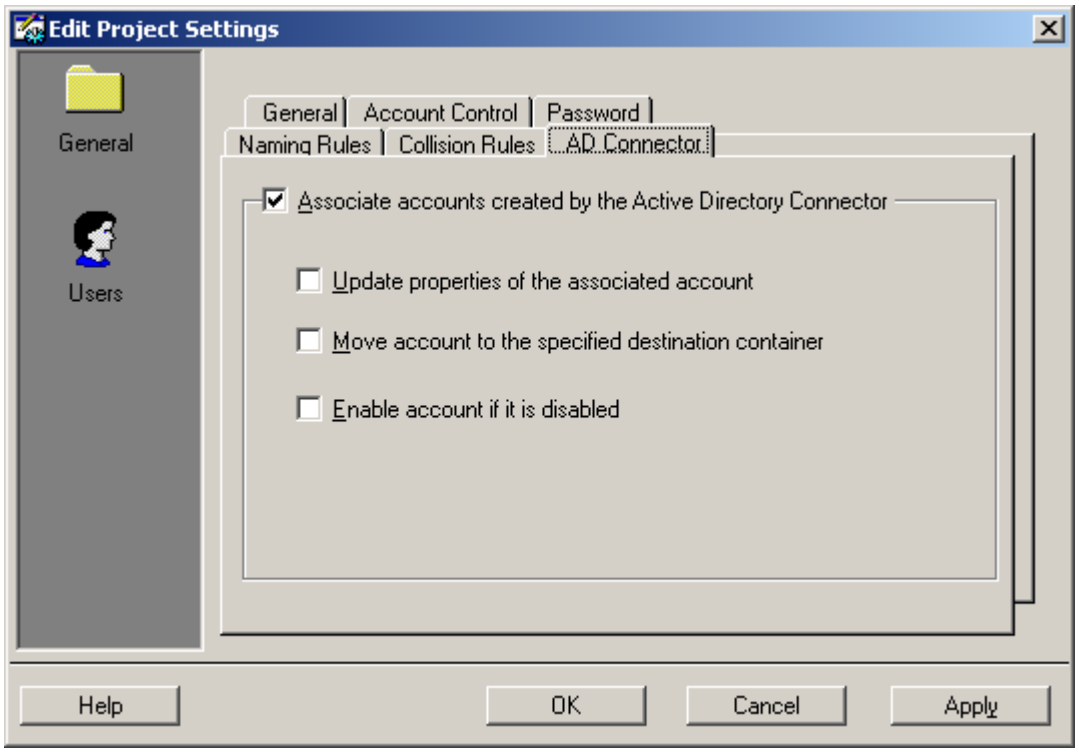

Figure 1: BindView's bv-Admin for Windows 2000 Migration provides account association.

What does "**ADC Aware**" mean? It means that when you create a migration project, you can specify what to do with ADC-created accounts. bv-Admin for Windows 2000 Migration recognizes that the ADC already created a user account in AD, and won't create another one when it migrates the Windows NT 4.0 account to Active Directory. Instead, it will simply populate the account created by the ADC with the appropriate

information from the old Windows NT 4.0 account, and move that account to the destination container you specify, while leaving the replication with Exchange 5.5 intact. You can also choose whether or not to enable the AD account. bv-Admin also provides you with several options for choosing how to update your AD account properties (e.g., User Principal Name, Display Name), as these values may differ between the two data sources.

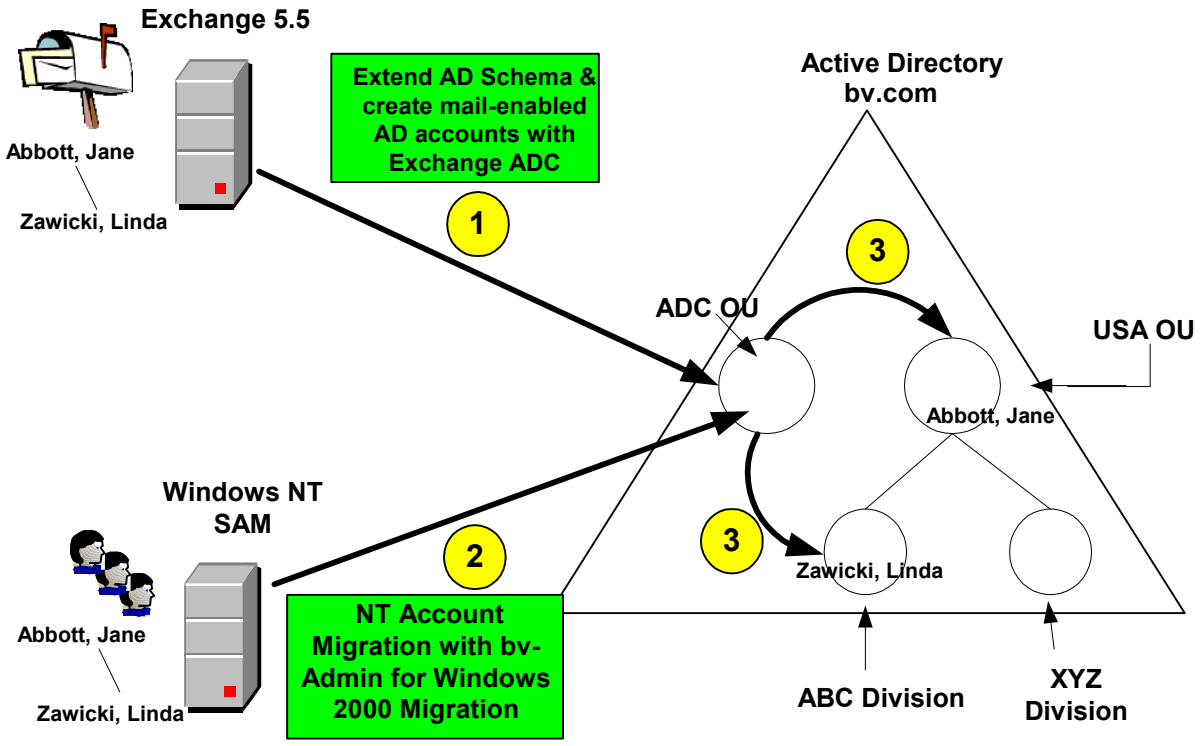

Figure 2: BindView's bv-Admin for Windows 2000 Migration allows you to merge migrating NT user accounts with ADC accounts during the user migration.

Step 1: ADC prepares Active Directory for Exchange. This includes schema extensions and creates mail-enabled user accounts. These accounts are created in one AD container (OU).

Step 2: Migrate Windows NT user accounts with bv-Admin for Windows 2000 Migration. bv-Admin first checks to see if an ADC account already exists and if found, associates the NT user properties with the ADC-created user account. This prevents duplicate accounts.

Step 3: bv-Admin for Windows 2000 Migration offers the option to move the updated ADC-generated user account to another destination in AD, enabling you to repopulate other OUs within the domain with the appropriate user accounts.

Ensure Access to Exchange Resources

This step requires Update to Security Permissions for Exchange 5.5 Resources. If you want your users to start logging in under their new AD accounts and you are not using SID History to migrate your Windows NT 4.0 accounts, then you must perform one additional step: You must use bv-Admin for Windows 2000

Migration to update the security permissions on the Exchange 5.5 directory to give the new AD account access rights. The new AD user becomes the primary user account and the Windows NT 4.0 user account becomes a secondary account. Both accounts retain full access to the mailbox and other Exchange directory objects (e.g., distribution lists, public folders) until the old Windows NT 4.0 account is disabled and/or the AD account is enabled.

At this point, you have a single AD user account in its proper location in AD with all of its security and mailbox information—ready to become the Exchange 2000 mailbox account when Exchange 2000 is loaded and the mailbox contents are migrated.

Understanding the Implications of "Tombstone" Accounts

Microsoft's own ADMT, as well as all third-party migration software other than bv-Admin for Windows 2000 migration, creates a second user account instead of recognizing the one that already exists. Not only do these other products require additional steps or utilities to merge the information and delete one of the two accounts, but more importantly, they produce tombstone accounts in AD. If you delete an account in AD, it is marked as deleted instead of being removed from the directory. After a preset interval (by default, 60 days), these accounts are removed through a process called online de-fragmentation. However, this de-fragmentation does not free up the space occupied by those deleted accounts, even after they have been permanently removed. This means that using a non-ADC-aware migration product could effectively double the size of your AD store, which creates needless additional replication traffic in the short term. And in the long term, a bloated AD store complicates disaster recovery because of the additional time required to back up and restore the AD store. The only way to recover the space occupied by deleted accounts is to take each domain controller offline, boot into directory restore mode, and perform an offline de-fragmentation. For many large enterprises, this amount of downtime is unacceptable.

Conclusion

If you are planning to migrate to Exchange 2000 using Microsoft's upgrade path, then bv-Admin for Windows 2000 Migration can reduce the time and effort associated with a migration project. Avoid the costs associated with poor data integrity, duplicate accounts and tombstones in Active Directory, and lack of access to un-migrated Exchange 5.5 resources during the transition to Exchange 2000.

For more information on our products, please visit our site http://www.bindview.com or call your local sales representative.