IBM Tivoli Access Manager

IBM Tivoli Access Manager Aelita Enterprise Directory Manager Integration Guide

Version 1.0

SC32-1124-00

IBM Tivoli Access Manager

IBM Tivoli Access Manager Aelita Enterprise Directory Manager Integration Guide

Version 1.0

SC32-1124-00

Note

Before using this information and the product it supports, read the information in Appendix B, "Notices", on page 19

First Edition (December 2002)

© Copyright International Business Machines Corporation 2002. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface v
Who Should Read This Guide v
Related Documents v
Base Information v
WebSEAL Information v
IBM Tivoli Access Manager Online Publications vi
IBM Tivoli Access Manager Web Information vi
Contacting Customer Support vi
Providing feedback about publications vi
Conventions Used in This Guide vii

Chapter 1. Introducing Tivoli Access Manager Integration with Aelita Enterprise Directory Manager 1
Integration Product Version Information 1

Chapter 2. Pre-Installation Tasks 3
Install and Configure Microsoft Internet Information Services 3
Install and Configure Microsoft Active Directory 3
Install and Configure Aelita Enterprise Directory Manager 3
Tivoli Access Manager Configuration 3

Chapter 3. Installation 5
Integration Components and Functions 6
The Tivoli Access Manager and Aelita Integration Script 6
Creating a New Policy Object 7
Required Changes 8
Enforcing Policy Objects 9

Chapter 4. Testing the Integration 11

Chapter 5. Security and Management Considerations 13

Chapter 6. Removing the Integration 15

Appendix A. Integration Related pdadmin Commands 17

Appendix B. Notices 19
Trademarks 20

© Copyright IBM Corp. 2002

Preface

This guide tells you how to configure and manage your IBM® Tivoli® Access Manager installation to work with Aelita® Enterprise Directory Manager™.

Who Should Read This Guide

This guide is for those responsible for the installation, deployment and administration of IBM Tivoli Access Manager and Aelita Enterprise Directory Manager.

Readers should be familiar with the following:

- PC and UNIX® operating systems.
- Security management
- Internet protocols, including HTTP, HTTPS and TCP/IP
- Microsoft® Active Directory®
- Microsoft Visual Basic® Scripting Edition
- Authentication and authorization

The reader should also be familiar with the administration of Tivoli Access Manager, Tivoli Access Manager WebSEAL and Aelita Enterprise Directory Manager.

Related Documents

These manuals complement the information contained in this document:

Base Information

- *IBM Tivoli Access Manager Base Installation Guide*

  Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Tivoli Access Manager Base Administrator's Guide*

  Describes the concepts and procedures for using Access Manager services. Provides instructions for performing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Tivoli Access Manager WebSEAL Installation Guide*

  Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*

  Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

© Copyright IBM Corp. 2002

- *IBM Tivoli Access Manager WebSEAL Developer's Reference*

  Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

IBM Tivoli Access Manager Online Publications

IBM Tivoli Access Manager publications are provided in Portable Document Format (PDF) and HTML format on the Tivoli Information Center Web site:

http://www.tivoli.com/support/documents/

IBM Tivoli Access Manager Web Information

IBM and Tivoli customers can find online information for Tivoli security products and for IBM Tivoli Access Manager for e-business.

For information about IBM Tivoli Access Manager for e-business, visit this Web site:

http://www.tivoli.com/products/index/access-mgr-e-bus/

For information about other Tivoli security management products, visit this Web site:

http://www.tivoli.com/products/solutions/security/

Contacting Customer Support

If you have a problem with any Tivoli product, you can contact IBM Customer Support for Tivoli products. See the *Tivoli Customer Support Handbook* at the following Web site:

http://www.tivoli.com/support/handbook/

The handbook provides information about how to contact Customer Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- What information to gather before contacting Customer Support

Providing feedback about publications

If you have comments or suggestions about Tivoli products and documentation, send an e-mail to pubs@tivoli.com or complete the customer feedback survey at the following Web site:

http://www.tivoli.com/support/survey/

Conventions Used in This Guide

The following typeface conventions are used in this book:

Bold Command names and options, keywords, and other information that you must use literally appear in **bold**.

Italic Variables, command options, and values you must provide appear in italics. Titles of publications and special words or phrases that are emphasized also appear in *italics*.

`Monospace` Code examples, command lines, screen output, file and directory names, and system messages appear in `monospace` font.

Chapter 1. Introducing Tivoli Access Manager Integration with Aelita Enterprise Directory Manager

The Tivoli Access Manager integration with Aelita Enterprise Directory Manager uses the policy capabilities and Software Development Kit from Aelita to perform scripted actions when events occur in Enterprise Directory Manager. When an Enterprise Directory Manager event occurs that involves users or groups, a policy script calls the **pdadmin** command line utility to perform Tivoli Access Manager tasks to reflect Active Directory® changes in the Tivoli Access Manager policy data. The integration scripts can be further extended to provide high-level error checking and handling, and includes the potential to perform further Tivoli Access Manager tasks.

Integration Product Version Information

This integration solution has been tested on, and is supported for, the following product versions:

- IBM Tivoli Access Manager Version 4.1
- Aelita Enterprise Directory Manager Version 4.1

The host operating system used during testing was Microsoft Windows® 2000 Advanced Server.

This document assumes there is a Tivoli Access Manager environment installed, configured and running, and Aelita Enterprise Directory Manager is installed, configured and running. This guide does not provide details on the installation and administration of these products.

© Copyright IBM Corp. 2002

Chapter 2. Pre-Installation Tasks

The tasks documented in this chapter should be completed prior to beginning the integration. The following topics are covered in this chapter:

- "Install and Configure Microsoft Internet Information Services"
- "Install and Configure Microsoft Active Directory"
- "Install and Configure Aelita Enterprise Directory Manager"
- "Tivoli Access Manager Configuration"

Install and Configure Microsoft Internet Information Services

In order to use the Web based administration console, the Web server component of Microsoft Internet Information Services (IIS) needs to be installed on the machine where the Aelita Enterprise Directory Manager is installed.

Refer to the Windows Server platform documentation for details on installing and configuring IIS.

Install and Configure Microsoft Active Directory

Aelita Enterprise Directory Manager must be installed into a Windows 2000 domain environment. Enterprise Directory Manager does not need to be installed on the Domain controller, but the machine where it is installed must be a member of the domain, and must be logged on as an Administrator of the domain when using the Enterprise Directory Manager.

Configure Active Directory using the tool provided within Windows 2000 Server and above. This is available from the *Configure Your Server* application in the *Administrative Tools* program group.

Install and Configure Aelita Enterprise Directory Manager

Before the integration can occur, Aelita must be configured to manage at least one Windows 2000 domain. Follow the instructions in the *Aelita Enterprise Directory Manager 4.1 - Installation Guide* for details on installing Aelita Enterprise Directory Manager, prerequisite software and licensing.

Refer to the *Aelita Enterprise Directory Manager 4.1 - User's Guide* for instructions on managing a domain and creating, installing and enforcing policies for the domain through the Enterprise Directory Manager.

Refer to the *Aelita Enterprise Directory Manager 4.1 - Web Interface User's Guide* for details on the Web interface.

Tivoli Access Manager Configuration

Ensure that Tivoli Access Manager is installed on a registered computer object within the managed Active Directory domain and you have logged on to the machine as an administrator of that domain.

© Copyright IBM Corp. 2002

Once you have installed the required Tivoli Access Manager 4.1 components, you need to configure them through the *Configuration* icon in the *Tivoli Access Manager for e-business* program group in the Windows *Start* menu.

Configure the Runtime Environment and Policy Server against the Active Directory configured for Aelita Enterprise Directory Manager.

Refer to the *IBM Tivoli Access Manager Base Installation Guide* version 4.1 for details on configuring Tivoli Access Manager to use Microsoft Active Directory.

Chapter 3. Installation

This chapter contains the following sections:

- "Integration Components and Functions" on page 6
- "The Tivoli Access Manager and Aelita Integration Script" on page 6
- "Creating a New Policy Object" on page 7
- "Enforcing Policy Objects" on page 9

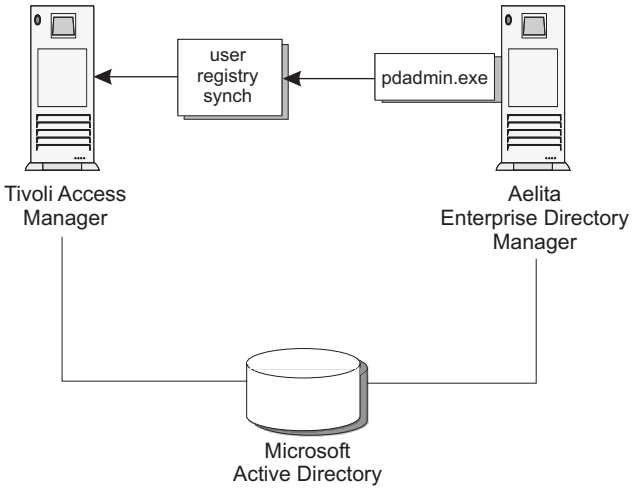
When a managed item (*User*, *Group*, *Computer*, *Contact*, *Shared Folder*) is created, deleted, modified, moved or renamed, an event is triggered prior (onPre) to the change being committed to Active Directory and another once the change has been committed (onPost). Using the Software Development Kit (SDK), the triggered events can be intercepted and a script run associated with the event. The Aelita SDK documentation contains details on Aelita events and their characteristics.

VBScript is used to perform calls to the Tivoli Access Manager command line utility, **pdadmin**, to reflect changes introduced by Enterprise Directory Manager in the Tivoli Access Manager policy data. A series of VBScript subroutines handle events that have a potential impact on the Tivoli Access Manager policy data. In particular the scripts: create, delete, modify attributes, rename and move, users and groups.

It is possible to manage other objects in Enterprise Directory Manager such as computers, contacts and network shares. However, these objects do not affect Tivoli Access Manager and these object events must be separated from valid user and group events.

This integration includes sample VBScripts that handle user and group events triggered by changes in Enterprise Directory Manager.

The Aelita Web-based front-end for the Enterprise Directory Manager can also be used to manage the Active Directory, which will still trigger the Tivoli Access Manager integration event handlers. Any errors for policy violation are displayed in a HTML page rather than a message box.



© Copyright IBM Corp. 2002

Figure 1. Component architecture of the Tivoli Access Manager Aelita Enterprise Directory Manager integration.

Integration Components and Functions

The integration package contains the following files:

`am_aelita_int_guide.pdf`	This document, which details how to achieve integration between Tivoli Access Manager and Aelita Enterprise Directory Manager.
`amAelitaIntegration.vbs`	A series of VBScript subroutines and functions that handle the event triggers from Aelita Enterprise Directory Manager. This file is imported into the Policy Objects of Aelita Enterprise Directory Manager and should then be deleted from the file system, as it contains the username and password for a Tivoli Access Manager security user in the iv-admin group.
`pdadmin_wrapper.bat`	A DOS batch script used when extended logging is switched on in the script to record the **pdadmin** error codes and text. The script accepts multiple arguments to write the log file and execute the request command by calling **pdadmin**. Copy this file to the `bin` directory of the Tivoli Access Manager installation (typically `%pd_home%\bin`) on the machine where the Aelita Enterprise Directory Manager is installed and running.

The Tivoli Access Manager and Aelita Integration Script

The `amAelitaIntegration.vbs` script included with the integration package contains all the base functionality for integrating Tivoli Access Manager with Aelita Enterprise Directory Manager. If required, the script can be further developed to add extra error checks and handling. For instance, you may want to extend the script to prevent the temporary command file from being deleted. With further code modification the script can be used as an undo log, or as a store of failed events, ready for execution when the Policy Server becomes available again.

The Windows Event Viewer also captures event notifications, which are useful in resolving errors encountered when performing actions in the Enterprise Directory Manager.

The following events are handled by the Tivoli Access Manager integration script:

- User and Group creation.
- User and Group deletion.
- User and Group description.
- Prevents the change of the UserID of GroupID (common link between Tivoli Access Manager and Aelita).
- Synchronizes *Account Disabled* in Aelita with *account-valid* in Tivoli Access Manager.
- Prevents users and groups from being moved between containers.

Creating a New Policy Object

`amAelitaIntegration.vbs` must either be imported into the Aelita Policy Objects container or copied and pasted as a new policy object. If there are currently other script policies in place that utilize the onPre and onPost event handlers, the Tivoli Access Manager integration script subroutines must be merged into the existing policy. Importing the Tivoli Access Manager integration script without merging the existing event handlers causes them to be overwritten.

Refer to the section *Managing Policy Objects* in the *Aelita Enterprise Directory Manager 4.1 - User's Guide* for details on importing policy objects into Aelita.

Below is an overview of the event handlers required for Tivoli Access Manager integration.

Creating Users and Groups

When a user or group is created in Enterprise Directory Manager, the user or group is also automatically imported into Tivoli Access Manager. Before the changes are committed to the Active Directory a check is made to determine if the Policy Server is contactable and the security user and password supplied are valid. This ensures that changes made in Active Directory which affect the integration can only be commited when the Tivoli Access Manager Policy Server is responding and the authentication is correct. If the Policy Server is not contactable or an incorrect username and password are supplied, the import into Tivoli Access Manager fails, the creation in Enterprise Directory Manager is cancelled, and an error message is returned to the user.

Tivoli Access Manager users are imported as GSO users with the account-valid flag set to *yes*. You will need to adjust the **onPostModify** event to disable the GSO option if required.

You should perform all user and group management through either the Aelita MMC Snap-in console or the Aelita Web front-end rather than from the **pdadmin** command line.

Note: As Tivoli Access Manager is a security based software suite, only *Global Security* groups from Active Directory can be imported into it. As a result, the integration script handles only actions that affect *Global Security* groups. Other groups (*Local Security*, *Local Distribution*, *Global Distribution*, *Universal Distribution*) can be created using the Aelita Enterprise Directory Manager, but they will not be imported into Tivoli Access Manager and will not have their properties synchronized by the integration script when changes occur in the Enterprise Directory Manager.

The key requirements for importing are:

- User logon name or group name must have the domain name removed. For example, *logon@domain* must be changed to *logon*.
- Existence of the Distinguished Name (DN) for the user or group; for example, a user of *domainuser* in the Active Directory domain of *domainname* in the Users container would be CN=domainuser,CN=Users,DC=domainname

Deleting Users and Groups

Before a user is deleted from Active Directory, the Tivoli Access Manager policy data needs to be removed. Once the user or group has been successfully removed from Tivoli Access Manager the user is deleted from the Active Directory.

Modifying User or Group Attributes

The user logon name and group name are the key points to linking the Tivoli Access Manager UserID / GroupID with the policy data. When a user or group is modified, a check ensures the ID cannot be modified, as this would break the integration.

Further checks are also done to update the description of users and groups in Aelita with the description in Tivoli Access Manager and to synchronize the *Account Disabled* option in Aelita with the *account-valid* flag in Tivoli Access Manager.

Moving and Renaming Users and Groups

Renaming and moving have the same effect as changing the Distinguished Name (DN) of the user or group. As Tivoli Access Manager uses the ID to link the ID to the DN, these changes do not affect the integration, as they are picked up automatically when Tivoli Access Manager reads from Active Directory.

Care should be taken when moving users and groups between containers with respect to where the Integration policy has been enforced. If the policy is enforced on a container such as *Users* and a user is moved from this container to the root of the directory, the policy would no longer apply. This could mean descriptions, deletions, account properties and events would not be reflected in Tivoli Access Manager through the integration script. Likewise, if a user was created outside of the *Users* container then moved into it, they would not be imported and hence all Tivoli Access Manager integration events would fail. For this reason it is suggested that the policy be enforced at the root of the managed domain and the moving of users and groups be disabled. The integration script defaults to disallowing users to be moved from where the policy is enforced.

Required Changes

Once the script has been imported some changes are required to ensure successful operation.

1. Change the *authUser* and *authPwd* values.

   While these values appear in plain text, the script itself is stored in the SQL database—included with the Aelita installation—that limits the visibility of the values. Once the script has been imported, the file can be removed from the file system further reducing the possibility of an intruder obtaining a security user for Tivoli Access Manager.

   To enhance security it is advisable not to use the sec_master user in the script, rather include a user who is a member of the iv-admin Tivoli Access Manager group. For details on creating a security user, refer to Appendix A, “Integration Related pdadmin Commands”, on page 17.

2. Enable or disable trace logging or extended logging.

   To enable either of the logging options, ensure their value is *True*. Alternatively, use *False* to disable. Logging will increase the time required for each operation in the Aelita console.

   Trace logging provides the Tivoli Access Manager command, the return status of the execution, and a time stamp. Extended logging includes the same as trace logging, but also includes any Tivoli Access Manager return text explaining the error.

3. Set the logging directory.

   The default for both log types is in the Tivoli Access Manager logging directory. If these paths are changed, ensure the directory structure in the file name is also on the physical file system.

Enforcing Policy Objects

Once the script has been imported into the Policy Objects of Enterprise Directory Manager, it must be enforced in order for the appropriate event handlers to be triggered. It is advisable to enforce the policy at the domain level to ensure that if users and groups are moved between Containers or Organizational Units, the policy is still applied to users and groups that have already been imported.

Refer to the section *Administrative Policy Enforcement* in the *Aelita Enterprise Directory Manager 4.1 - User's Guide* for details on enforcing policy objects.

Chapter 4. Testing the Integration

After the integration is complete the, creation, deletion, modification, moving or renaming of users and groups in Active Directory should be reflected in the Tivoli Access Manager policy data.

Use the Tivoli Access Manager command line utility, **pdadmin**, to check that changes have occured successfully:

1. Open **pdadmin** and logon as a security user from the iv-admin group.

   ```
   pdadmin> login –a sec_master –p XXXXX
   ```

2. Use the *list* command to display a list of the users/groups that are recorded in Tivoli Access Manager. Specify all syntax matches and all users ensuring they have been created or deleted successfully.

   ```
   pdadmin> user|group list * 0
   ```

3. For further detail, use the show command to view the object details for a particular user or group.

   ```
   pdadmin> user|group show UserID|GroupID
   ```

Note: It is possible that a delay period between the Active Directory update and the Tivoli Access Manager update will occur. Refer to the *IBM Tivoli Access Manager Base Installation Guide* for details on this delay period and possible solutions to it.

© Copyright IBM Corp. 2002

Chapter 5. Security and Management Considerations

- The security user password is stored in clear text in the policy script. To enhance security, a standalone application could be written to save the security user and password in an encrypted file. In each event handler, a script could be added to open the file, read the encrypted username and password, and then decrypt them for use. Doing this may introduce further security concerns such as exposing the cipher and passing a non-numeric value from a shell to VBScript.
- All management of users and groups should be performed using Aelita Enterprise Directory Manager. Script functions other than those for the Tivoli Access Manager integration (for example, creating home directories or Exchange mail boxes) are not invoked.
- Care should be taken to ensure that any of the objects in the Tivoli PD Domains container are not modified, as this is where the Tivoli Access Manager policy data is stored. Altering objects and their properties in this container will not only break the integration, it could also break the Tivoli Access Manager environment.

© Copyright IBM Corp. 2002

Chapter 6. Removing the Integration

To remove the Tivoli Access Manager Aelita Enterprise Directory Manager integration:

1. Remove any enforcements of the Tivoli Access Manager integration script.
2. Remove the Tivoli Access Manager integration script from the Policy Objects.
3. Unconfigure Tivoli Access Manager (Refer below).
4. Manually remove the Tivoli Access Manager policy data from Active Directory by clicking on the Tivoli PD Domains container and deleting it.

On your Tivoli Access Manager Policy server:

1. Select Tivoli Access Manager Policy Server and click **Unconfigure**. Click **Yes** when the component unconfiguration window appears.
2. Select *Tivoli Access Manager Runtime* and click **Unconfigure**.
3. Click **Close** to exit the *Access Manager Configuration* window

Once you have unconfigured Tivoli Access Manager you can uninstall the components from the Windows 2000 Add/Remove Programs facility.

© Copyright IBM Corp. 2002

Appendix A. Integration Related pdadmin Commands

Although there are further options that can be specified when importing users and groups, they are not required as Tivoli Access Manager shares the Active Directory registry. This ensures that group memberships will be reflected in Tivoli Access Manager once a change is made in Enterprise Directory Manager.

Importing Users and Groups from Active Directory

User

```
pdadmin> user import "UserID" "UserDN"
pdadmin> user modify "UserID" account-valid yes
```

Group

```
pdadmin> group import "GroupID" "GroupDN"
```

Where: UserID and GroupID correspond to the Active Directory pre-Windows 2000 logon name.

Displaying Imported Users and Groups

User

```
pdadmin> user list * 0
```

Group

```
pdadmin> group list * 0
```

Where: UserID and GroupID correspond to the Active Directory pre-Windows 2000 logon name

Showing Details of Users and Groups

Users

```
pdadmin> user show "UserID"
```

Group

```
pdadmin> group show "GroupID"
```

Where: UserID and GroupID correspond to the Active Directory pre-Windows 2000 logon name

Deleting Users and Groups from Access Manager

User

```
pdadmin> user delete "UserID"
```

Group

```
pdadmin> group delete "GroupID"
```

Where: UserID and GroupID correspond to the Active Directory pre-Windows 2000 logon name

Creating a new Security User

Create a user in the Aelita console before importing the integration script. Manually import the user and add them to the iv-admin group.

```
pdadmin> user create "security_user" "CN=security_user_name,CN=Users,DC=domain"
pdadmin> user modify "security_user" account-valid yes
pdadmin> group modify iv-admin add "security_user"
```

© Copyright IBM Corp. 2002

Appendix B. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2002

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM

IBM(logo)
SecureWay
Tivoli
Tivoli (logo)
Universal Database
WebSphere
IBM-Lotus Trademarks
Domino
iNotes
Lotus Notes
Lotus
Notes

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.

Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Printed in U.S.A.

SC32-1124-00