

IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2

*AccessAgent on Virtual Desktop
Infrastructure Guide*



IBM® Security Access Manager for Enterprise Single
Sign-On
Version 8.2

*AccessAgent on Virtual Desktop
Infrastructure Guide*



Note

Before using this information and the product it supports, read the information in "Notices" on page 17.

Edition notice

Note: This edition applies to version 8.2 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724-V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2013.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Overview	1
Virtual desktop infrastructure.	1
Chapter 2. Configurations and limitations for a Virtual Desktop Infrastructure	3
Chapter 3. Single sign-on setup	5
Verifying the VDI environment	5
Creating the VDI machine policy template for the base image	5
Configuring the base image	6
Creating virtual desktop pools	8
Creating a machine catalog	9
Updating the base image after changes on the AccessAgent	9

Using AccessProfiles	10
--------------------------------	----

Chapter 4. User workflows for accessing the virtual desktop 11

Accessing the virtual desktop from client computer with AccessAgent installed	11
Accessing the virtual desktop from client computer without AccessAgent	12

Appendix A. Troubleshooting 13

Appendix B. VDI settings 15

Notices 17

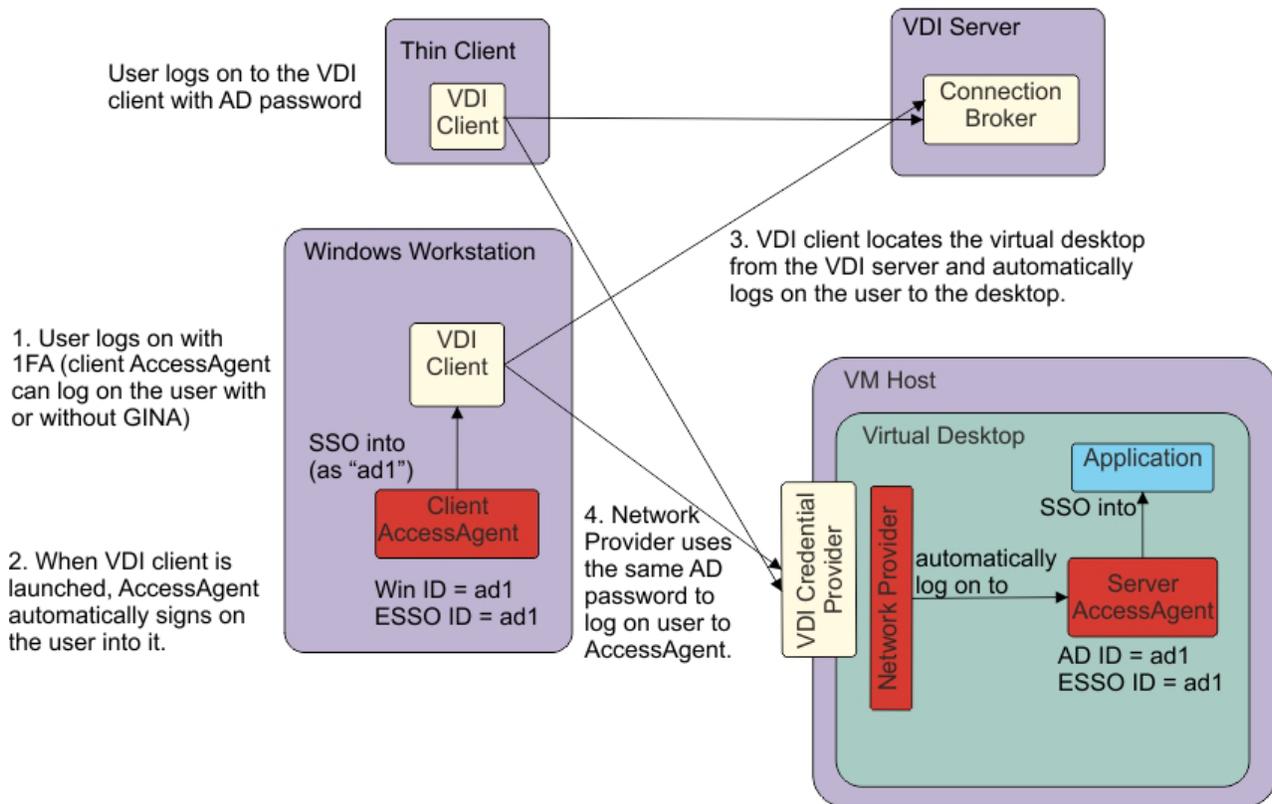
Chapter 1. Overview

A Virtual Desktop Infrastructure consists of desktop operating systems hosted within virtual machines on a centralized server. IBM® Security Access Manager for Enterprise Single Sign-On supports single sign-on to virtual desktops and applications on these virtual desktops through AccessAgent.

Users can access the virtual desktops and applications from a desktop PC client or thin client.

AccessAgent support for Virtual Desktop Infrastructure workflow

The following diagram describes the workflow for Virtual Desktop Infrastructure support.



Virtual desktop infrastructure

The Virtual Desktop Infrastructure consists of several components.

The following table lists the different VMware View Virtual Desktop Infrastructure and Citrix Virtual Desktop Infrastructure components.

Component	VMware View Virtual Desktop Infrastructure	Citrix Virtual Desktop Infrastructure
Client software	<p>VMware View Client</p> <p>This component is installed on all the computers and thin clients through which you want to access the virtual desktops.</p>	<p>Citrix Web Access</p> <p>This component provides users with web access to their virtual desktops.</p>
Base image agent	<p>VMware View Agent</p> <p>This component is installed on all the virtual desktop templates and pools that are remotely accessed through the VMware View Client. Use this component to register the computer with the server to gain access to the computer.</p>	<p>Virtual Desktop Agent</p> <p>The desktop-side components of Citrix XenDesktop.</p>
Connection server	<p>VMware View Composer</p> <p>Use this component to rebalance, recompose, or refresh desktop images regularly.</p>	<p>Citrix XenController</p> <p>This component creates and manages virtual desktops for users.</p>
Administrative console	<p>VMware View Administrator</p> <p>This component is available on the computer where you installed the VMware View Connection Server.</p>	<p>Citrix Desktop Studio</p> <p>The console from which Administrators can install, configure, create, and manage virtual desktops.</p>

Chapter 2. Configurations and limitations for a Virtual Desktop Infrastructure

This section describes the supported configurations and limitations for single sign-on on a Virtual Desktop Infrastructure.

AccessAgent configuration guidelines

The following configuration is supported:

- AccessAgent supports:
 - VMware View versions 4.5, 4.6, and 5.1
 - Citrix XenDesktop version 5.5 and 5.6
- The virtual desktop base image can be any of the following platforms:
 - Windows XP 32-bit
 - Windows 7 32-bit and 64-bit
- The virtual desktop can connect to the IMS Server.
- The user is registered to IBM Security Access Manager for Enterprise Single Sign-On.
- Active Directory password synchronization is enabled.
- EnNetworkProvider is enabled.

Note: When EnNetworkProvider is enabled, the Wallet caching option (`pid_wallet_caching_option`) policy is not respected. Wallet is always cached upon first logon from any virtual desktop.

- Personal desktop mode is supported. See *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide* for more information.

To achieve good performance:

- Ensure that the **Enhanced Cached Wallet Security** policy in the default machine policy template, is disabled.

The **Enhanced Cached Wallet Security** policy is used to bind Wallets to physical machines with unique characteristics. This policy is not suitable for the Virtual Desktop Infrastructure with provisioning. This policy cannot be overridden through a registry setting.
- Every *N* weeks, recompose the virtual desktop template after AccessAgent synchronizes with the IMS Server so that the latest system data is cached into the updated base image. Unnecessary data synchronizations are avoided when new virtual desktops are activated. This step is important for non-persistent desktops.
- For deployments with non-persistent desktops:
 - Allocate additional server capacity so that AccessAgent can download the user Wallet upon every logon.
 - Run the cached Wallet pruning script to remove expired and duplicated cached Wallets that are more than 30 days old in the IMS Server database.

Limitations

This supported configuration has the following limitations:

- Second-factor authentication is not supported on the virtual desktop.
- EnGINA and EnCredentialProvider are not supported on the virtual desktop.

Chapter 3. Single sign-on setup

To set up single sign-on support on a Virtual Desktop Infrastructure, Administrators must:

Table 1. Single sign-on setup

VMware	Citrix XenDesktop
<ol style="list-style-type: none">1. Verify the VDI environment.2. Create the VDI machine policy template for the base image.3. Configure the base image.4. Create virtual desktop pools. <p>For complete documentation, see "Creating Desktop Pools" from http://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.ICbase%2FPDF%2Fic_pdf.html.</p>	<ol style="list-style-type: none">1. Verify the VDI environment.2. Create the VDI machine policy template for the base image.3. Configure the base image.4. Create a machine catalog. <p>For complete documentation, see http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-create-new-scheme-rho.html.</p>
Optional tasks: <ul style="list-style-type: none">• Update the base image after changes on the AccessAgent.• Customize AccessProfiles.	Optional tasks: <ul style="list-style-type: none">• Update the base image after changes on the AccessAgent.• Customize AccessProfiles.

Verifying the VDI environment

An Administrator must verify the VDI environment before preparing the base image and the virtual desktops.

Using VMware View

Prepare the VMware components. See http://www.vmware.com/support/pubs/view_pubs.html for the product documentation.

1. Verify that the View Connection Server is running.
2. Verify that the VMware vCenter Server settings and the View Composer Settings are correct.

Using Citrix XenDesktop

Prepare the Citrix XenDesktop components. See <http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-install-wrapper-rho.html> for the product documentation.

Verify that the Citrix XenController is running.

Creating the VDI machine policy template for the base image

Use a machine policy template to apply a set of policies specific for Virtual Desktop Infrastructure support.

Procedure

1. Log on to AccessAdmin.
2. Select **Machine Policy Templates > New template**.
3. Set the name of the new template to VDI BaseImage MPT.

Note: The name is case-sensitive, so **Example** and **example** are two different template names.

4. Specify a criteria to assign a machine policy template. For example: **machine tag**.

Note:

- If you use machine tag, assign a name for it. The machine tag name must be the same with the value specified in the `VDI_config.reg` file. The default value is `vdi_tag_example`.
 - You can also use other criteria such as IP address, host name or others. See "Setting machine criteria" in the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.
5. Enable Network Provider in this machine policy template.
 - a. Navigate to **AccessAgent Policies > Logon/Logoff Policies**.
 - b. Set the value of **Enable Network Provider** to **Yes**.
 6. Click **Add** to save the new settings.
 7. Under **Machine Policy Assignment**, select the **VDI BaseImage MPT** template and click the **Up arrow** icon until the **VDI BaseImage MPT** is at the top of the **Machine Policy template assignments** list.
 8. Verify that the base image machine name is removed from the IMS Server using AccessAdmin.

Configuring the base image

An Administrator must configure AccessAgent on the base image to support single sign-on on a Virtual Desktop Infrastructure.

Before you begin

- Ensure that you have created the VDI BaseImage MPT machine policy template. See "Creating the VDI machine policy template for the base image" on page 5.
- Verify the VDI environment.
- Ensure that the VDI Agent is installed on the virtual machine before AccessAgent.
 - For VMware View: VMware View Agent
 - For Citrix XenDesktop: Virtual Desktop Agent
- Ensure that base image can communicate with VMware View or Citrix XenDesktop server. For example: `ping <server name>`
- Make a copy or know the location of the following files:
 - AccessAgent installer
 - `VDI_config.reg`. See Appendix B, "VDI settings," on page 15 for the content of this file.
- Verify that the base image machine name is removed from the IMS Server using AccessAdmin.

About this task

All virtual desktops are created from a base image. Different desktop pools use different base image.

This task consists of:

- Pre-configuring and installing AccessAgent.
- Configuring and applying the registry settings.

Procedure

1. Configure the SetupHlp.ini file in the AccessAgent installer.
 - a. Open the <AccessAgent_installer>\Config\SetupHlp.ini file with any file editor.
 - b. Set **EnginaEnabled** to 0. Default value is 1.
 - c. Set **EncentuateCredentialProviderEnabled** to 0. Default value is 1.
 - d. Set **DisableWin7CAD** to 0. Default value is 1.
 - e. Ensure that **EncentuateNetworkProviderEnabled** is set to 1. Default value is 1.
 - f. Save the file.
2. Copy the VDI_config.reg file into the <AccessAgent_installer>\Reg folder.

Important:

- Make sure that the **MachineTag** name in this registry file, is the same as the machine tag criteria specified in the **VDI BaseImage MPT** machine policy template. See step 4 on page 6 from “Creating the VDI machine policy template for the base image” on page 5.
 - Assign a proper VDI group name in the registry file. This can be your VDI pool name. The VDI group name that you specify in the registry file is used as the host name for managing the policies in AccessAdmin.
3. Install AccessAgent.
 - a. Set the IMS Server location.
 - b. Ensure that the machine Wallet is downloaded.

Note: The machine Wallet is not downloaded until you restart the computer.

AccessAgent automatically applies the SetupHlp.ini settings and the registry settings to the base image.

4. Verify that the correct **VDI BaseImage MPT** machine policy template is assigned to the base image.
 - a. Log on to AccessAdmin.
 - b. Search the machine and check the assigned template.
5. Restart the computer.
6. Install the latest fixpack (if any).
7. Log on to the computer through Windows logon with a domain account that is registered with the IMS Server.
8. Verify that you are automatically logged on to AccessAgent with the same domain account you used during the Windows logon.
9. Shut down the computer.

10. Take a snapshot of the virtual machine where you pre-configured and installed AccessAgent.
 - a. Assign a name for the virtual machine snapshot and provide a description for it.
 - b. Click **OK**.
 - c. Ensure that the snapshot is complete before you create a virtual desktop pool.

Results

AccessAgent is installed and with the required policies configured.

You created the base image to be used for the virtual desktops.

What to do next

- For VMware View: Create a virtual desktop pool.
- For Citrix XenDesktop: Create a machine catalog.

Creating virtual desktop pools

Create pools of desktops to deliver View desktop access to users. You can choose from automated pool or manual pool.

Before you begin

Complete the following tasks:

- "Verifying the VDI environment" on page 5.
- "Configuring the base image" on page 6.

About this task

This task is intended for Administrators.

Administrators must see "Creating Desktop Pools" and "Entitling Users and Groups" in the http://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.ICbase%2FPDF%2Fic_pdf.html for the detailed steps and explanations. This is a high-level procedure for VMware View Virtual Desktop Infrastructure.

Procedure

1. Log on to the VMware View Administrator with a domain user account.
2. Select **Inventory > Pools**.
3. Click **Add** to start the Add Pool wizard.
4. Follow the wizard. Select the settings as per your requirement.
5. When configuring the vCenter settings, select the snapshot of the base image that has the installation of AccessAgent.
6. Follow the wizard. Select the settings as per your requirement.
7. Double-click the desktop pool that you created to view the details and for additional configurations.
8. Select the users who can access the desktops in the pool you created.
9. Click **OK**.

Results

The desktop pool is created and users are assigned to the desktop pool.

Users can start accessing the virtual desktops created from the desktop pool.

Creating a machine catalog

In Citrix XenDesktop, create a Catalog of machines and desktop groups to deliver desktops to users.

Before you begin

Complete the following tasks:

- “Verifying the VDI environment” on page 5.
- “Configuring the base image” on page 6.

About this task

This task is intended for Administrators.

See <http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-create-new-scheme-rho.html> for the detailed steps and explanations. This is a high-level procedure for Citrix XenDesktop.

Procedure

1. Log on to Citrix Desktop Studio with a domain user account.
2. Click **Machines > Create Catalog**.
3. Follow the wizard. Select the settings as per your requirement.
4. On the **Master Image** page, select the snapshot of the base image that has the installation of AccessAgent.
5. Follow the wizard. Select the settings as per your requirement.

Results

You have a Catalog of machines. To deliver desktops to users from your Catalog, allocate the machines to users by creating desktop groups. See <http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-create-desktops-t-rho.html>

Users can start accessing the virtual desktops created from your Catalog.

Updating the base image after changes on the AccessAgent

Update AccessAgent in the base image to apply a fix pack or change a registry policy.

About this task

This task is intended for Administrators.

Procedure

1. Log on to the virtual machine you used for the base image.
2. Update AccessAgent in the base image. You can update AccessAgent by:

- Applying the latest AccessAgent fix pack.
 - Updating the registry policies. See Appendix B, “VDI settings,” on page 15 for the configurable policies.
3. Wait for AccessAgent to synchronize with any changes in the system policies and AccessProfiles.
 4. Take a snapshot of the virtual machine where you applied the fix pack.
 5. If you are using VMware View:
 - a. Log on to the VMware View Administrator.
 - b. Select the desktop pool.
 - c. Open VMware View Composer.
 - d. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.
 6. If you are using Citrix XenDesktop:
 - a. Log on to the Citrix Desktop Studio.
 - b. Click **Machines**.
 - c. Select your Catalog.
 - d. Click **Update machine**.

Related information:

Updating User Desktops: <http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-update-master-vm-rho.html>

Using AccessProfiles

Use an AccessProfile to automatically log on the user to the VDI portal.

The AccessProfile can be used if there is an AccessAgent installed in the client computer. The AccessProfile is used with AccessAgent to single sign-on the user to the VDI portal. The AccessProfile uses automatic authentication service. You can customize this profile to use domain authentication service.

Table 2. AccessProfiles

AccessProfile for	File name
VMware View	VMWareViewClient.eas
Citrix XenDesktop	XenDesktopWebAccess.eas

Important: If you are using Citrix XenDesktop, update the XenDesktopWebAccess.eas profile. Edit the site signature to match the actual Citrix Web Access URL. See the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide* for the procedure.

Chapter 4. User workflows for accessing the virtual desktop

Users can log on to a virtual desktop from a computer with AccessAgent or from a thin client.

The following topics describe the differences between these workflows.

- “Accessing the virtual desktop from client computer with AccessAgent installed”
- “Accessing the virtual desktop from client computer without AccessAgent” on page 12

Accessing the virtual desktop from client computer with AccessAgent installed

If users use a local computer with an installed AccessAgent, they can automatically log on to the virtual machine and on the selected virtual desktop.

Using VMware

1. Verify that you have the following components installed on the client computer:
 - VMware View Client
 - AccessAgent
2. Ensure that you have a VMware AccessProfile.
3. On your local computer, log on to AccessAgent.
4. Open the VMware View Client.
5. Specify the **Connection Server** IP address or host name.
6. Click **Connect**. The Log On window is displayed.
7. Select the virtual desktop you want to use.
8. Click **Connect**.

Using Citrix XenDesktop

1. Verify that you have the following components installed on the client computer:
 - Citrix Online Plug-in or Citrix Receiver
 - AccessAgent
2. Ensure that you have a Citrix XenDesktop AccessProfile.
3. Ensure that you installed the Citrix plugin. Otherwise, you are prompted to install the plugin when you log on to Citrix Web Access.
4. Open Citrix Web Access. For example: `http://<server name>\Citrix\DesktopWeb`.
5. Select the virtual desktop or desktop group.

Results

You are connected to the selected virtual desktop.

You are automatically logged on to AccessAgent in the virtual desktop.

You can single sign-on to applications in the virtual desktop.

Accessing the virtual desktop from client computer without AccessAgent

Users can access a virtual desktop from a thin client or from a local computer without an installed AccessAgent. In this scenario, users are not automatically logged on to the virtual machine.

Using VMware

1. Verify that you have a VMware View Client installed.
2. Open the VMware View Client.
3. Specify the **Connection Server** IP address or host name.
4. Click **Connect**. The Log On window is displayed.
5. Enter your domain user account password.
6. Click **Login**.
7. Select the virtual desktop to be used.
8. Click **Connect**.

Using Citrix XenDesktop

1. Verify that you have a Citrix Online Plug-in or Citrix Receiver installed.
2. Ensure that you installed the Citrix plugin. Otherwise, you are prompted to install the plugin when you log on to Citrix Web Access.
3. Open Citrix Web Access. For example: `http://<server name>\Citrix\DesktopWeb`.
4. Log on with your user name and password.
5. Select the virtual desktop or desktop group.

Results

You are connected to the selected virtual desktop.

You are automatically logged on to AccessAgent in the virtual desktop.

You can single sign-on to applications in the virtual desktop.

Appendix A. Troubleshooting

You might encounter issues when accessing the virtual desktop. Misconfiguration can cause these issues.

Misconfiguration issues

Issue 1: Logon to Windows succeeded. Log on to AccessAgent using EnNetworkProvider failed.

Symptom: When user logs on to the virtual desktop, VMware View Client automatically logs on the user to Windows. However, the user is not automatically logged on to AccessAgent.

Cause: Any of these factors can cause this issue:

- Active Directory password synchronization is not enabled.
- The **VDI BaseImage MPT** machine policy template is not applied in the base image.
- The required registry settings are not applied in the base image. See Appendix B, “VDI settings,” on page 15.
- The virtual machine cannot connect to the IMS Server and there is no cached Wallet.

Solution:

- Verify that the Active Directory password synchronization is enabled.
- Verify that EnNetworkProvider is enabled in the **VDI BaseImage MPT** machine policy template and that this template is applied to the base image and virtual desktops. See “Creating the VDI machine policy template for the base image” on page 5.
- Make sure that the **VDI BaseImage MPT** machine policy template is at the **top** of the Machine Policy template assignments list. See step 7 on page 6 from “Creating the VDI machine policy template for the base image” on page 5.
- Verify that automatic logon succeeds in the base image.
- The virtual machine can connect to the IMS Server.

Issue 2: Logon to Windows failed. ESSO GINA or ESSO Credential Provider is displayed.

Symptom: When user logs on to the virtual desktop through VMware View Client, the user is not automatically logged on to Windows. The user is prompted with the ESSO GINA or ESSO Credential Provider.

Cause: The required AccessAgent installer settings were not configured before AccessAgent was installed in the base image.

Solution:

1. Uninstall AccessAgent from the base image.
2. Reconfigure the base image.

Important: Ensure that the **EnginaEnabled** and **EncentuateCredentialProviderEnabled** settings in the AccessAgent installer are set to 0.

3. Log on to the VMware View Administrator.

4. Select the desktop pool.
5. Open VMware View Composer.
6. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.

Issue 3: Logon to Windows failed. Microsoft Credential Provider is displayed.

Symptom: When user logs on to the virtual desktop through VMware View Client, the user is not automatically logged on. The user is prompted with the Microsoft Credential Provider. This issue occurs only in Windows 7.

Cause: The **DisableWin7CAD** setting in the AccessAgent installer is not configured correctly.

Solution:

On the base image:

1. Open the Local Security Policy Console.
 - a. Click the **Start** menu.
 - b. Type Local Security Policy.
 - c. Press **Enter**.
2. Expand the **Local Policies**.
3. Click **Security Options**.
4. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**.
5. Select **Disabled**.
6. Click **OK**.
7. Log on to the VMware View Administrator.
8. Select the desktop pool.
9. Open VMware View Composer.
10. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.

Appendix B. VDI settings

Ensure that you apply the required registry settings to support Virtual Desktop Infrastructure.

Required registry settings

The settings required for Virtual Desktop Infrastructure support are:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISAM ESSO\DeploymentOptions]
"VDIGroupName"="vdi_pool_example"
"MachineTag"="vdi_tag_example"
```

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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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.

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 document 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 measurement 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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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



Java[™] and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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



Printed in USA