IBM Vault Registry

Configuring Multiple CA Agents

IBM Vault Registry

Configuring Multiple CA Agents

Contents

© Copyright IBM Corp. 1999

Chapter 1. Overview

This document addresses ways to improve the performance of your IBM Vault Registry system with respect to the number of certificate applications it can process within a given timeframe. The document assumes that you have a working knowledge of AIX and have experience installing and configuring the Vault Registry system. Examples used throughout the document are based on the Vault Registry default configuration with the assumption that you will adapt the procedures to your environment using your organization's names and naming conventions.

The default configuration of Vault Registry assumes that there is a one-to-one correspondence between the certificate authority (CA) and the CA Agent, as shown in Figure 1 on page 2. To increase the flow of certificate processing beyond the capacity of the default configuration, you can create additional registration paths by adding registration applications and configuring the Master RAs, validator vaults, and CA Agents needed to do the job.

The ability to add Master RAs, validator vaults and applications already exists using the Vault Registry Configuration applet. A manual procedure to provide multiple CA Agents to a specified Organization CA has been developed now, as well. This procedure allows multiple applications to be configured to share the same Organization CA through different CA Agents. This capability increases the capacity of the Organization CA to process certificates by overcoming the bottleneck created by the single-threaded nature of the CA Agent process.

Expanded Configuration

The number of CA Agents (and associated Master RAs, validator vaults and applications) you add depends on the platform you are using and the number of certificates your organization expects the CA to process. Figure 1 on page 2 illustrates an expanded configuration with a ratio of four CA Agents to one Organization CA. On an IBM RISC System/6000 Model 7025-F50 system with four processors, this configuration generates a throughput of 14 certificates per minute.

© Copyright IBM Corp. 1999

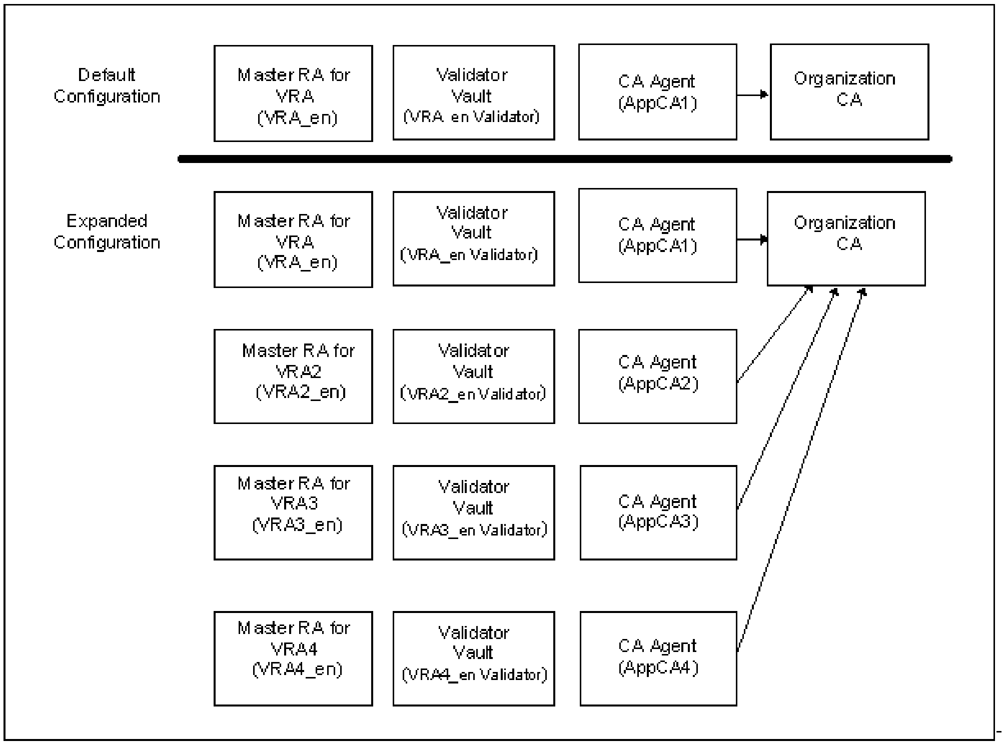

Default Configuration
Master RA for VRA (VRA_en)
Validator Vault (VRA en Validator)
CA Agent (AppCA1)
Organization CA
Expanded Configuration
Master RA for VRA (VRA_en)
Validator Vault (VRA_en Validator)
CA Agent (AppCA1)
Organization CA
Master RA for VRA2 (VRA2_en)
Validator Vault (VRA2_en Validator)
CA Agent (AppCA2)
Master RA for VRA3 (VRA3_en)
Validator Vault (VRA3_en Validator)
CA Agent (AppCA3)
Master RA for VRA4 (VRA4_en)
Validator Vault (VRA4_en Validator)
CA Agent (AppCA4)

Figure 1. Default and Expanded Vault Registration Application Configurations

Roadmap to Procedures

To create additional registration paths by adding CA Agents and associated Master RAs, validator vaults, and applications, follow these steps:

1. Before you begin, make sure you have the latest version of this document and that you have reviewed the latest version of the Vault Registry Readme file. These documents are located at:

   `http://www.software.ibm.com/security/registry/library/`

2. Start the Vault Registry Configuration applet. See the *Installation and Configuration Guide* for instructions.
3. Add a Master RA using the procedures documented in “Master RAs” on page 5.
4. Add a validator vault using the procedures documented in “Validator Vaults” on page 8.
5. Add a registration application using the procedures documented in “Applications” on page 11. Note that you must open each option page when configuring the application, even if you intend to accept the default configuration values. Follow the instructions in the *Installation and Configuration Guide* if you need help with this.
6. Repeat steps 3 through 5 to configure all the Master RAs, validator vaults, and applications you want to use for a given Organization CA.
7. Commit the settings to the system as described in the *Installation and Configuration Guide.*
8. Add the number of CA Agents you want to use by following the procedures documented in “Adding CA Agents” on page 15.

9. Validate your results by following the procedures documented in “Testing Your Results” on page 18.

Chapter 2. Adding an Application

This chapter steps you through a skeletal IBM Vault Registry configuration procedure for adding an application (Master RA, a validator vault, and an application). These instructions are intended specifically for the purpose of increasing the rate of certificate application processing. To perform these tasks, you must use the Vault Registry Configuration applet. Refer to the *Installation and Configuration Guide* for detailed instructions on starting the Configuration applet as well as configuring and reconfiguring Vault Registry.

Master RAs

The Master RA is a collection of background daemons that process registration requests in accordance with the rules and policies established for a given application. The Configuration applet includes building blocks for one Master RA, `Master RA for VRA`, which is typically used with the predefined Vault Registration Application domains.

Adding a Master RA

To configure another Master RA, use the following procedure to add an entry for it to the applet's menu so that you can configure it.

Note: You can remove a Master RA after saving your settings if it is the last entry in the list of those available for configuration and if it is not referenced by another part of the system. However, once you have committed the configuration to the system (see the chapter on committing configuration settings in the *Installation and Configuration Guide*), you cannot remove a configured component.

1. After starting the Configuration applet, select the `Master RA` component.

© Copyright IBM Corp. 1999

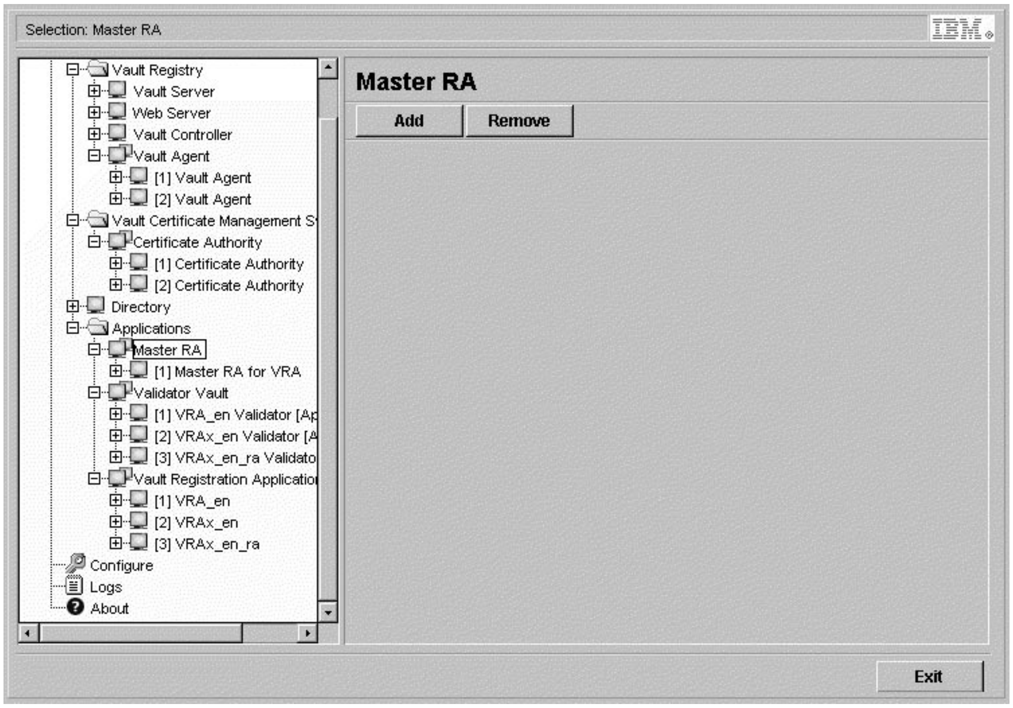
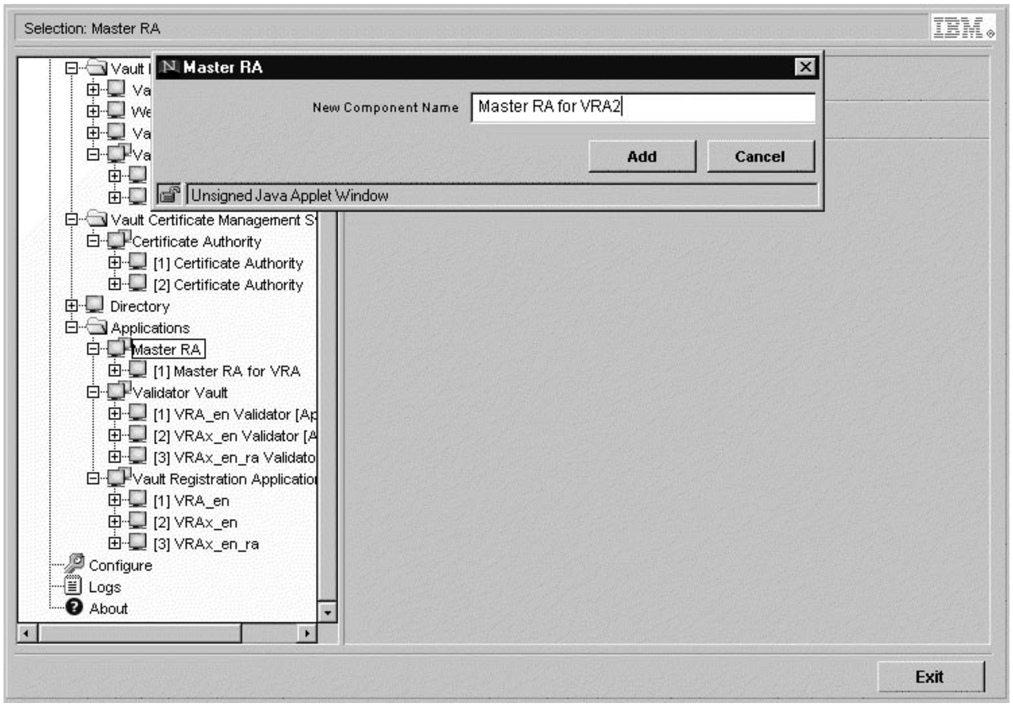


Figure 2. Configuration Applet — Master RA

2. To add a Master RA:
   a. Click on Add.

      The system prompts you for the unique name you want to use to distinguish this Master RA from other Master RAs in your system.
   b. Type the new name for the Master RA and click on Add. Figure 3 on page 7 shows an example of adding a Master RA named Master RA for VRA2.

      The system adds your new Master RA to the list available for configuration and assigns a numerical identifier to it ([1], [2], and so on).
   c. Follow the procedure on “Master RA Identification” on page 7 to specify configuration values for the new Master RA.



New Component Name: Master RA for VRA2

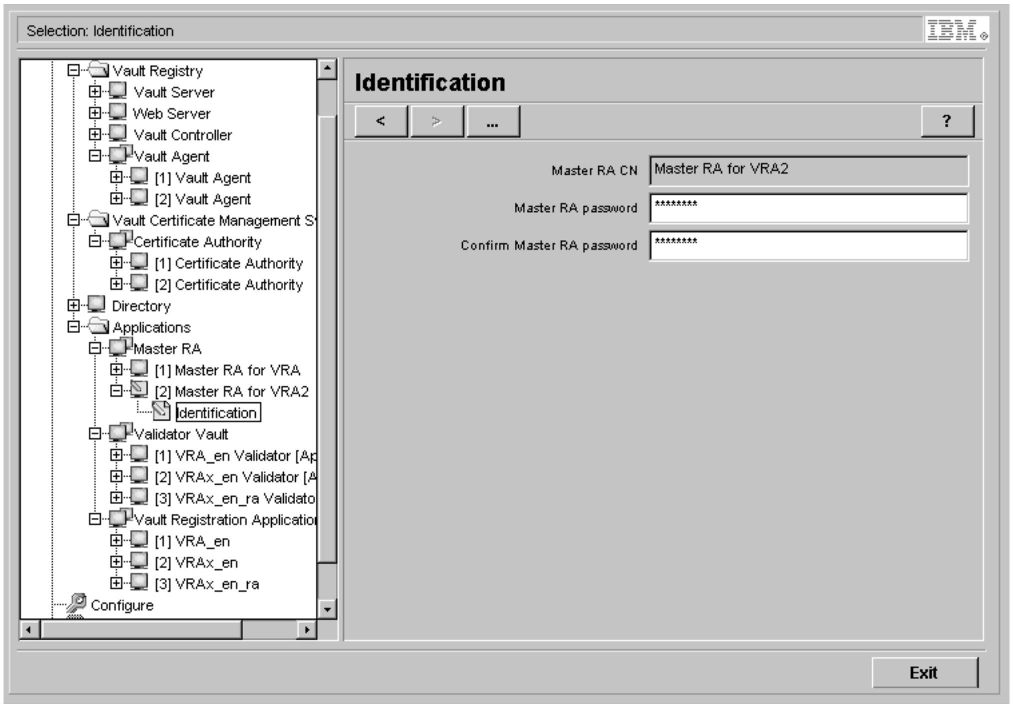
Figure 3. Configuration Applet — Add a Master RA

Master RA Identification

1. With the Configuration applet up and running, select the Master RA you want to configure ([1], [2], and so on), and select `Identification`.
2. `Master RA CN` displays the common name you specified when adding this Master RA to the list of configurable components (see “Adding a Master RA” on page 5).

   You cannot change this entry.
3. In `Master RA password`, type a password for this Master RA.

   The default value is `Secure98`. The password you specify should be at least six characters long, contain a mix of uppercase and lowercase characters, and include at least one number.
4. In `Confirm Master RA password`, retype the Master RA password.



Master RA CN: Master RA for VRA2

Master RA password: ********

Confirm Master RA password: ********

Figure 4. Configuration Applet — Identification

Validator Vaults

Validator vaults process requests from users who do not have certificates, such as requests from new users and users who need to renew certificates.

Adding a Validator Vault

To configure another validator vault, use the following procedure to add an entry for it to the applet’s menu so that you can configure it.

Note: You can remove a validator vault after saving your settings if it is the last entry in the list of those available for configuration and if it is not referenced by another part of the system. However, once you have committed the configuration to the system (see the chapter on committing configuration settings in the *Installation and Configuration Guide*), you cannot remove a configured component.

1. With the Configuration applet up and running, select the `Validator Vault` component.

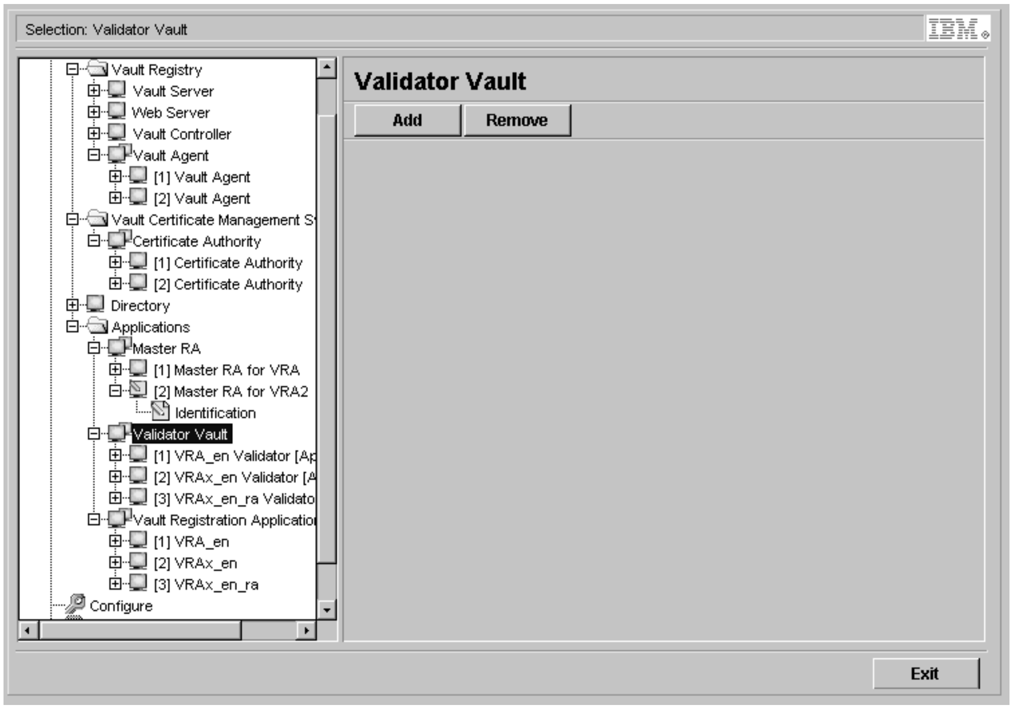


Figure 5. Configuration Applet — Validator Vault

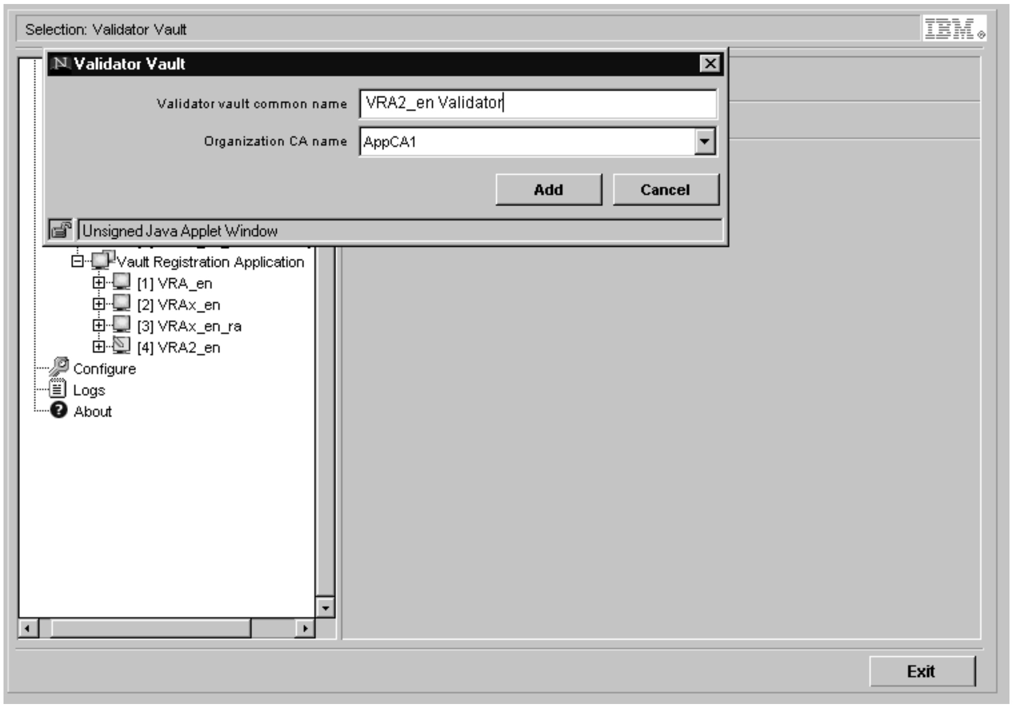
2. To add a vault:
   a. Click on Add.

      The system prompts you for information about the new vault.
   b. In Validator vault common name, type the unique name you want to use to distinguish this validator vault from others in your system. Figure 6 on page 10 shows an example of adding a vault named VA2_en Validator.
   c. In Organization CA name, select the CA that should be used to create this vault. The validator vault works with the Organization CA to process vault access requests.

      For the predefined application domains, this value is AppCA1. The name you select should correspond to the Organization CA you intend to use with the application that will use this validator vault.
   d. Click on Add.

      The system adds your new validator vault to the list available for configuration and assigns a numerical identifier to it ([1], [2], and so on).

      Note: When creating the validator vault, the system uses the name you specify as the vault's common name. After adding it, you cannot change it. If you decide you prefer a different name, and if you have not yet associated the vault with an application or defined additional validator vaults, remove this entry and create a new one with the name you prefer.

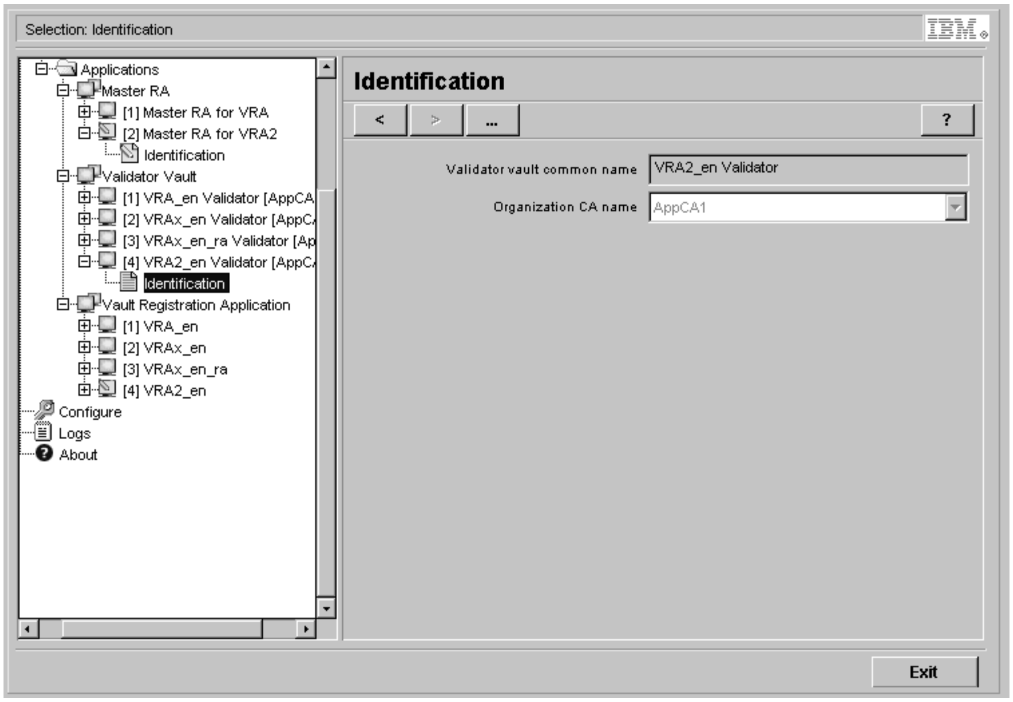


Validator vault common name: VRA2_en Validator

Organization CA name: AppCA1

Figure 6. Configuration Applet – Add a Validator Vault

Validator Vault Identification



Validator vault common name: VRA2_en Validator

Organization CA name: AppCA1

Figure 7. Configuration Applet — Validator Vault Identification

1. With the Configuration applet up and running, select the validator vault you want to configure (`[1]`, `[2]`, and so on), and select `Identification`.

2. Validator vault common name displays the common name you specified when adding this validator vault to the list of configurable components.

   You cannot change this entry.

3. Organization CA name displays the CA you selected when adding this validator vault to the list of configurable components.

   You cannot change this entry.

Applications

You can configure one or more implementations of the Vault Registration Application. For each application that you customize and deploy, you must specify:

- General information about the application, such as its location on your system and the names of the Master RA and Organization CA it uses to administer certificates
- Which policy exits should be invoked when a request is processed
- The names of the notification letters that should be sent to let applicants know whether a request has been approved or rejected
- The functions that should be available to applicants or certificate holders, such as whether a user can check the status of a pending request or renew a certificate
- Database setup, administration, and connection options, such as whether data stored in the database should be encrypted

Notes:

- You must open each option page when configuring the application, even if you intend to accept the default configuration values.
- Do not click on the Save Settings button until you are satisfied with all the configuration options specified for the new application, including the values you specify for the Organization CA associated with this application.

Adding an Application

The Configuration applet includes predefined building blocks for the following Vault Registration Application domains, where en indicates that the application is in English:

- VRA_en, which is designed for processing registration requests automatically
- VRAx_en, which is designed for use by an RA administrator who manually approves and rejects requests
- VRAx_en_ra, which is designed for use by administrative users (Master RA users, RA administrators, and operators)

To configure another application, use the following procedure to add an entry for it to the applet's menu so that you can configure it.

Note: You can remove an application after saving your settings if it is the last entry in the list of those available for configuration and if it is not referenced by another part of the system. However, once you have committed the configuration to the system (see the chapter on committing configuration settings in the *Installation and Configuration Guide*), you cannot remove a configured component.

1. If the new application is not using an existing database, make sure that the file system required for the new database has been created and mounted. The section on setting up AIX disk partitions in the *Installation and Configuration Guide* provides sizing guidelines.
2. After starting the Configuration applet, select the `Vault Registration Application` component.

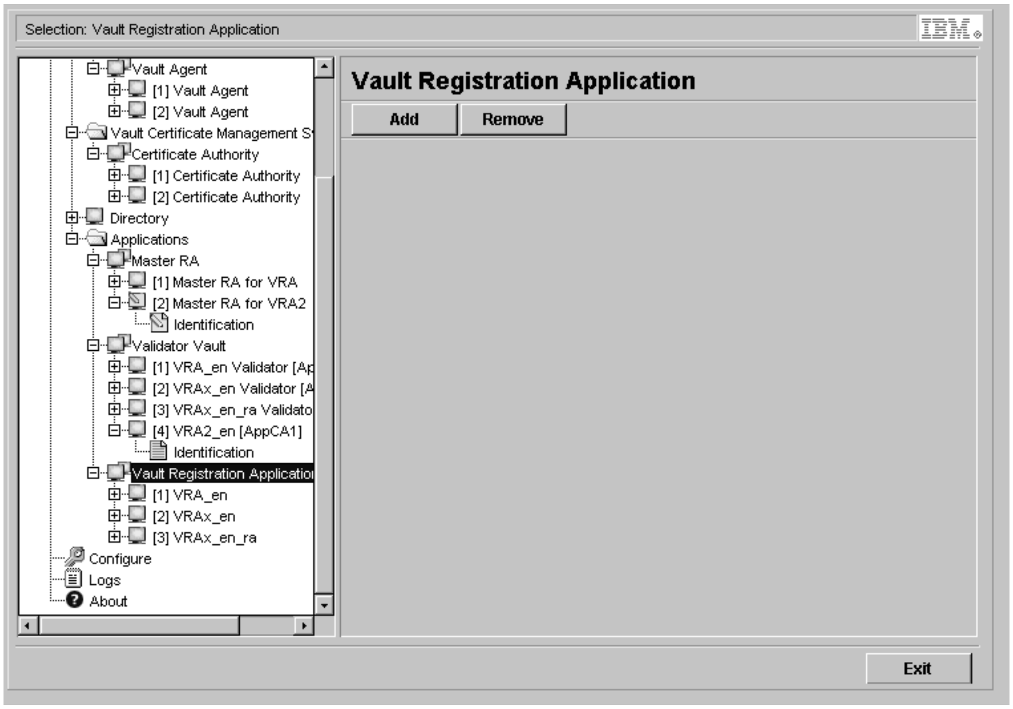


Figure 8. Configuration Applet — Vault Registration Application

3. To add an application:
   a. Click on `Add`.

      The system prompts you for the unique name you want to use to distinguish this application from other customized implementations in your system.

      To follow the naming convention used for the predefined domains, identify the application language and increment its name numerically. For example, use `VRA_`*en*, `VRA2_`*en*, and so on.

   b. Type the name of the new application and click on `Add`. Figure 9 on page 13 shows an example of adding an application named `VRA2_en`.

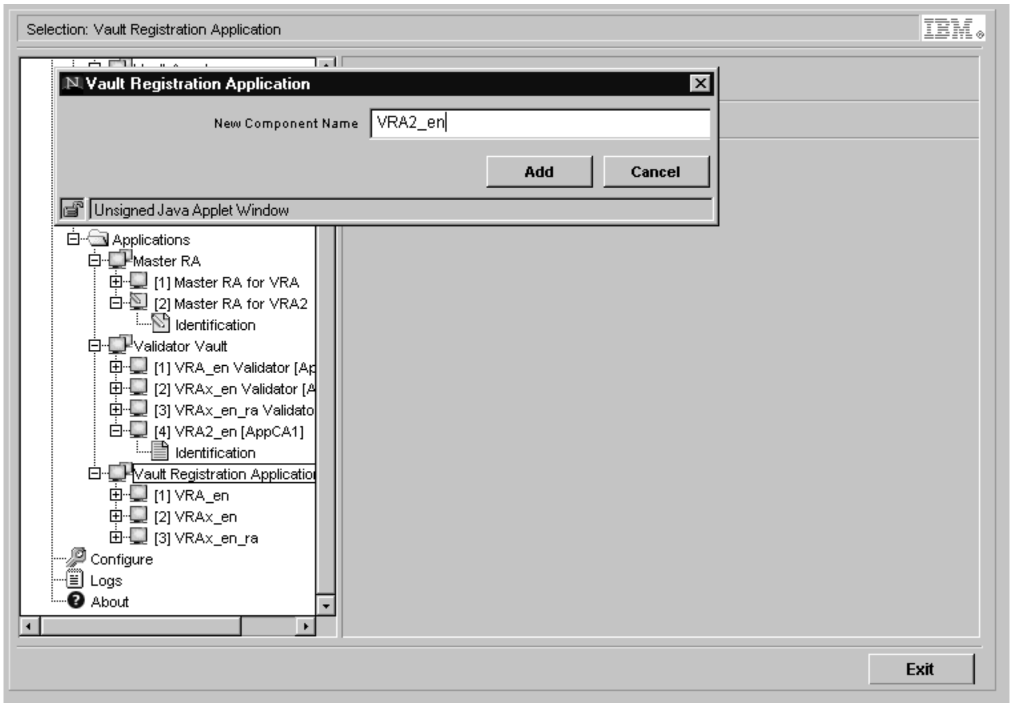
      The system adds your application to the list of domains available for configuration and assigns a numerical identifier to it (`[1]`, `[2]`, and so on).

      Note: The name you specify is used as the application name. After adding it, you cannot change it. If you decide you prefer a different name, and if you have not yet saved the settings for this application or added other applications, remove this entry and add a new one with the name you prefer.

   c. Follow the procedures in the *Installation and Configuration Guide* to specify configuration values for the new application.

Notes:

- You must open each option page when configuring the application, even if you intend to accept the default configuration values.
- Do not click on the `Save Settings` button until you are satisfied with all the configuration options specified for the new application, including the values you specify for the Organization CA associated with this application.
- Be sure to follow the procedure on completing the configuration of new application domains in the *Installation and Configuration Guide* to finalize the configuration of each new domain. You must perform this step after committing configuration values to the system.



Selection: Vault Registration Application

Vault Registration Application

New Component Name: VRA2_en

Figure 9. Configuration Applet — Add an Application

Chapter 3. Adding CA Agents and Testing Results

This chapter provides the manual procedures for adding CA Agents and testing your results.

Adding CA Agents

After you have finished adding Master RAs, validator vaults, and applications using the Vault Registry Configuration applet, use the following procedure to create additional CA Agents:

1. If you have not already done so, follow these steps to locate and download the `VR_MulCA.tar` tar file containing Vault Registry C shell scripts for adding CA Agents:
   a. Follow the *Download* link from the *Vault Registry* Web site (`http://www.software.ibm.com/security/registry/`).
   b. From *Enhancements and add-ons*, select **Vault Registry for AIX**.
   c. Click on **Configuring Multiple CA Agents** and follow the online procedures to download the tar file to a temporary directory on your workstation, such as `C:\tmp`.
2. Log in to the AIX Vault Registry server as `root`.
3. Change directories to `/usr/lpp/irg/admin`.
4. Using FTP, transfer the tar file from your workstation to the current directory.
5. Untar the tar file:

   ```
   tar xvf VR_MulCA.tar
   ```
6. Give execute permission to the Vault Registry C shell scripts you just extracted from the tar file:

   ```
   chmod +x createCaAgentVault.sh
   chmod +x createCaAgentValidator.sh
   chmod +x applyDNAttr.sh
   chmod +x autoStart.sh
   chmod +x addAcl.sh
   ```
7. Create a user account for the CA Agent you want to add. Using the example in Figure 1 on page 2, you would create an account for a CA Agent named `AppCA2`. For example:

   ```
   /usr/bin/mkuser pgrp='irg' home='/home/AppCA2' AppCA2
   ```
8. Create a vault for the new CA Agent by executing this command:

   ```
   ./createCaAgentVault.sh
   ```

   Following are the prompts returned by the system and examples of the responses that you might make. Possible responses are shown in bold except for passwords which remain blank.

   ```
   Enter Directory Search base (for VaultCA e.g. o=IBM, c=US)-->
   o=IBM, c=US
   Enter Directory Administrator DN (for VaultCA e.g. cn=DirAdmin, o=IBM, c=US)-->
   cn=DirAdmin, o=IBM, c=US
   Enter Directory Administrator password (for VaultCA)-->
   Enter Administrator user name (for VaultCA e.g. ca0off1)-->
   ca0off1
   Enter Administrator password (for VaultCA)-->
   Enter the user's account create from previous step (e.g. AppCA2)-->
   AppCA2
   ```

© Copyright IBM Corp. 1999

```
Enter CA password -->
Enter the CA Agent name (e.g. AppCA2)-->
AppCA2
The system is about ready to create AppCA2 CA Agent, Enter yes to continue
   or no to quit-->
yes
```

The system responds with informational messages. Look for lines similar to the following toward the end of the display:

```
...
...
[DEBUG]:Vault created successfully!
cn=AppCA2 + serialNumber = 2526807609,  o=IBM, c=US
cn=User aaA24
aaA24
...
...
```

9. Record the newly created vault ID (for example, aaA24) and DN (for example, `cn=AppCA2 + serialNumber = 2526807609, o=IBM, c=US`) displayed in this message for use later.
10. Create a validator vault for the new CA Agent by executing this command:

    ```
    ./createCaAgentValidator.sh
    ```

    Following are the prompts returned by the system and examples of the responses that you might make. Possible responses are shown in bold except for passwords which remain blank.

    ```
    Enter the user's account create from previous step (e.g. AppCA2)-->
    AppCA2
    Enter CA password (for VaultCA)-->
    Enter the new CA Agent Validator name (e.g. AppCA2 Validator)-->
    AppCA2 Validator
    Enter this new CA Agent password -->
    Repeat the password to confirm -->
    Enter Directory Administrator password (for VaultCA)-->
    Enter Administrator password (for VaultCA)-->
    Enter CA Agent Vault created from previous step (e.g. aaAxx)-->
    aaA24
    Enter Administrator user name (for AppCA1 e.g. ca1off1)-->
    ca1off1
    Enter Directory Search base (for AppCA1 e.g. o=IBM1, c=US)-->
    o=IBM, c=US
    Enter Directory Administrator DN (for AppCA1 e.g. cn=DirAdmin, o=IBM1,
       c=US)-->
    cn=DirAdmin, o=IBM, c=US
    The system is about ready to create validator for this CA Agent, Enter yes to
       continue or no to quit-->
    yes
    ```

    The system responds with informational messages. Look for lines similar to the following toward the end of the display:

    ```
    ...
    ...
    [DEBUG]:Created Validator Vault successfully for AppCA2 Validator
    [DEBUG]:The ID of the created vault:aaA25
    ```
11. Use the vault ID for the CA Agent (for example, aaA24) and the serial number (for example, 2526807609) created in step 8 on page 15 and apply the DN attributes to the CA Agent by executing this command:

    ```
    ./applyDNAttr.sh
    ```

Following are the prompts returned by the system and examples of the responses that you might make. Possible responses are shown in bold except for passwords which remain blank.

```
Enter CA password -->
Enter the new CA Agent DN created from previous step (e.g. cn=AppCA2 +
   serialNumber=nnnnnnnn, o=IBM, c=US)-->
cn=AppCA2 + serialNumber=2526807609, o=IBM, c=US
Enter the new CA Agent Vault DN created from previous step (e.g. cn=User aaAxx,
   o=IBM, c=US)-->
cn=User aaA24, o=IBM, c=US
The system is about ready to apply DN attributescreate for the new CA Agent,
   Enter yes to continue or no to quit-->
yes
```

12. Add the CA Agent to the AutoStart and Monitor systems by executing this command:

    ./autoStart.sh

    Following are the prompts returned by the system and examples of the responses that you might make. Possible responses are shown in bold except for passwords which remain blank.

```
Enter the new CA Agent password -->
Enter the new CA Agent Vault ID created from the previous step (e.g. aaAxx)-->
aaA24
Enter the user's account create from previous step (e.g. AppCA2)-->
AppCA2
The system is about ready to add the CA Agent to autoStart and monitor system,
   Enter yes to continue or no to quit-->
yes
```

    The system responds with the following informational message:

```
IRGY0221I System monitor (with auto-restart capability) is running.
```

13. Add the Master RA for the application domain that will use this CA Agent to the ACL of the new CA Agent by executing this command:

    ./addAcl.sh

    Following are the prompts returned by the system and examples of the responses that you might make. Possible responses are shown in bold except for passwords which remain blank.

```
Enter the new CA agent password -->
Enter the new CA Agent vault ID created from previous step (e.g. aaAxx)-->
aaA24
Enter the application domain you want to add to the new CA Agent ACL
   (e.g. cn=Master RA for VRA2 + serialNumber=xxxxxxxx, o=IBM, c=US)-->
cn=Master RA for VRA2 + serialNumber=4256279481, o=IBM, c=US
The system is about ready to add application domain to the new CA Agent ACL,
   Enter yes to continue or no to quit-->
yes
```

    Note: To find the serial number for the Master RA, you can either search for it using the AIX command `ldapsearch` (for example, ″`cn=Master RA for VRA2`″), or you can go to the `/usr/lpp/irg/admin` directory and search the `instCfg.log` file.

14. Edit the file `/usr/lpp/irg/pkrf/etc/raconfig.cfg` under the corresponding application domain, and replace the value of the `appCertCA` parameter with the name of the new CA Agent. For example, **appCertCA=AppCA2**.

15. Edit the file /usr/lpp/irg/pkrf/VRA2_en/ra_var_app_defs.ds under the corresponding application domain, and replace the value of the var autoAppDomain parameter with the name of the new Master RA. For example, **var autoAppDomain="VRA2_en"**.
16. Repeat steps 7 through 15 to create additional CA Agents, as needed.
17. Using the runm command to recycle Vault Registry, enter the following:

```
su - irguser
cd /usr/lpp/irg/bin
./runm -d -a        # to shutdown the system
./runm -u -a        # to bring up the system
```

Testing Your Results

For each CA Agent that you add, you should verify that it has been created successfully. You can test the procedure by obtaining a new certificate. Because on a running production system it is important to account for every certificate, you should label the certificate something like dummy test certificate and be sure to revoke the certificate immediately after the test has completed.

To verify that the CA Agent has been successfully created, follow these steps:

1. Using your browser, access your registration application's home page, for example:

   http://*VRAserver*/VRA2_en/index.html
2. On the Basic Enrollment and Vault Entrance form, go to the Service field and select Enroll Directly for Organization Certificate from the pulldown menu.
3. Select the application you want to test, and click **Go**.
4. Complete the Direct User Enrollment form and click **Submit Request**.
5. When you have completed the certificate request, go to the directory /local/vaults/aaA*xx* and search the caAgentd.log to ensure that the certificate was created successfully.
6. If the test is successful, use the RA Desktop or your custom registration application to revoke the test certificate immediately.

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.