Lotus Notes ID Vault
OPEN MIC LOTUS TEAM

- Hemant Parulekhar – Lotus Technical Advisor
  - Presenter

- Shrikant Jamkhandi – Lotus Support Engineer
  - Presenter

- Hansraj Mali - Lotus Technical Advisor
  - Focussing on Notes/Domino, LotusLive

- Ranjit Rai - Lotus Technical Advisor
  - Focussing on entire Notes/Domino

- Soumitra Limaye – Lotus Support
  - Facilitator for Open Mics
Agenda

- Overview
- Advantages of using the ID vault
- Configuring ID Vault
- Managing the Notes ID vault
- Password Reset Authority Administration
- Understanding the Notes ID vault
- Troubleshooting
- ID vault notes.ini settings
- References
- Q & A
What is Notes ID vault?

ID Vault

- The ID vault is an server-based database that holds protected copies of IBM® Lotus® Notes® user IDs.
- ID vault allows administrators and users to easily manage Notes user IDs.
- Users are assigned to a vault through policy configuration, and copies of user IDs are uploaded to a vault automatically once the policy has taken effect.
- Secure, centralized, server-based repository for Notes ID files, Replaces expensive to manage ID file and password recovery systems and significantly reduces costly user downtime and help desk costs.
- Simplifies provisioning of Lotus Notes IDs, Automatically uploads ID files to vault for existing Lotus Notes users.
- Streamlines process for resetting forgotten passwords.
- Help desk options Programmatic interfaces for self-service password applications Manages changes across multiple copies of Notes ID files.
- Provides “Auditor” function to extract ID files for legal discovery/access to encrypted data.
Advantages of ID Vault

- The ability for authorized personnel to change (reset) passwords on IDs stored in a vault when users forget them, without access to the ID files or the vault.
- Support for the use of a custom application to reset passwords
- Easy recovery of lost or damaged user IDs
- Automatic synchronization of multiple ID copies
- No user involvement during ID renames
- No user involvement during ID key rollover
- Use of the ID vault is strongly recommended. However, the ID recovery feature from earlier releases is still supported for customers who prefer it.
Advantages of ID Vault...

In short ID Vault removes the pain from

- Password Recovery
  - By allowing password resets without access to the id itself
- Lost ids
  - By re-distributing the vault copy.
- Users with multiple id copies (we know you’re out there)
  - By keeping multiple copies in sync
- User renames
- Re-issuing the keys
  - By doing both without needing any user involvement
Advantages of ID Vault...

So...

- IBM® Lotus Notes and Domino have been providing a secure Public Key Infrastructure (PKI) environment for years. There is a cost associated with managing ID files.
- Use of ID Vault significantly lower this cost without compromising security.
- It makes you happy because you can keep your environment secure and not wait on users to complete your work.
- It makes users happy because they have one sync’d id and can easily get a password reset.
- It makes audit happy because you no longer have that backup directory of id files.
Prerequisites for Enabling ID vault

In order to enable ID vault for a given Domino 8.5 server or later.

**Server Side:**
- At least one Domino server running version 8.5 or later.
- A Notes client running 8.5 or later with the Administrator client.
- An ID that has at least Editor access to the Domino Directory (no specific roles are necessary)
- An ID with the ability to create templates/databases on the server where the vault will be located.
- Access to any certifiers whose IDs will be added.

**Client side:**
- A Notes client running 8.5 or later.
- Local address book should be of version 8.5 or later.
Configuring ID Vault
Configuring ID Vault continued..

The name you specify is used to form the hierarchical name, the database file name and the ID file name for the Notes ID vault. The name cannot be the same as any organization or organizational unit. Example: "ACMEVault" results in the hierarchical vault name "ACMEVault", the vault database file name "acmevault.nsf" and the vault ID file "acmevault.id". Once the Notes ID vault is created in the last step of this tool, you cannot change its name.

Specify a password and file location for the vault ID file.

Password: XXXXXXXXXXXXXXX
Verify: XXXXXXXXXXXXXXX

This step obtains the information to create the vault ID file. Specify a password that is at least eight characters long and that conforms to secure password rules. Vault administrators are prompted for the vault ID file and password when they add or remove replicas of the ID vault. Making a backup copy of the ID file is recommended.
Configuring ID Vault continued..

**Create and Configure Notes ID Vault**

Select the Notes ID vault replace server.

- **Vault server**:
  - INMAIL01/Node

Specify the server on which to create the ID vault. To replicate the vault to additional servers, use the ID Vaults - Manage tool later.

**Create and Configure Notes ID Vault**

Select the Notes ID vault administrators.

- **The following administrators can manage the Notes ID vault**:
  - Admin Notes/Node

You must select at least one Notes ID vault administrator. You can select user names only, not group names. Only vault administrators can add and remove vault servers, delete ID files from a vault, and add and remove other vault administrators. The vault administrator names are added to the ACL of the vault database and to the vault document in the Domino Directory.
Configuring ID vault continued..
Configuring ID Vault continued...

Application for auto processing password resets you will need a server authorized as 'Self Service Password Reset Authority' and also an agent signer

Password Reset

You have authorized a self-service password reset application for organization /Acme for a server name. If the application is an agent, you have selected a server on which to deploy the agent, you must also give 'Self-service password reset authority' to the user that signs the agent. Click Yes to continue or click No to return to the previous window and make changes.

Yes  No
Configuring ID Vault continued..

**Create and Configure Notes ID Vault**

- **How is this policy assigned?**
  - Create a new policy applicable to an organization
  - Create a new policy assigned to specific people or groups
  - Create a new policy assigned to a home server
  - Edit an existing policy
  - I will specify an Notes ID vault policy at another time

This step assigns a vault to users by creating or editing a Security Settings document and assigning it to a policy applied to users. It also enables you to specify help text that users see when they click the Forgotten Password button. User IDs are only stored in a vault if they are descendent from an organization or organizational unit that has a Vault Trust Certificate in the Domino Directory. To skip this step, select I will specify an Notes ID vault policy at another time and click "Next.

**Create and Configure Notes ID Vault**

- **Select organizations to which this policy will be assigned.**

Select the users, organizations, or organizational units that will use the ID vault. If an organizational policy does not exist for a selected organization, one is created and a Security Settings document that includes the ID vault settings is added. If a selected organization already has an organizational policy, a Security Settings document is added or updated to include the ID vault settings.

**Forgotten Password Help Text**

Please enter the help text that will be displayed to the user as part of the password prompt when they have forgotten their password.

Call the help desk @ 1800 999 where you will be asked to confirm your identity, OR click below link for "Reset Notes Password Now".

HREF="http://INMAIL01.in.ibm.com/pwdresetexample.nsf"">Reset Notes Password Now</A>
Configuring ID Vault continued..
Configuring ID Vault continued..

You have successfully created the Notes ID vault ‘IBM Demo Vault’.

In the process of creating the vault the following tasks have been run.
- Created Notes ID vault Document
- Created Notes ID vault Trust Certificates
- Created Notes ID vault Password Reset Authorities
- Created Notes ID vault ID file (C:\Program Files\IBM\Lotus\Notes\Data\ds\vault\ibm demo vault.id)
- Created Notes ID Vault /IBM Demo Vault

Vault database path: \IBM_ID_VAULT\IBM Demo Vault.nsf

Add vault trust certificates to the following organizations:
- /Acme was successfully added.
- /Marketing/Acme was successfully added.
- /Sales/Acme was successfully added.

Policy work done.
- Added Notes ID vault name to security document IBMDemoVaultVaultSetting
- Added Notes ID vault help text to security document IBMDemoVaultVaultSetting
- Applied users/groups to master policy /IBMDemoVault\VaultPolicy

[Copy to clipboard]
Configuring ID Vault continued..

Resulting documents

Multi-purpose group: IBM Demo Vault Vault HSGroup

<table>
<thead>
<tr>
<th>Basics</th>
<th>Comments</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name: IBM Demo Vault Vault HSGroup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group type: Multi-purpose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description: Vault homeserver group for IBM Demo Vault</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail Domain:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Address:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Populate Method:</td>
<td>Home Server</td>
<td></td>
</tr>
<tr>
<td>Home Server(s):</td>
<td>CN=INMAIL01/0-Acme</td>
<td></td>
</tr>
<tr>
<td>Additional Members:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Excluded Members:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Members: Admin Notes/Acme
John Doe/Acme
Rhino Moor/Acme
Smith Jones/Acme | | |

Policy: /IBM Demo Vault Vault Policy

<table>
<thead>
<tr>
<th>Basics</th>
<th>Policy Assignment</th>
<th>Policy Precedence</th>
<th>Comments</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name: /IBM Demo Vault Vault Policy</td>
<td></td>
<td></td>
<td></td>
<td>Create</td>
</tr>
<tr>
<td>Policy type: Explicit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description: Vault policy for IBM Demo Vault</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setting Type</th>
<th>Setting Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration:</td>
<td></td>
</tr>
<tr>
<td>Setup:</td>
<td></td>
</tr>
<tr>
<td>Archiving:</td>
<td></td>
</tr>
<tr>
<td>Desktop:</td>
<td></td>
</tr>
<tr>
<td>Security: IBM Demo Vault Vault Setting</td>
<td></td>
</tr>
</tbody>
</table>
Configuring ID Vault continued..

Resulting documents

Security Settings : IBM Demo Vault Vault Setting

<table>
<thead>
<tr>
<th>Security Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basics</td>
<td>- Password Management</td>
</tr>
<tr>
<td></td>
<td>- Execution Control List</td>
</tr>
<tr>
<td></td>
<td>- Keys and Certificates</td>
</tr>
<tr>
<td></td>
<td>- Signed Plug-ins</td>
</tr>
<tr>
<td></td>
<td>- Portal Server</td>
</tr>
<tr>
<td></td>
<td>- ID Vault</td>
</tr>
</tbody>
</table>

**ID Vault Options:**

<table>
<thead>
<tr>
<th>ID Vault Options</th>
<th>How to apply this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned vault</td>
<td>IBM DemoVault</td>
</tr>
<tr>
<td>Forgotten password help text</td>
<td>Call the helpdesk @ 1800 999 where you will be asked to confirm your identity. OR click below Link for &quot;Reset Notes Password Now&quot;&lt;A HREF=&quot;http://INMAIL01.in.ibm.com/pw/dreetsample.nsf&quot;&gt;Reset Notes Password Now&lt;/A&gt;</td>
</tr>
</tbody>
</table>

- Enforce password change after password has been reset: Yes
- Allow Notes-based programs to use the Notes ID Vault: No

**Automatic ID Downloads:**

<table>
<thead>
<tr>
<th>Automatic ID Downloads</th>
<th>How to apply this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow automatic ID downloads:</td>
<td>No</td>
</tr>
<tr>
<td>Allow ID downloads for:</td>
<td>7 days</td>
</tr>
<tr>
<td>ID download authorization failure message:</td>
<td>Your Notes account has been expired. Please call the helpdesk @ 1800 999. Help Now to re-activate your Notes account</td>
</tr>
</tbody>
</table>

**Automatic ID Downloads**

- Enabling ‘Yes’ for automatic ID downloads means an id is downloaded to whatever clients need it with no limit on the number of times they can be downloaded.

- If you know that a user has only 1 pc to work on then you can limit this by choosing ‘no’ and setting a number of downloads per user.

You can also control how long after an id change can that id still be downloaded. If you restrict it to 1 day then after than one day the id will no longer automatically download.

- You can present a customized message to the user explaining that their updated id tried and failed to download and why.
Configuring ID Vault continued..

Resulting documents

ID Vault: /IBM DemoVault

**Basics**
- **Vault name:** /IBM DemoVault
- **Description:** The Primary Vault for Demo
- **Vault Administrators:** Admin Notes/Acme
- **Vault servers:** INMAIL01/Acme
- **Path to Vault:** IBM_ID_VAULT/IBM DemoVault.nsf

**Lotus Notes**
- **User name:** John Doe/Acme
- **Password:**
- **At location:** Online

**Forgot your password?**
Call the helpdesk at 1800 999 where you will be asked to confirm your identity. OR click below Link for "Reset Notes Password Now"
Managing ID vault

- Edit vault description
- Edit vault ID password
- Manage vault replica servers
- Add or remove vault administrators
- Add or remove organization that trust the vault
- Add or remove password reset authorities
- Create or edit vault policy settings
Password Reset Authority Administration

Reset Password

Set ID Download Count
Password Reset Authority Administration cont..

Extract ID from Vault

Extract ID File From Notes ID Vault

- User whose ID file should be extracted from the vault: John Doe/Amel

- Name of the Notes ID vault from which to extract the ID: /IBM DemoVault

Save ID File As

- Save in: My Documents

New Password for Extracted ID File

- Please enter a new password for the extracted ID file.
  - New password: XXXXXXXXXXXX
  - Confirm new password: XXXXXXXXXXXX
Password Reset Authority Administration cont..

**Password Reset Authority**

- **Directory:** Acme’s Directory
- **Available users, groups and servers:**
  - Administration Requests
  - Doe, John
  - IBM Demo Vault Vault HSGroup
  - INMAIL01/Acme
  - Jones, Smith
  - Local Domain Admins
- **Available organizational units:**
  - /Marketing/Acme
  - /Sales/Acme

**Password reset authority by organization:**
- /Acme
  - Admin Notes/Acme
- INMAIL01/Acme
  - /Marketing/Acme
  - /Sales/Acme
Understanding how ID vault works

How IDs are uploaded to a vault initially

- Parent certifier of the user ID has issued a Vault Trust Certificate
- Effective policy has a Security Settings document that specifies the vault name
- If these conditions are met for a new user being registered, the process of user registration uploads the ID to the vault.
- It also does for non-vaulted users, that is the first time the user authenticates with the home server.
- If the above conditions are met for an existing user, a copy of the user's ID is uploaded from the Notes client to the vault automatically

How copies of IDs on Notes clients are kept synchronized with the vault copies

- To synchronize a local copy of an ID with the vault copy, a client asks its home server for a list of servers that have a replica of the vault.
- If the home server is unavailable or does not run release 8.5 or higher, the client searches for a server in the home server cluster to provide the list
Understanding how ID vault works

How copies of IDs on Notes clients are kept synchronized with the vault copies

• The client tries each vault server in the list until it returned one satisfy its request.

• For better performance the client caches the location of the first vault server that responds.

• This cache is cleared periodically to ensure that load balancing is maintained.

• When a user changes ID file on a client, switches IDs, or provides a new password after a password reset, the client attempts synchronization immediately.

• Otherwise it will check periodically every 8 hours.

• If sync fails, three retry attempts are made at five-minute intervals. If still not successful, checking resumes at the next eight-hour checking interval.

• If a client has been started and stopped three times and it has been more than 24 hours since it has checked for the need to synchronize, it checks about five minutes after startup.
Understanding how ID vault works

How new passwords are synchronized across multiple ID copies

- When the password on a ID is changed anywhere (in the vault or on a client), the user can provide the new password from any client as long as the client can connect to the network to synchronize with the vault.
- Other clients will periodically check to see if the ID in the vault is different from their ID and they need to resync with the vault.
- If a client doesn’t have network connectivity, a user can continue to use the old password until a connection becomes available.
Understanding how ID vault works

How ID recovery works for an ID in a vault

• If the ID file on a user's computer is deleted, a copy of the ID is downloaded to the Notes client from the vault.
• This recovery occurs the next time the user attempts to access the ID file through Notes when the client is connected to the network.

How ID renaming and key rollover work with a vault

• A user who requests a name change through the User Security window is not given the option to approve the change. The option to "Ask your approval before accepting name changes" is unavailable.
• Change is always made on the client ID copy automatically during client-vault synchronization when the name change is detected on the server.
• A user with a vaulted ID cannot request a key rollover through the User Security window, only an administrator can initiate key rollover through policy configuration.

How shared-login-enabled IDs work with a vault

• Shared-login-enabled user IDs can be stored in a vault. In this case, the steps to recover the ID or to respond to a stolen ID are different than for non-shared-login-enabled IDs.
• Notes password must be reset on the copy of the ID in the vault. After the reset, the following actions occur: (a) User prompted for the new password. (b) After new password is given a Id file downloaded from vault to client. C) Local ID is re-enabled for shared login and the user is no longer prompted for the password.
Troubleshooting

Where and how to find logs for ID vault .

Security events in the local/server log.nsf

Security Events

Time: 05/10 11:14 PM - 05/10 11:16 PM
Elapsed Time: 1.7 minutes

Events:
05/10/2011 11:14:18 PM ID: O:\Program Files\IBM\Lotus\Notes\Database\people\doe.id' failed to synchronize with vault 'O=IBM DemoVault' on server 'CN=INMAIL010=Acme'. John Doe/Acme' made request. Error: Illegal null parameter passed to security function.
05/10/2011 11:14:25 PM ID: O:\Program Files\IBM\Lotus\Notes\Database\people\doe.id' failed to synchronize with vault 'O=IBM DemoVault' on server 'CN=INMAIL010=Acme'. John Doe/Acme' made request. Error: Illegal null parameter passed to security function.
05/10/2011 11:14:27 PM ID: O:\Program Files\IBM\Lotus\Notes\Database\people\doe.id' failed to synchronize with vault 'O=IBM DemoVault' on server 'CN=INMAIL010=Acme'. John Doe/Acme' made request. Error: Illegal null parameter passed to security function.

Security Events

Time: 05/01 04:04 PM - 05/01 09:04 PM
Elapsed Time: 300.5 minutes

Events:
05/01/2011 04:04:12 PM ID failed to authenticate in vault 'O=IBM DemoVault' for 'Admin Notes' (IP address 192.168.1.8.2244) made request. Error: Entry not found in index.
05/01/2011 06:26:34 PM ID Vault 'O=IBM DemoVault' on server 'CN=INMAIL010=Acme' successfully created by 'Admin Notes/Acme' (IP address 192.168.1.8.2289).
05/01/2011 07:16:47 PM Unable to find ID for 'John Doe/Acme' in vault 'O=IBM DemoVault'. Error: Entry not found in index.
05/01/2011 07:16:47 PM ID failed to authenticate in vault 'O=IBM DemoVault'. 'John Doe/Acme' (IP address 192.168.1.8.2324) made request. Error: Entry not found in index.
05/01/2011 07:16:49 PM ID successfully synchronized with vault 'O=IBM DemoVault' for 'John Doe/Acme' (IP Address 192.168.1.8.2326).
05/01/2011 07:17:24 PM Unable to find ID for 'Admin Notes/Acme' in vault 'O=IBM DemoVault'. Error: Entry not found in index.
05/01/2011 07:17:24 PM ID failed to authenticate in vault 'O=IBM DemoVault'. 'Admin Notes/Acme' (IP address 192.168.1.8.2334) made request. Error: Entry not found in index.
05/01/2011 07:17:25 PM ID successfully synchronized with vault 'O=IBM DemoVault' for 'Admin Notes/Acme' (IP Address 192.168.1.8.2336).
05/01/2011 07:17:30 PM Failed to reset password for 'John Doe/Acme' with 1 downloads on server 'CN=INMAIL010=Acme'. Error: Agent containing ResetUserPassword method must be signed by a designated Password Reseter.
05/01/2011 07:38:30 PM Password for 'John Doe/Acme' with 1 downloads was reset by 'INMAIL010=Acme' (IP Address 192.168.1.8.2366) from process server.
05/01/2011 07:38:30 PM Password for 'John Doe/Acme' with 1 downloads was reset on server 'CN=INMAIL010=Acme'.
05/01/2011 07:38:32 PM ID successfully synchronized with vault 'O=IBM DemoVault' for 'John Doe/Acme' (IP Address 192.168.1.8.2369).
05/01/2011 07:40:57 PM ID successfully synchronized with vault 'O=IBM DemoVault' for 'John Doe/Acme' (IP Address 192.168.1.8.2371).
Troubleshooting

Using the administrator client for analyzing the Vault issues.
# Troubleshooting

## Domain monitoring: DDM database

### DDM

<table>
<thead>
<tr>
<th>By Severity</th>
<th>By Date</th>
<th>By Type</th>
<th>By Database</th>
<th>By Server</th>
<th>By Assignment</th>
<th>Open Configuration</th>
</tr>
</thead>
</table>

### Open Events

<table>
<thead>
<tr>
<th>Open Events By Severity</th>
<th>Date</th>
<th>Server</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td></td>
<td>INMAIL01/Acme</td>
<td>ATTEMPT TO ACCESS DATABASE mail/notes.nsf by John Doe/Acme was denied</td>
</tr>
<tr>
<td>Warning (High)</td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to set download court for ‘Rhino Moore/Acme’ to 0; Entry not found in index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to set download court for ‘Rhino Moore/Acme’ to 0; Entry not found in index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to authenticate in vault ‘…’; Entry not found in index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>ATTEMPT TO ACCESS DATABASE events4.nsf by John Doe/Acme was denied</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>ATTEMPT TO ACCESS DATABASE dotedm.nsf by John Doe/Acme was denied</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to authenticate in vault ‘D=IBM DemoVault’; Entry not found in index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to authenticate in vault ‘D=IBM DemoVault’; Entry not found in index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INMAIL01/Acme</td>
<td>Failed to authenticate in vault ‘D=IBM DemoVault’; Entry not found in index</td>
</tr>
</tbody>
</table>

### Server

<table>
<thead>
<tr>
<th>Server: Monitoring</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mon 05/09 INMAIL01/Acme</td>
</tr>
<tr>
<td></td>
<td>Mon 05/09 INMAIL01/Acme</td>
</tr>
</tbody>
</table>
Troubleshooting

Error Messages

- Error when trying to extract ID file from ID vault: “Server Error: You are not authorized to perform that operation”

> This is due to administrator don’t have the “Auditor” role in the ID vault database.

> In other case even though administrator has the “Auditor” role however the server notes.ini SECURE_DISABLE_AUDITOR=1 can prevent ID file to be extracted.

- User registration fails to upload the new user's ID to the Lotus Domino ID Vault with the error, "Error: File does not exist"

> During the registration process, a copy of the Notes ID for the new user is written to a local temporary directory. Make sure administrator client has sufficient privileges to read and write to temporary directories and that no third-party applications, such as anti-virus solutions is blocking it.

- ID upload to an ID vault can fail during user registration. User registration process is completed with error: FAILED: ID upload to Notes ID Vault failed.

> In some cases problem was caused because of corruption in Domino Directory (names.nsf)
Troubleshooting

- ID upload to an ID vault can fail during user registration. User registration process is completed with error: FAILED: ID upload to Notes ID Vault failed.

- In some cases the issue will be resolved by copying the certificates from the server address books to the local address book.

- A user loses his ID or it becomes corrupt. You attempt to launch their Notes client and download a new ID for this user, but you receive the error message "File cannot be created".

- KeyFileName that specifies the location to store the ID has been incorrectly set. In one particular case the folder specified to store the downloaded ID was accidentally deleted. Client is unable to download the ID to a location that does not exist.

- Error is generated in the Domino logs repeatedly: "Failed to authenticate with server Abc/Test. This server does not have the vault. A referral was returned."

- This error message is merely informational. The server in question does not contain a replica of the ID Vault and as a result, a referral is returned to the requesting server with details about which server actually does contain a replica of the ID Vault. Can be prevented by having replica of the ID vault on the server in question.
Troubleshooting

> When administrator tries to reset the password for the user ID it gives the error message: “Server Error: Missing or invalid Password Reset Trust certificate, Check the log file for details.”

> This issue can be seen if the certified public Key in the certifier document of the certifier was not matching with the public Key which is stored in the cert.id file. Can be resolved by copying the public key from the certifier id to the certifier document.

> The other cases it can be caused if the one of the below field or all the fields on the certifier document appended with "/“.

FullName="/O=Acme“  IssuedBy="/O=Acme“  IssuedTo="/O=Acme“

Could be resolved by editing & resaving the certifier document or modifying the fields with an agent to have the value as O=Acme.

Which debugs used to collect the logs for the ID vault issues.

<table>
<thead>
<tr>
<th>Client Side</th>
<th>Server Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug_IDV_TrustCert=1</td>
<td>Debug_IDV_TrustCert=1</td>
</tr>
<tr>
<td>Debug_Namemlookup=1</td>
<td>Debug_Namemlookup=1</td>
</tr>
<tr>
<td>Console_log_enabled=1</td>
<td>Console_log_enabled=1</td>
</tr>
<tr>
<td>DEBUG_IDV_TRACE=1</td>
<td>Debug_threadid=1</td>
</tr>
</tbody>
</table>
ID vault NOTES.INI settings

- IDV_POLL_INTERVAL
- IDVault_Max_Auth_Failures
- IDVault_Max_Auth_Failure_Cache_Size
- IDVAULT_RESYNC_INTERVAL
- SECURE_DISABLE_AUDITOR
- IDVAULT_CTRCT
- IDVaultLastFlushTime
- IDVaultLastServer
- IDVAULT_STAMP1

Debug notes.ini for ID vault

- DEBUG_IDV_CONNECT
- DEBUG_IDV_TRACE
- DEBUG_IDV_TRUSTCERT
- DEBUG_IDV_UPDATE
- DEBUG_IDVAULT_SERVER_SELECTION
Resources

Lotus Domino Wiki Link for ID vault documents
Lotus Domino and Notes Information Center
ID vault logging for 8.5 FAQ
Open Mic "Lotus Domino ID Vault" call of October 22 2009
Open Mic Q&A: ID Vault & Notes Shared Login - 20 October 2010
Q&A