Taking Advantage of Windows with Zope

Mark Hammond
Enfold Systems

enfoldsystems

About this talk

- The Why and How of Zope on Windows
- No demos, no code
  - Every customer has different requirements
  - Trying to convey breadth of ideas, not depth of implementation
  - Examples at the end of the talk
- Assume knowledge of Zope and Plone

enfoldsystems

Why Windows?

- Plone making inroads to the Enterprise
- Enterprises use Windows for their server architecture
  - The focus of this talk is not the Windows desktop for users
  - Users and administrators expect integration
- How to take advantage of this infrastructure in Zope?

enfoldsystems

What infrastructure?

- ActiveDirectory
- Message Queueing
- IndexServer
- Security and encryption
- The rest (ADO, WMI, etc)

enfoldsystems

How to take advantage?

- Core Zope and Plone services grow to support certain features
  - Single sign-on
  - Users integrated with AD
- Your Zope and Plone applications can leverage other features
  - Queue custom message types or Index Server catalog
  - Query/Update corporate databases

enfoldsystems

Core Zope and Plone Support

- Complete, functioning pywin32 extensions
- More reliable services
- Safe shutdown
- Log rotation
  - Different than Linux, but at least allows rotation!
- Above are all in latest Zope 2.7 and 2.8 releases

enfoldsystems

Enfold EES Support

- Allow explicit user to run the service.
- Tight ActiveDirectory integration
- Publish Zope and Plone sites in ActiveDirectory
- Windows Scheduled Tasks
- NTLM authentication via PAS
  - Kerberos should be possible too
- Caching proxy server for IIS

enfoldsystems

Windows Security

- MS recommends against running services as LocalSystem
  - Unrestricted access to local machine.
- MS recommends running as a Domain User
  - Allows centralized administration of the accounts used to run the service
- Implications in a more restricted environment
  - Installation programs must do more work – service generally unable to write to registry.

enfoldsystems

Windows Authentication

- Single sign-on
  - User never has to provide their password to an application
- Impersonation
  - Let Windows determine the permissions of the user
  - Integration with Windows audit facilities
- Challenges when interacting with form/cookie based login.

Active Directory (core)

- Basic integration possible today with LDAPUserFolder
  - Requires Windows username/password entered in ZMI
  - Requires complex setup
- AD specific solution requires zero configuration
  - Credentials of running process automatically used, Global Catalog

enfoldsystems

Active Directory (apps)

- Easier than using LDAP for 'casual' use by your application code
- Query for “well known” services on the network
  - SQL servers
  - IIS servers, including config information
  - Other Zope and Plone servers
- Store custom attributes for all objects
  - Users, groups – even create new object types

Microsoft Message Queue

- Simple COM interface to all MSMQ features
- Client applications can submit messages from anywhere on the network
  - Zope can read these messages and process them
- Zope can submit messages for other applications
  - Picture a server dedicated to creating PDF versions of content

enfoldsystems

Windows Encryption

- Builtin facilities for encrypting sensitive data
  - No need to rely on external encryption
  - “Don't blame us” if MS screws up :)
- Some restrictions
  - Can only be decrypted by the same user
  - Generally only on the same machine
  - Suitable for information that can be re-acquired – such as passwords.
- may require a pywin32 update

enfoldsystems

About Index Server

- Service that scans and indexes all content on your hard disk
- Execute sophisticated queries against this content
- Pluggable system to “crack” documents into words and properties.
  - So 3rd parties can have custom formats indexed.
  - Used by main index server, but can be used directly by apps to crack individual docs.

enfoldsystems

Using Index Server

- Query indexed content.
  - Locate all objects outside of Zope that meet certain criteria
- Crack Individual documents
  - Reuse the IndexServer pluggable system to extract works and properties from files.
  - Suitable for use by the catalog

enfoldsystems

Index Server Limitations

- Tied closely to indexing a file-system
  - No effective way of “feeding” content - all it can do is scan the file-system
- Extracting content from documents requires a temporary file

enfoldsystems

Using COM with Zope/Plone

- Full win32com support exists in Zope
  - IndexServer, MSMQ, ActiveDirectory all rely on it.
- May be suitable for a cross-language “plugin” system for your application
  - Allow your clients to implement their own components using VB, .NET, etc
  - Use almost any COM component
    - Microsoft Provided (DAO, ADO, WMI)
    - 3rd Party Provided (you name it!)

Using COM with Zope/Plone (cont.)

- Threading Complications
  - Requests are not called by the main thread – CoInitializeEx necessary
  - Can't simply pass COM objects between threads
  - Python Programming on Win32 covers this
- Desktop Complications
  - Services generally can not interact with the desktop
  - COM objects that create a GUI may fail

Examples and More Information

- Can be tricky to find the information you need
  - Often not Zope specific
    - python-win32@python.org
    - Python Programming on Win32
  - Often not even Python specific
    - Look for examples in C++, VB etc
- Following are some examples and pointers to information you can browse over

Windows Authentication

- pywin32 'sspi' demos
  - Demonstrates how to fetch a URL from a server using NTLM auth
    - Eg, a secure page on an IIS site
  - Demonstrates how to perform server authentication and impersonation
    - Sadly not in a form ready for Zope
  - *win32\demos\security\sspi*

enfoldsystems

ActiveDirectory

- pywin32 ActiveDirectory samples
  - Examples of searching and updating the ActiveDirectory
  - Demos of how to register “services” in AD, and managing security on AD objects
  - *win32comext/adsi/demos*
- Wealth of VB ActiveDirectory samples
  - As above, search beyond the Python world for specific examples

Query Index Server

```
>>> from win32com.client import Dispatch
>>> q = Dispatch('IXSSO.Query')
>>> q.Query = "@filename *.txt"
>>> q.Columns = "DocTitle, DocAuthor, ..."
>>> rs = q.CreateRecordSet('sequential')
>>> for field in rs.Fields:
...  print field.Name, field.Value
...
DOCTITLE None
DOCAUTHOR None
CREATE 06/17/98 14:00:00
WRITE 06/17/98 14:00:00
FILENAME rds11readme.txt
>>> rs.MoveNext()
>>>
```

Query Document Properties

- pywin32 demo dumps all information about a supported document
- ```
  % filterDemo.py Itinerary.pdf
  Body
  ... many words snipped! ...
  Properties
  body : <body length: 40140>
  author : Virgin Blue Airlines Pty Ltd
  description : Virgin Blue Tax Invoice ...
  title : Virgin Blue Tax Invoice ...
  ```
- *win32comext\ifilter\demo*
  ```

Message Queue

- Put item in message queue
- ```
  >>> from win32com.client.gencache import
  EnsureDispatch
  >>> from win32com.client import constants as c
  >>> info = EnsureDispatch('MSMQ.MSMQQueueInfo')
  >>> info.PathName = r'.\Private$\Foo'
  >>> q=info.Open(c.MQ_SEND_ACCESS,
  ...             c.MQ_DENY_NONE)
  >>> message = EnsureDispatch('MSMQ.MSMQMessage')
  >>> message.Body = "Foo"
  >>> message.Send(q)
  ```
- Getting a message is a very similar process.
- Assumes queue exists, but can be created
  ```

Windows Encryption

- `>>> import win32crypt`
- ```
  >>> b = win32crypt.CryptProtectData("Data",
  ...             "Data Desc",
  ...             None, None, None, 0)
  >>> b
  "\x01\x00\..."
  >>> win32crypt.CryptUnprotectData(b, None,
  None, None, 0)
  [u'Data Desc', 'Data']
  ```
- Please read MSDN
- Simple to use, and not our fault if it gets cracked :)
  ```

Summary and Questions

Contact me at

mark@enfoldsystems.com

The End