

# Lotus knows.

Smarter software for a Smarter Planet.

## BP108 Worst Practices.... Orlando we have a problem

Paul Mooney | Senior Architect, Bluewave  
Bill Buchan | Directory, HADSL



CREATED WITH LOTUS® SYMPHONY™

lotusknows.com



**Lotus knows.**

Smarter software for a Smarter Planet.

**Stand for the pledge....**

**Lotus knows.**

Smarter software for a Smarter Planet.

I

**state your name**

**Lotus knows.**

Smarter software for a Smarter Planet.

**Pledge solemnly**

**Lotus knows.**

Smarter software for a Smarter Planet.

**To fill out the evaluation for this session**

**Lotus knows.**

Smarter software for a Smarter Planet.

**And give excellent evaluations**

**Lotus knows.**

Smarter software for a Smarter Planet.

**No matter how hungover Bill is**

**Lotus knows.**

Smarter software for a Smarter Planet.

**And further more....**

**I shall wear a yellow banana costume to the closing session and memorise the legal disclaimer at the end of every session.**

# Lotus knows.

Smarter software for a Smarter Planet.

**So say we all :)**

# Lotus knows.

Smarter software for a Smarter Planet.

## BP108 Worst Practices.... Orlando we have a problem

Paul Mooney | Senior Architect, Bluewave  
Bill Buchan | Directory, HADSL



CREATED WITH LOTUS® SYMPHONY™

lotusknows.com



## Who are we?

- Bill Buchan
  - Supreme commander
  - HADSL
  - We make a very good product
- Paul Mooney
  - Lowly admin guy
  - Bluewave Technology
  - Does a lot of Notes stuff

# Lotus knows.

Smarter software for a Smarter Planet.

## What did we do this weekend?



**Lotus knows.**

Smarter software for a Smarter Planet.

## What did we do this weekend?



# Lotus knows.

Smarter software for a Smarter Planet.

## What did we do this weekend?



**Lotus knows.**

Smarter software for a Smarter Planet.

## What did we do this weekend?



## What is this session about?

- Mistakes are made by everyone
  - How do you deal with them?
  - Blame?
  - Ignore?
  - Denial?
- Large or small
  - Enterprise or SMB
- Know your environment
  - Especially if you inherit it
- Prevention beats the hell out of the cure
  - As you will see

## Other titles for this session

“ Worst Practices. You can't fix stupid”  
Paul Mooney

“ Worst Practices. Because you're worth it”  
Duffbert

“ Worst Practices. It's back and its pi\$\$ed”  
Bill

## Other titles for this session

“ Worst Practices. The investigation into non IBM caused software related situations that may or may not of caused momentary challenges to the strategic paradigm in the collaborated community of the smarter live e-planet which is not affiliated, related or liable to IBM, any subsidiary, partner, software, product, vendor, technology, hardware, gadget, race, colour, creed, gender, life form, non life-form, past, present or future...

Express”

## Agenda

- For each case study, we shall
  - Look at the errors
  - Diagnose the problem
  - Determine the problem
  - How was it resolved
  - What lessons can be learned
- We have 10 case studies
- We cover both infrastructure and development...
- All new
- All true
  - Seriously, you can't make these up....

## Case Studies

- In case of emergency
- Out of employment
- “Sure, thats an easy change”
- Mobile madness
- DAOS done dumbly
- Readers and Authors Unpeeled
- Workspace Blues
- Web Views from Hell
- Discovered Check
- Lotusknows lotusnotes

Shorties..

## 1 In case of emergency

- The Story...
  - A large corporate environment
  - Moved to managed service
  - Single data centre
  - Mother of all SANs
    - Domino/Citrix/Notes
  - Excellent contingency documentation
    - Full procedures documented
  - Data centre shuts down over weekend
    - Everything is down

## 1 In case of emergency

- The Cause
  - New data centre
  - Full data centre air conditioning
  - Power for DC air conditioning
    - Linked to power system for building air conditioning
  - Weekend
    - Fire alarm tripped
    - False alarm
    - Automated system
    - Shuts off air conditioning
    - INCLUDING DATA CENTRE
  - Things get warm in there
    - SAN did not shut down from heat
    - Hard crash of SAN

## 1 In case of emergency

- The Investigation and Resolution
  - All SME's called to site
  - Gentle power up of data centre
  - Documentation for restart of SAN and primary applications
  - Bring everything back online.. slowly
    - Damage to backup system and drives
  - Full test of systems/applications/user access
  - Restart everything again
  - Check logs
- This took two days
  - Why?

## 1 In case of emergency

- Lessons learned
  - You get what you pay for
    - Full documentation on restore process is excellent
    - Everything proceduralised for this situation in documentation
    - Presented to customer before implementation of Data Centre
    - Called the “redbook”
  - Customer kept the redbook
    - Saved as a PDF on the SAN
    - Backup not available

## 2. Readers and Authors unpeeled

- The Story...
  - Very large customer
  - Mission critical evaluation system
  - Lots of reader fields
  - And one day, lots of documents disappeared
- The Investigation
  - Analysed replication history, logs, etc.
- Gotcha!
  - Only one user had a large number of deletions..
  - Did you delete 1,565 documents ?
    - No....

## 2. Readers and Authors unpeeled

- Cause
  - He was impatient and didn't want to wait for the hub to replicate with his server...
    - He had manually replicated between a hub based server, and his normal server
    - It had used his credentials
    - It had removed all the documents he didn't have access to
- Resolution
  - Clear replica history and re-replicate
    - Thankfully it was caught quickly
  - Shoot the user
  - Fix the access control on the servers

## 2. Readers and Author fields unpeeled

- Lessons learned
  - Reader/Author fields are dangerous. Like scissors. Don't run with them
  - Don't let users replicate between servers
- And while we're at it (and you've heard all this before)
  - Always use canonicalised names in a reader, author or names field.
    - Don't use abbreviated or common names for hierarchical users
  - Multiple entries in a field require use of a multi-value field!
    - Well, d'oh!
  - Always create a database role or group entry for the servers
  - Anytime you want to change them
    - Stand well back
    - Test, test and test again
    - Don't run it on live..
  - Full Access Administrator is your friend

## 3 Out of employment

- The Story...
  - 18,000 user site
  - Limited administrators / developers
  - Developer goes on leave Friday evening
  - Monday morning
    - The developer has received 6000 emails from different people
    - Help desk going nuts with calls about vacations
- The Investigation
  - Hands off everything
  - Review support calls
  - Review log file
  - Numerous agents executing
  - Opened a mail file

## 3 Out of employment

- Gotcha!
  - Out of office agent enabled
  - In everyone's mail file
  - By one developer
- The Cause
  - The developer was working
  - Call from Manager
    - He forgot to enable OOO
    - Asked dev to enable for him
  - Dev enabled OOO
    - In template (person was working there)
  - Design task ran
    - Everyone's OOO enabled

## 3 Out of employment

- Resolution
  - Disable OOO in template
  - Run the design task
  - Inform users
  - Address emails
- Lessons learned
  - “Quick fixes for users are bad ideas”
    - Call logging system
  - Template modification in production domain is dangerous
    - Release management systems?
    - Application template management?
  - Just because you can, doesn't mean you should
    - The Boss should of logged a support call

## 4. Workspace blues

- The Story...
  - A multinational, multibillion pound approval system
  - About a heartbeat before a huge deal closes...
    - All the users are locked out of the production web application
- The Investigation
  - Check logs
  - Check http stack
  - Check change control
  - Check security
- Gotcha!
  - The Database Access Control 'Advanced' setting 'Maximum Internet Access' had been set to 'none'

## 4. Workspace blues

- Cause
  - Release team were deploying a new test application into the test environment
  - The developer's workspace had become corrupted
  - The icon for the 'test' environment was mistakenly pointing at Production
  - The same User ID had 'god' access in Test and Production
  - Changes being made to "test" were actually being made to production
- Resolution
  - DONT use the same ID for all environments.
  - For release, use ID's that only work in the target environment
- Lessons learned
  - Shoot the Admin / Developer- (we can't agree on this)
  - Shoot both?
  - Don't rely on 'Workspace' icons. Workspace, even in 8.5.1, becomes corrupt surprisingly easily

## 5 That's an easy change

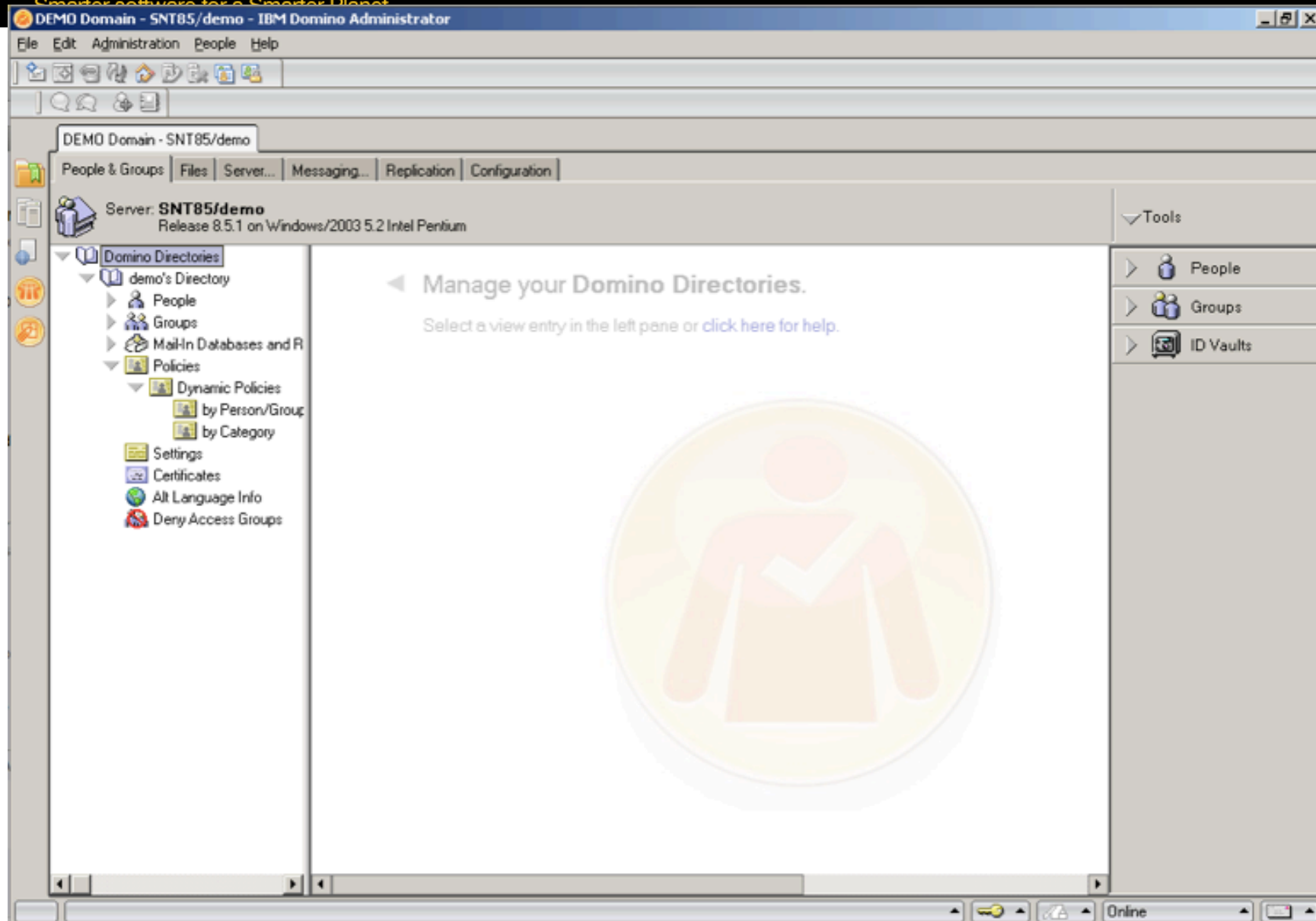
- The Story...
  - 24,000 global user site
    - Centralised management of domino domain
    - Dynamic, cutting edge site
  - Acquire new companies frequently
    - Mandatory migration to domino
  - One day
    - VAST majority of inbound internet email fails
    - SMTP Domain errors

## 5 That's an easy change

- The Investigation
  - Hands off everything
  - Check DNS
  - Check MX records
  - Review support calls
    - Any commonalities in the domain suffix?
  - Check delivery failures
    - Delivery failures in Domino excellent
  - Ask for change control logs
  - Review router logs
  - Check SMTP servers
    - Enhance SMTP logging
- Gotcha
  - Checked the global domain document

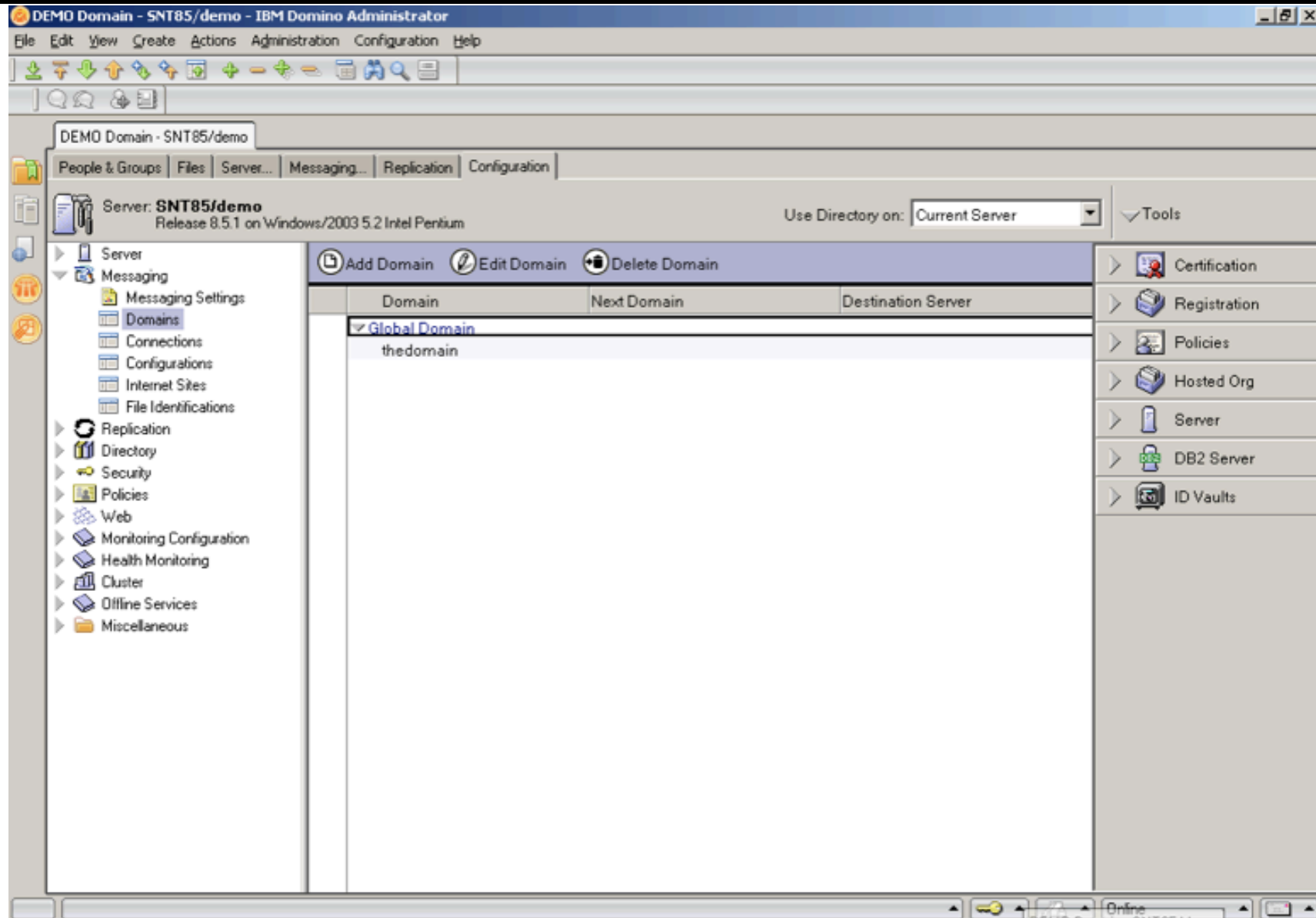
# Lotus knows.

Smarter software for a Smarter Planet



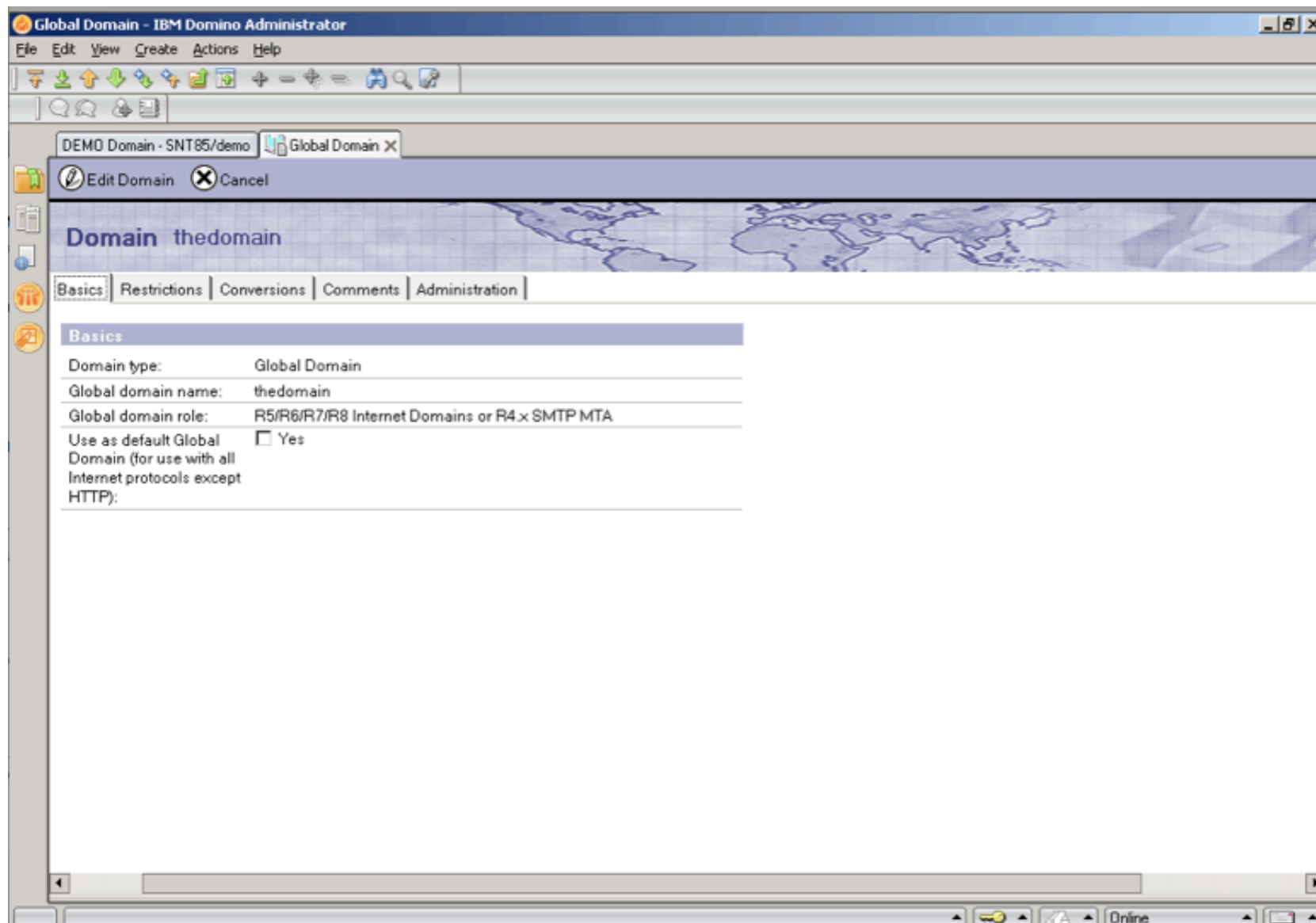
# Lotus knows.

Smarter software for a Smarter Planet.



# Lotus knows.

Smarter software for a Smarter Planet.



# Lotus knows.

Smarter software for a Smarter Planet.



# Lotus knows.

Smarter software for a Smarter Planet.

Global Domain - IBM Domino Administrator

File Edit View Create Actions Text Help

DEMO Domain - SNT85/demo Global Domain X

Save & Close Cancel

## Domain thedomain

Basics | Restrictions | Conversions | Comments | Administration

SMTP Address Conversion	X.400 Address Conversion
Local primary Internet domain: <input type="text" value="COMPANYNAME.COM"/>	Outbound mail restriction <input type="text" value="Restrict to global domain"/>
Alternate Internet domain aliases: <input type="text" value="OTHERCOMPANY.COM OTHERCOMPANY.NET PMOONEY.NET BILL.NET JOE.NET EDBRILL.NET LOTUSNOTES.NET EVENMORECOMPANIES.NET ALLTHECOMPANIES.NET"/>	Country name: <input type="text"/>
Internet address lookup: <input type="text" value="Disabled"/> <i>If disabled or no match</i>	ADMD name: <input type="text"/>
Local part formed from: <input type="text" value="Full name"/>	PRMD name: <input type="text"/>
Domino domain(s) included: <input type="text" value="None"/>	Domino domain attribute: <input type="text" value="None"/>
Domino domain(s) position: <input type="text" value="Left of '@'"/>	
Domino domain separator: <input type="text" value="% - percent sign"/>	

This is the protected text area of the form.

Online

# Lotus knows.

Smarter software for a Smarter Planet.

The screenshot shows the IBM Domino Administrator interface for configuring a domain named 'thedomain'. The window title is 'Global Domain - IBM Domino Administrator'. The interface includes a menu bar (File, Edit, View, Create, Actions, Text, Help) and a toolbar with various icons. Below the toolbar, there are tabs for 'DEMO Domain - SNT85/demo' and 'Global Domain X'. A 'Save & Close' button and a 'Cancel' button are visible. The main content area is titled 'Domain thedomain' and has several tabs: 'Basics', 'Restrictions', 'Conversions', 'Comments', and 'Administration'. The 'Basics' tab is selected, showing two columns of configuration options. The left column is titled 'SMTP Address Conversion' and includes fields for 'Local primary Internet domain:' (COMPANYNAME.COM), 'Alternate Internet domain aliases:' (OTHERCOMPANY.COM, OTHERCOMPANY.NET, PMOONEY.NET, BILL.NET, JOE.NET, EDBRILL.NET, LOTUSNOTES.NET, EVENMORECOMPANIES.NET, ALLTHECOMPANIES.NET), 'Internet address lookup:' (Disabled), 'Local part formed from:' (Full name), 'Domino domain(s) included:' (None), 'Domino domain(s) position:' (Left of '@'), and 'Domino domain separator:' (% - percent sign). The right column is titled 'X.400 Address Conversion' and includes fields for 'Outbound mail restriction:' (Restrict to global domain), 'Country name:', 'ADMD name:', 'PRMD name:', and 'Domino domain attribute:' (None). At the bottom of the window, there are status icons for 'Online' and a small globe icon.

# Lotus knows.

Smarter software for a Smarter Planet.

The screenshot shows the IBM Domino Administrator interface. The title bar reads "Global Domain - IBM Domino Administrator". The menu bar includes "File", "Edit", "View", "Create", "Actions", "Text", and "Help". The toolbar contains various icons for file operations and navigation. The main window displays the configuration for a domain named "thedomain". The interface is divided into two main sections: "SMTP Address Conversion" and "X.400 Address Conversion".

**SMTP Address Conversion**

- Local primary Internet domain: COMPANYNAME.COM
- Alternate Internet domain aliases: newcompany.com4
- Internet address lookup: Disabled
- Local part formed from: Full name
- Domino domain(s) included: None
- Domino domain(s) position: Left of '@'
- Domino domain separator: % - percent sign
- Address example: JMD@acme.com
- Outbound mail restriction: Unrestricted

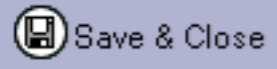
*NOTE: The following settings are not used in R5, R6, or R7. They only apply to R4.x SMTP MTAs*

**X.400 Address Conversion**

- Outbound mail restriction: Restrict to global domain
- Country name:
- ADMD name:
- PRMD name:
- Domino domain attribute: None

# Lotus knows.

Smarter software for a Smarter Planet.



# Lotus knows.

Smarter software for a Smarter Planet.

**It replicates to the SMTP server.....**

# Lotus knows.

Smarter software for a Smarter Planet.



## 5 That's an easy change

- The Cause
  - The administrator was asked to add a new smtp domain to the global domain document
    - This means the domino server will accept messages addressed to that domain
  - He did
    - Accidentally selected all the other alternate domains
    - added "new" domain
    - Saved
    - Router reloads configuration
    - Stops accepting inbound email for other domains

## 5 That's an easy change

- Resolution
  - Add in the alternate domains again
    - Do this on SMTP inbound server if under pressure
    - Tell router update configuration
    - Mails start to come inbound again
    - Shoot administrator
- Lessons learned
  - Limit access to names.nsf
  - CHANGE CONTROL
  - Procedure your changes
  - Test processes

## 6. Web views from Hell

- The Story...
  - A large, mandatory tracking system, web clients
  - Users would wait 10-20 minutes to open a view,
    - 10-20 minutes to page forward, etc
  - Servers were on their knees
- The Investigation
  - The web application used a notes agent to construct the client view
  - It generated XML for the entire view, and passed this back

## 6. Web views from Hell

- Gotcha!
  - Each page being passed back was over 4mb in size!
- Cause
  - The view contained every view entry, despite the client only being able to display the first 100 or so
  - The developer, in testing, only had 100 or so documents. The target system had 100,000+ documents
- Resolution
  - Fix the views
    - Use AJAX from the client to call 'ReadViewEntries' and render properly
- Lessons learned
  - XML is great - when used correctly.
    - When used badly, it can perform as badly as 'old' technology

## 7 Mobile madness

- The Story...
  - Small customer site
  - Implemented Lotus Traveler (1st release)
  - All is well
  - Person loses their windows mobile device
  - Reports it to IT
  - IT said they will disable account
- Next day
  - Person's address book "empties"
  - New contacts start appearing
    - People the customer does not know

## 7 Mobile madness

- The Investigation
  - Check Log.nsf
  - Check traveler configuration
- Gotcha
  - Account still active on traveler
  - Mobile device in use!
  - BUT - The admin guy reset the password?!

## 7 Mobile madness

- The Cause
  - The administrator was asked to “deal with losing mobile device”
  - No device wipe at the time on WMD
  - Reset the internet password to “password” to lock out account
    - Problem - the last password was “password”
    - Account remained active
  - Meanwhile.....
    - Thief ignores traveler
    - Deletes all the contacts on the device
    - This syncs with the contacts in the mail file
    - This syncs with the pnab
    - Using “Synchronise contacts feature”

## 7 Mobile madness

- Unusual resolution
  - One of the “new” entries is DAD.. with mobile number
  - The customer KNEW the dad
  - Customer calls the mobile number
  - A conversation is had
  - Mobile device returned... with apology
- Lessons learned
  - Incident lead password resets need to be more complex
  - Password reset policies need to be implemented in your domain
  - Complexity levels need to be implemented in your domain

## 8. Discovered Check

- The Story...
  - A huge organisation tracking client confidential information
  - Being moved from one part of the organisation to another
  - One side outsourced to a service provider
  - System was migrated, but some agents consistently failed
- The Investigation
  - The agents' code was examined in some depth - no bugs found
  - Systems were examined in detail (where available)
    - No obvious misconfigurations found
  - Finally, a copy of the system was ran in isolation...

## 8. Discovered Check

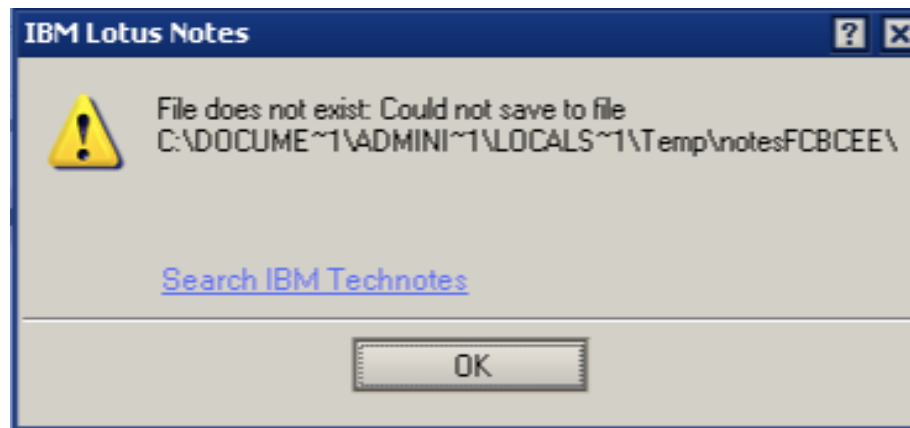
- Gotcha!
  - The agents were timing out
- Cause
  - The agents were designed for a run-time of 1 hour, not the 10 or 15 minutes default
  - The old system was set to a 1 hour timeout
  - The old system didn't kill agents
- Resolution
  - Recoded agents to run in 10 or 15 minute time windows

## 8. Discovered Check

- Lessons learned
  - Every time a system changes ownership, information is lost
  - In this case, an assumption about server setup - each server had to set agent timeout to an hour
  - Institute proper logging for all agents
    - Start time, end time, all run-time errors, terminations event
    - In this case, no end-time comments led to the assumption that the terminated agent completed successfully
  - Document - in the agents - that they require a non-standard environment
  - Test, test, and test again, in a representative test environment
    - Same hardware, same documents, same views, same versions

## 9 DAOS done dumbly

- The Story...
  - Mid size customer site in Europe
  - Desperately low on free disk space
  - Eagerly awaiting DAOS to be released
  - Implemented in in January 2009
    - It was out only a few days
  - Few months later OS failure
  - Box to be rebuilt
  - Customers start to complain opening attachments



## 9 DAOS done dumbly

- The Investigation
  - Review the error message
  - DAOS .nlo related
  - Review daoscatalog database
  - Query for missing .NLO files
- Gotcha
  - ALL the .NLO's missing

## 9 DAOS done dumbly

- The cause
  - When doing rebuild
  - Administrator restored all .nsf files from the previous night's backup
  - Nightly backups did not include the DAOS directory
  - Monthly backups did not include DAOS directory
    - No copy of attachments
- Resolution
  - Replica copies of mail files from DR server
  - If there were no replicas of these .nsf files?
    - Prayer?

## 9 DAOS done dumbly

- Lessons learned
  - Be aware of what DAOS is
  - Fantastic tool
    - Very new
    - Different container model
  - Understand DAOS and backups
  - Understand any new technology before you implement it
  - COMMUNICATE
    - Did you tell your backup team about DAOS
  - Disaster recovery tests?
    - Complete after every major system change/upgrade
    - AND, on schedule too!

## 10. LotusKnows lotusnotes

- The Story...
  - Very Large financial organisation using Lotus Notes for everything
  - Request for a new expense approval application
  - Remote developer sends in the application for deployment
  - 1 year later... SERIOUS security breaches noticed.
    - SERIOUS INVESTIGATION
    - SERIOUS FINGER-POINTING
    - Who approved what?
- The Investigation
  - Check database access
  - Check reader fields/author signatures
  - Check ACL
  - Some expense claims appear to be forged. The client is blaming Notes Security.
- Gotcha
  - We reviewed some expense reports...
  - Expenses being submitted, approved, closed in sub - 5 minutes!

## 10. Lotusknows lotusnotes

- The cause
  - We reviewed the customer site
  - We found a H:\ drive directory called H:\notes\id files
  - We found a text file which stated all passwords were 'lotusnotes'
  - People were switching IDs and approving their own expenses
  - People were also deleting the submission/approval application emails
- The Resolution
  - Stop laughing
  - Shoot the admin
  - Enforce password changes
- Lessons Learnt
  - Security is holistic. It all is connected. There is no point in creating the worlds most secure safe, and then writing the combination on the door.

## Shorties...

- Don't have two domino domains with the same name in your organisation
- Check the code in you directory
  - Is there anything that shouldn't be there
- Using shared mail in 2010 should be illegal
- Dont keep "encrypted" text in clear text
- Remember to renew domains
  - We didn't

## Summary

- Everyone makes mistakes
- Put systems in place to prevent the obvious ones
- Its how you deal with them that makes you professional
  - No Blame Culture
  - Admit soon, Admit well...
- Major system disasters
  - Sometimes cant be prevented
  - Are usually the combination of many small errors
- Learn from these mistakes!

## Thank you

- Paul Mooney (pmooney@pmooney.net)
- Bluewave
- pmooney.net / bluewavegroup.eu
  
- Bill Buchan (bill@billbuchan.com)
- hadsl
- billbuchan.com / hadsl.com