

# BP 104 - Best Practices Clusters are Cheaper to Run !

## How to Secure Lotus Domino Clusters While Maximizing High Availability and Performance

[George\\_Chiesa@dotNSF.com](mailto:George_Chiesa@dotNSF.com)

[Daniel\\_Nashed@nashcom.de](mailto:Daniel_Nashed@nashcom.de)

Y & B GH V-VIII

Tuesday, Jan 28th

12:15pm - 1:30pm

HTML Document

## Legal Disclaimers and other fine print :-)

### ■ Trademarks:

- "dotNSF" is a registered Trade Mark of dotNSF, Inc.
- **All IBM Corp's Trademarks acknowleged.**
- **All other Trademarks acknowledged.**

### ■ License:

- dotNSF, Inc. hereby grants IBM the non-exclusive license with limited right to use, reproduce, display, perform, and distribute the presentation materials for Lotus' educational, marketing and promotional purposes, attributing dotNSF as the source. It may be placed on Lotusphere CDs, Lotusphere Web Sites, or other media at discretion of Lotus. Like most presentations, this one is best presented by the original authors/speakers, who had access to the raw material summarized here; thus we kindly request communication to us of the effective or intended reuse of this material: dotNSF, Inc - and NashCom - will make best efforts to have this material presented by the original speakers - upon request of IBM - or any other third parties, at very reasonable probono rates.

- **Copyright 2000-2003 dotNSF, Inc and its suppliers.**  
**All rights reserved (-: and we mean it :-)**

Please contact us for further information:



**the extension  
you already  
know**

**George Chiesa**

George Chiesa <[Chiesa@dotNSF.com](mailto:Chiesa@dotNSF.com)>  
Mobile Phone: [+44 771 85 87 673](tel:+447718587673)  
Tel/Ans/Fax: [+44 1753 830 600](tel:+441753830600)  
Web Site: <http://dotNSF.com>

"dotNSF" is a TradeMark of dotNSF, Inc.  
© MM dotNSF, Inc. All Rights Reserved  
It's about business, not just technology!



**Nash!Com**  
Communication Systems

Daniel Nashed

Weidenweg 58  
40723 Hilden  
Germany

+49 172 2141912  
[nsh@nashcom.de](mailto:nsh@nashcom.de)

Lotus/IBM Business Partner/ISV

## Abstract / Agenda

- *\*\*\* This is an advanced best practices presentation \*\*\**
- New IBM licensing makes Domino native clustering an even more attractive strategy. *[5 % of time allocated to licencing !]*
- We'll highlight the field tips & tricks, caveats & gotchas of deploying Lotus Domino Clustering in a secure and highly available way. *[75 % of time dedicated to technical issues !]*
- We'll also map out the integration with other IBM, Lotus, Sametime, QuickPlace, iNotes, Tivoli and Websphere products, including when and how to use secure reverse caching proxies, dispatchers, and more! *[ 20 % of time: Live Q&A ! ]*
- The post-presentation version will be available for download from our sites <http://dotNSF.com> and <http://nashcom.de>

# Skeleton Agenda (1 of 2)

- New Licensing
  - Clustering used to require to buy extra "Domino Enterprise License"
  - It now runs on the "Enterprise Server" & new "Domino Utility Server"
- What is Clustering?
  - Clustering 101 (intro to useful vocabulary)
  - what is "in the box"
    - what is called "1352 Native Clustering"
    - what is called "Internet Cluster Management (ICM)"
  - what else is available?
    - Why may I need something else?
    - How do I put this all together?
  - Other Issues with:
    - Native Notes Clients & iNotes w/ DOLS/
    - Sametime, QuickPlace, etc
    - Tivoli Access Manager for e-Business
    - Websphere Edge Server



## Skeleton Agenda (2 of 2)

### ■ Security

- Basics (101s, useful terminology + unusual bibliography)
- Implementation of an Internet Native Domino Cluster Security
  - How to design/deploy Internet Business Friendly Security
  - Certification and Cross-certification issues
    - How & why NOT to bother collecting SAFE.IDs
    - Why Collecting Signed Notes Documents.
- Implementation of Intranet and Extranet "http" based clusters:
  - Session Spraying, Stickyness, and other caveats
  - Directories, synchronization, referral, etc
  - Password, sync, issues, etc.
  - Single Sign-On/In a.k.a. SSO/SSI, including LTPA issues
- Security Interfaces with IBM Tivoli Access Manager for e-Business
- Security Interfaces with IBM Websphere Edge Server plug-ins

### ■ Questions and Answers:

- your chance to ASK whatever you want to hear in more detail !

## About the Speakers - George Chiesa

- Founder and CTO of "dotNSF, Inc."
- Former Loti who has been running Notes/Domino since V1.
- Pioneered usage of Native Notes Clustering over the internet for provisioning services to thousands of Business Partners in Lotus EMEA (Europe Middle East & Africa)
- dotNSF, Inc. specialises in IBM and Lotus Software high availability+security, with links to Tivoli and other pillars.
- dotNSF's product and tools, are IBM e-Serverproven and were finalist in Lotusphere 2001 "Best Tools" Beacon Awards.
- dotNSF is a proud member of the Penumbra Group

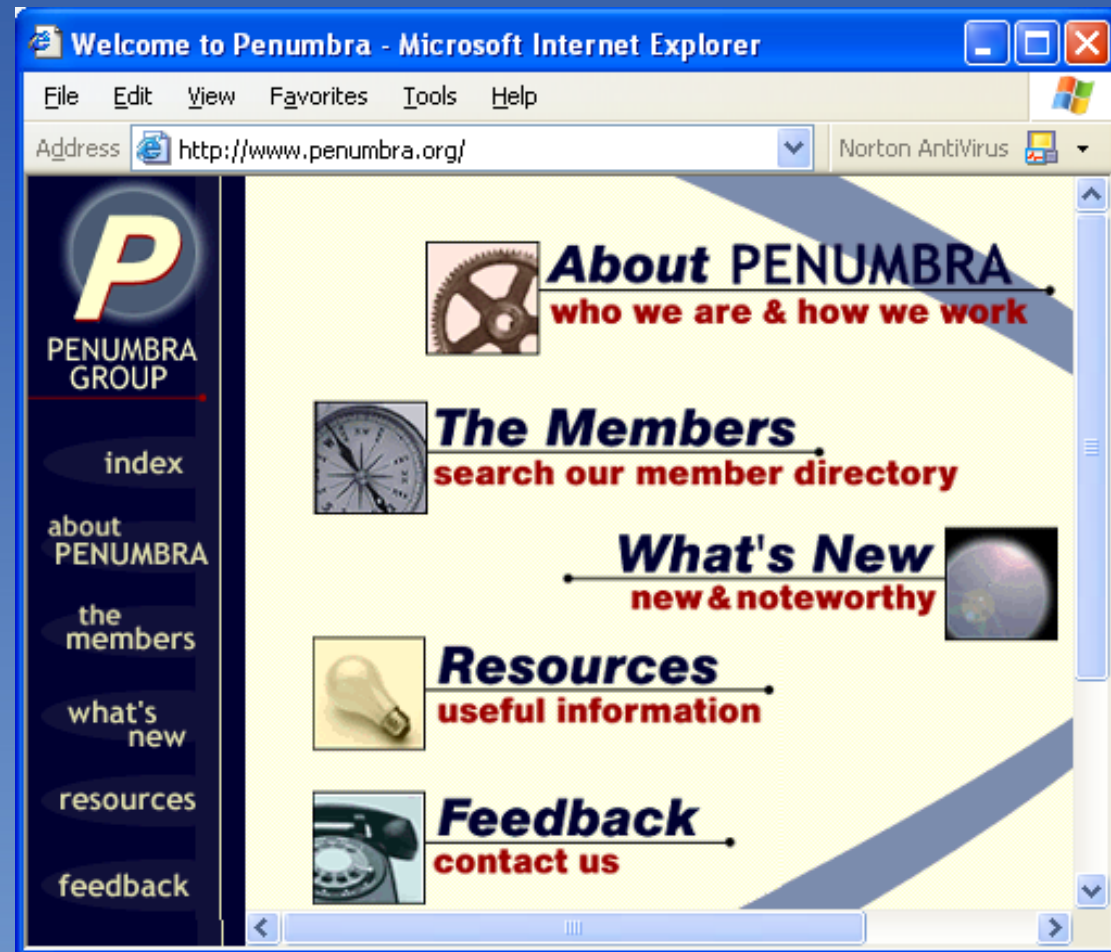
## About the Speakers - Daniel Nashed

- Nash!Com
  - Established 1999
  - first German member of Penumbra Group
  
- focused on
  - Cross-Platform C-API Dev.,
  - Domino Infrastructure,
  - Administration, Integration  
& Troubleshooting
  - on W32, Linux, AIX & Solaris
  
- Technical writer for Groupware Magazine (Germany)



# About Penumbra

- Penumbra Partnering Inc.  
<http://www.penumbra.org>
- Consortium of companies
  - pooling their resources
  - and management skills
  - to create the ideal
  - collaborative technology
  - provider network.



## From Lotus Operating Principles:

- "Establish Purpose Before Action"
  - as in
- Alice (In wonderland)
  - Tell me Mr. Cat, which "Route" should I use?
- Cat:
  - Where do you want to go ?
- Alice:
  - Dunno, haven't figured that out yet!
- Cat:
  - THEN...
  - it does not matter which one you choose!

## Q & A: YOUR chance to make this presentation more relevant for YOUR specific needs - ask !

- F I L L   Y O U R   E V A  
L  
- p l e a s e -
- if you don't have forms,
  - ask us,
  - we have them
- The BP TRACK
  - needs YOU
  - to fill the EVAL Forms !

## Q & A:

- ALL the "answers"
  - are already out there
    - somewhere
      - most, in the internet
  
- the KEY VALUE question is
  - how to figure out
    - WHAT ARE THE
      - RELEVANT QUESTIONS ?
  
- It's useful to define "relevant"
  - the "YOU ARE HERE"
    - has changed
      - from "my Domino World"
      - to "my Enterprise choices"

HTML Document

## The "Nines":

- 2 nines (99%) = circa= 88 hours/year
- 3 nines (99.9%) = circa= 9 hours/year
- 4 nines (99.99%) = circa= 52 minutes/year
- 5 nines (99.999%) = circa= 5 minutes/year
  
- Downtime costs per user = [  
(Total hours of Unscheduled downtime (25% of user population) X  
(Hourly user salary)  
+  
(Total hours of Scheduled downtime X Hourly Messaging Administrator  
Salary)  
] / Number of messaging users
  
- NOTA BENE: R.S.E. and Change Management/Control needs
-



# Money 101s: Total Cost of WHAT ?

- Check Our Clustering "BP112" Session last Lotusphere 2002 !

We will NOT cover again all the concepts, just the main issues.

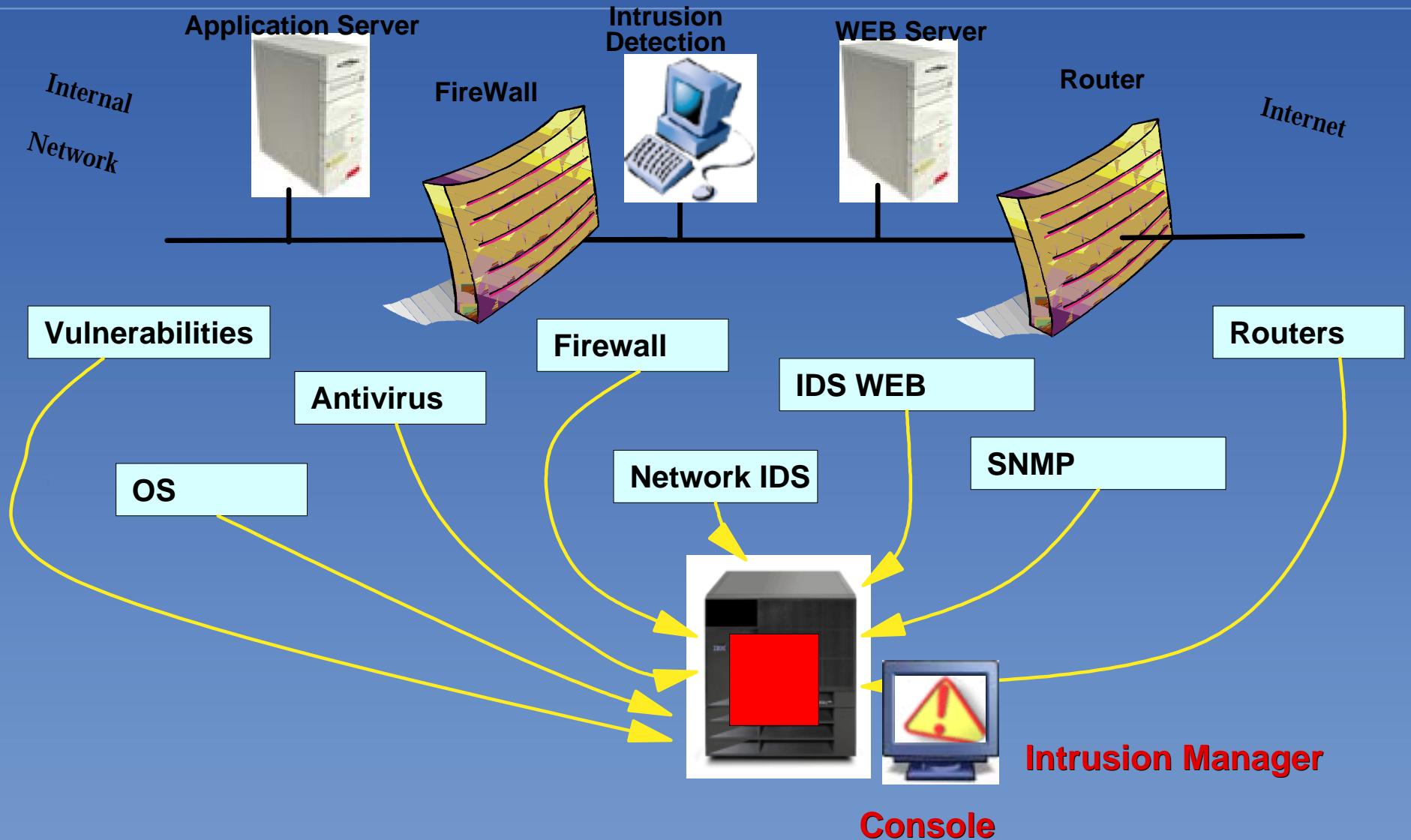
- It's NOT (just) what it costs to buy the hardware...
- It's NOT (just) the cost of licensing (but great news here)...
- It's NOT (just) the cost of people associated issues...
- It's NOT (just) the TCO = Total Cost of Ownership...
  
- IT IS HOW MUCH YOU LOOSE/WASTE/ETC when you do not have your mission critical system available as you expected!
  
- a.k.a. Your Total Cost of NON OWNERSHIP ! ! !

# Putting Things in Perspective

- The "i" in RAID stands for:  
***In-Expensive***
  - ▶ In 1987, Patterson, Gibson and Katz at the University of California Berkeley, published "A Case for Redundant Arrays of Inexpensive Disks (RAID)". This paper described various types of disk arrays, referred to by the acronym RAID. The basic idea of RAID was to combine multiple small, inexpensive disk drives into an array of disk drives which yields performance exceeding that of a Single Large Expensive Drive (SLED). Additionally, this array of drives appears to the computer as a single logical storage unit or drive.



# IBM Tivoli Intrusion Manager



# The IBM Tivoli Security Solution Portfolio

## Identity Management

Efficiency through role-based configuration

- Consistently enforce policies
- Automate processes
- Delivers on Service Level Agreements
- Reduce costs
- 

## Threat Management

### Align Systems Opps and Security enforcement

Align Systems Opps and Security enforcement

- Mitigate risks - lower cost
- Reduce Analysis costs
- Detect, Alert, & Respond in real-time
- Auditing and reporting for compliance

## Access Management

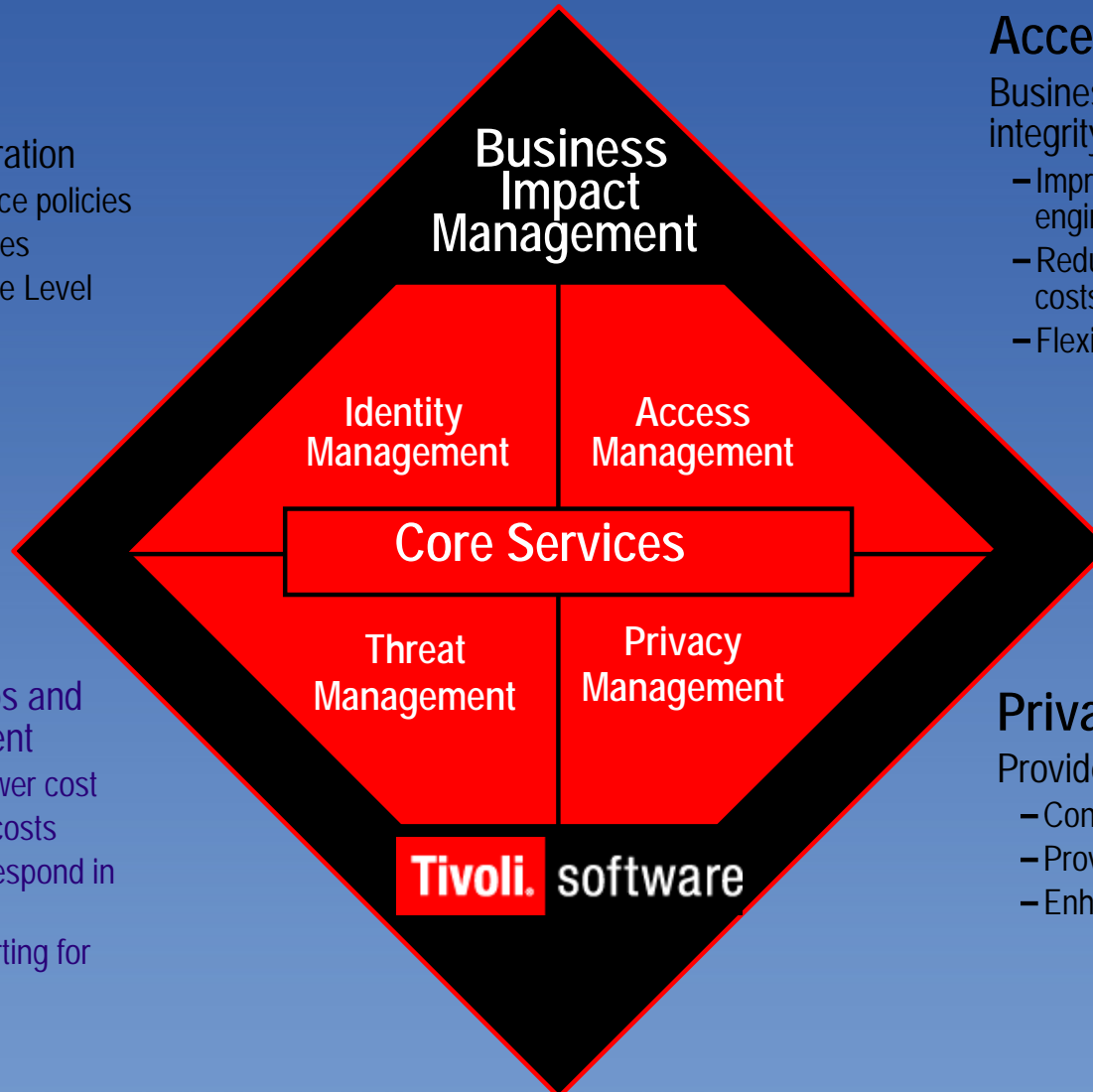
Business success dependent on IT integrity

- Improve ROI with common Security engine
- Reduce Application Development costs
- Flexible Authentication

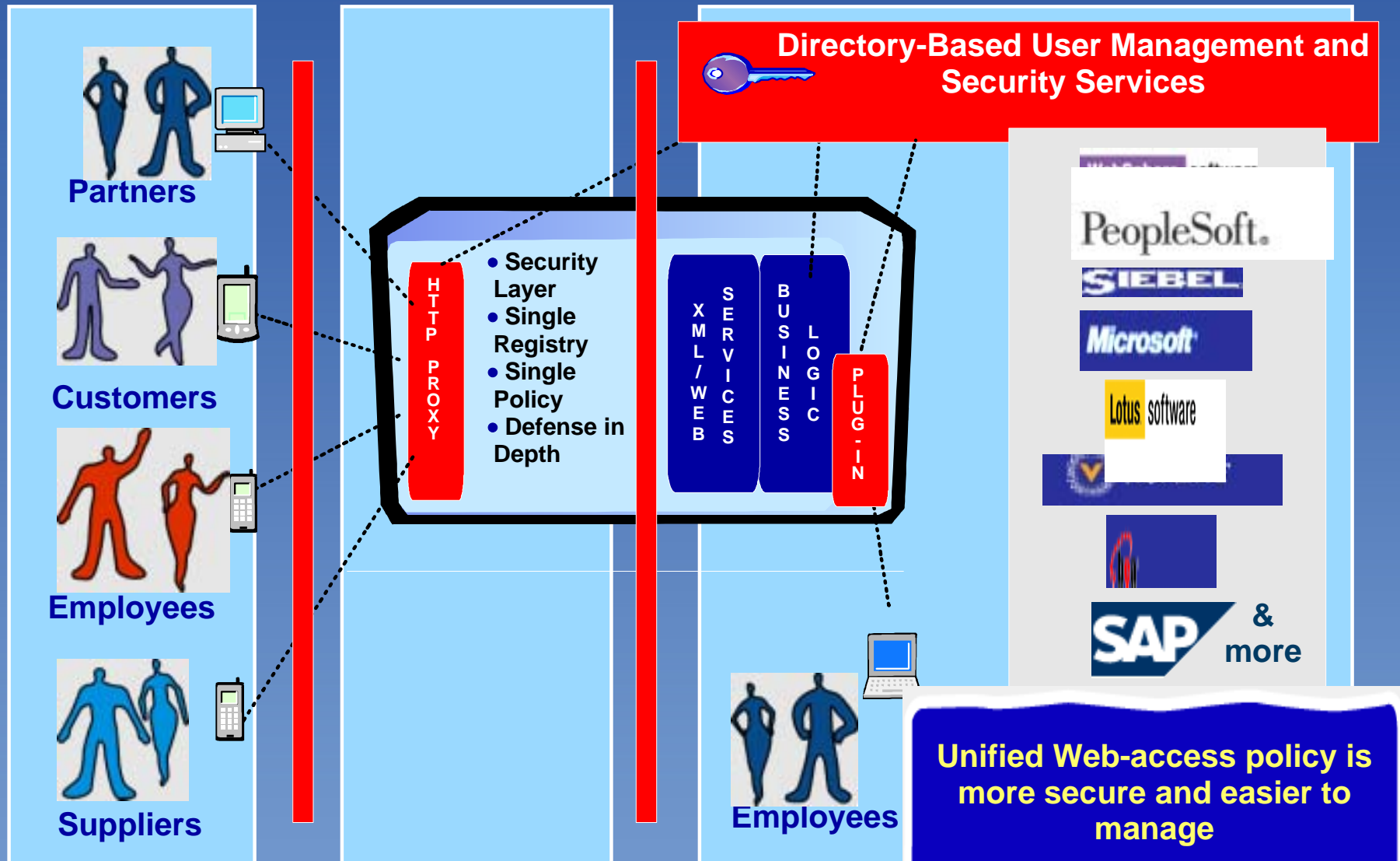
## Privacy Management

Provide user managed privacy

- Conform to EU/Country Laws
- Provide user choice
- Enhance Customer Care



# Customers Want Access Manager's Integrated Approach



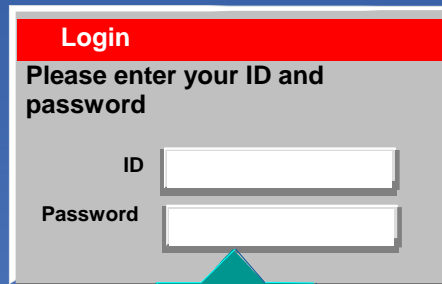
Open Internet

Demilitarized Zone

Secure  
Intranet



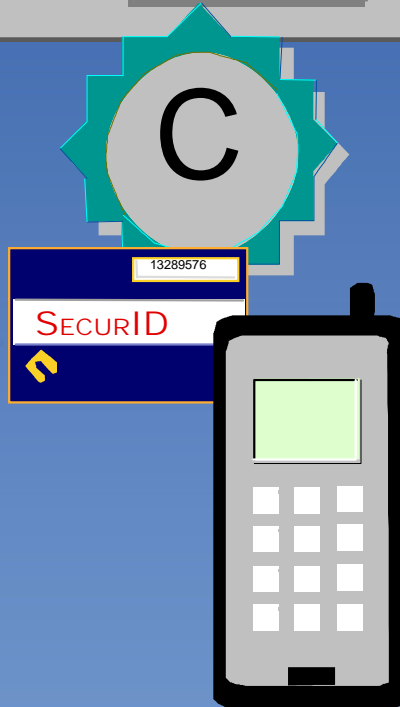
# Authentication Possibilities



**Login**  
Please enter your ID and password

ID

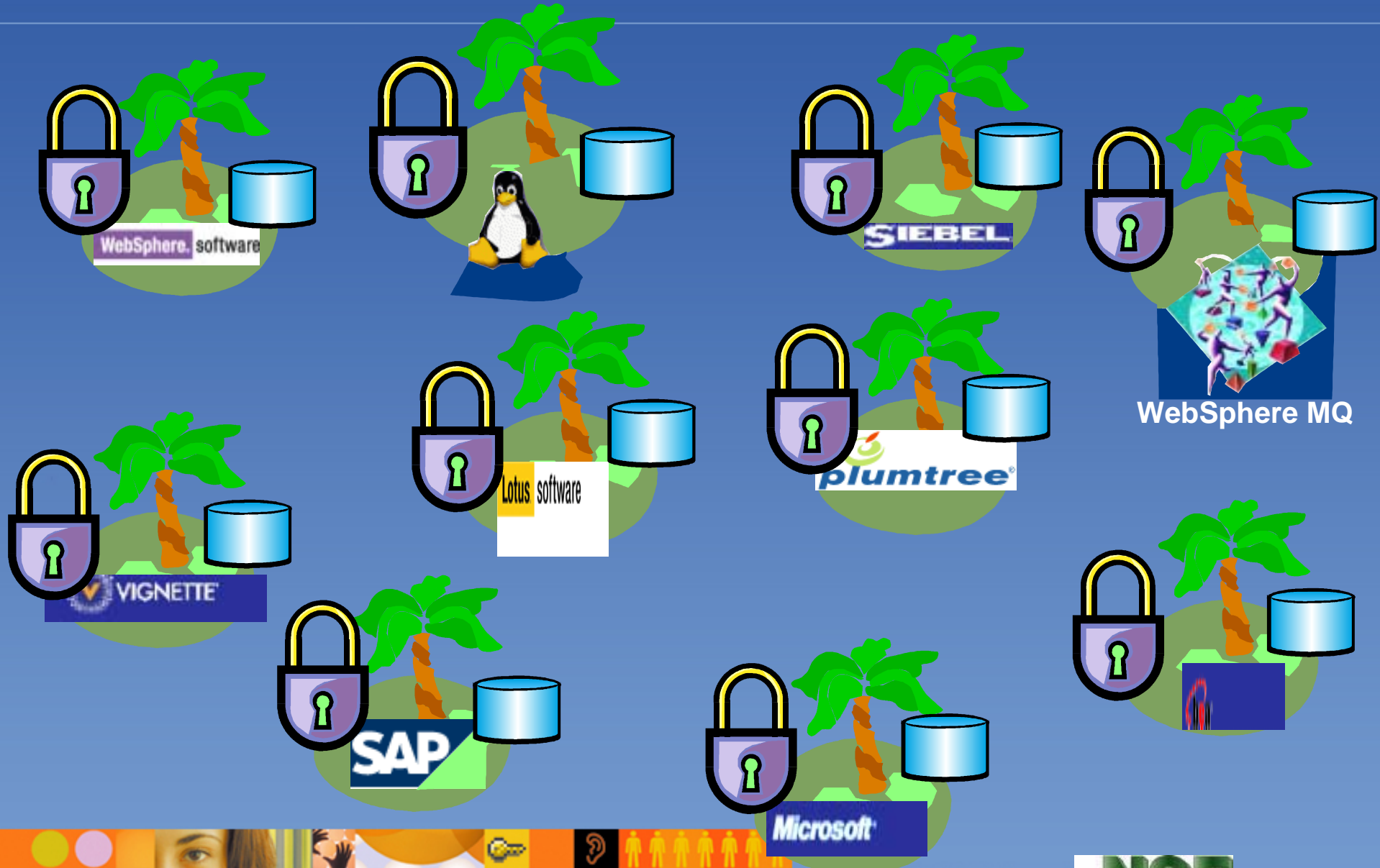
Password



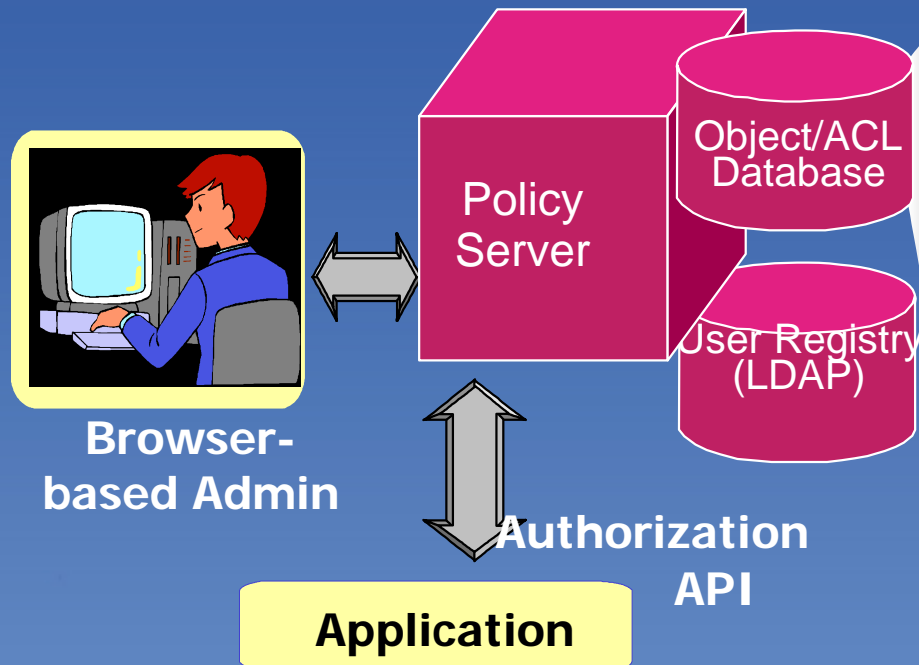
- *Forms-based login*
- *HTTP basic authentication*
- *Digital Certificate (X.509v3)*
- *RSA SecurID Token*
- *WAP identity mechanism*
- *Resource-sensitive authentication*
- *Custom methods*

# IBM has a solution for this problem...

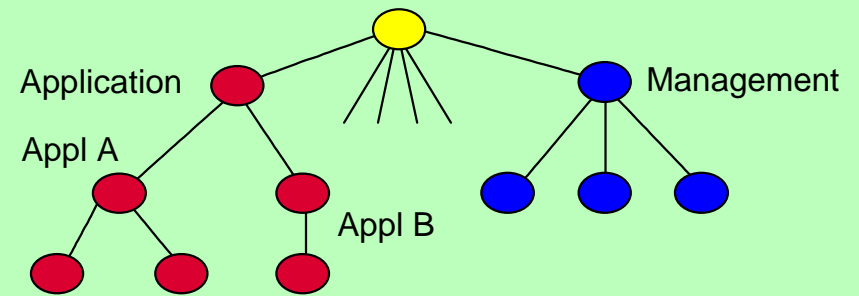
## Instead of This . . .



# Access Manager Administration Concepts



## Protected Object Namespace



## Policy Templates



Corporate Web ACL



Employee Database ACL

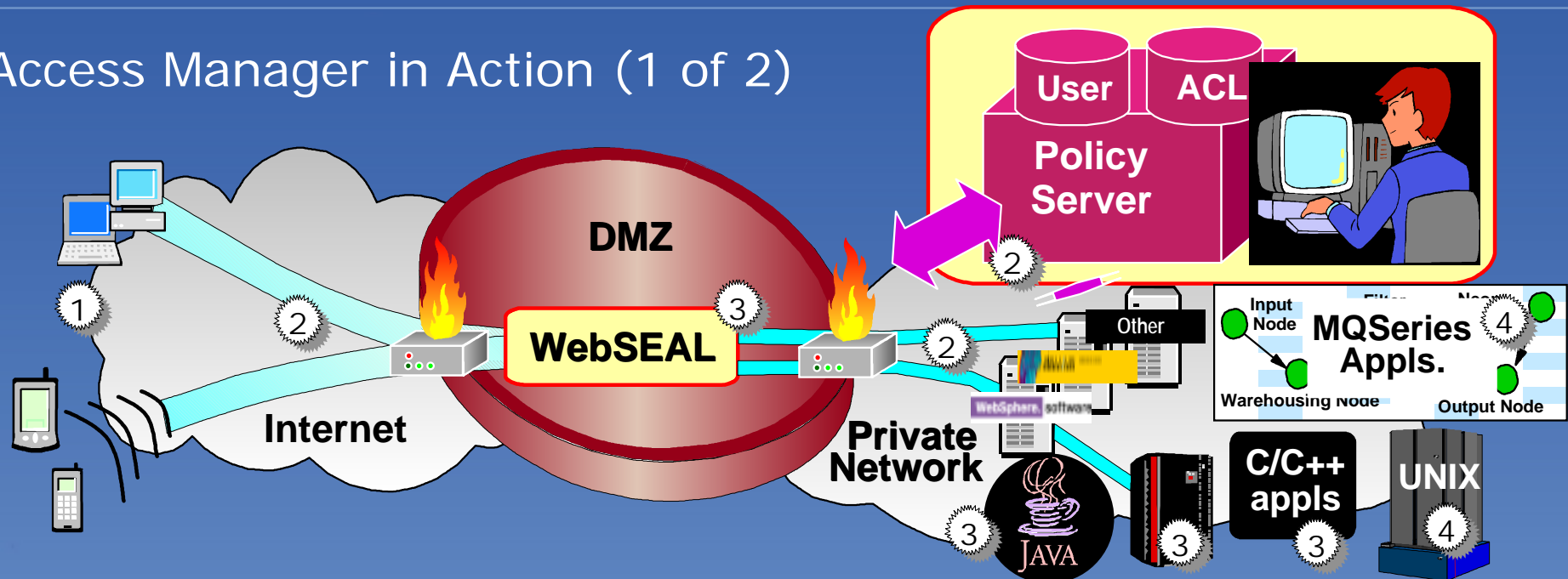


Protected Object Policy

- **Web-based Management GUI** (Delegatable admin)
- **Policy Manager** (Master Authentication/Authorization Services)
- **Single Security Policy** (Policy Templates applied to Namespace)
- **Single, Consistent Authorization Approach**

# Tivoli Access Manager

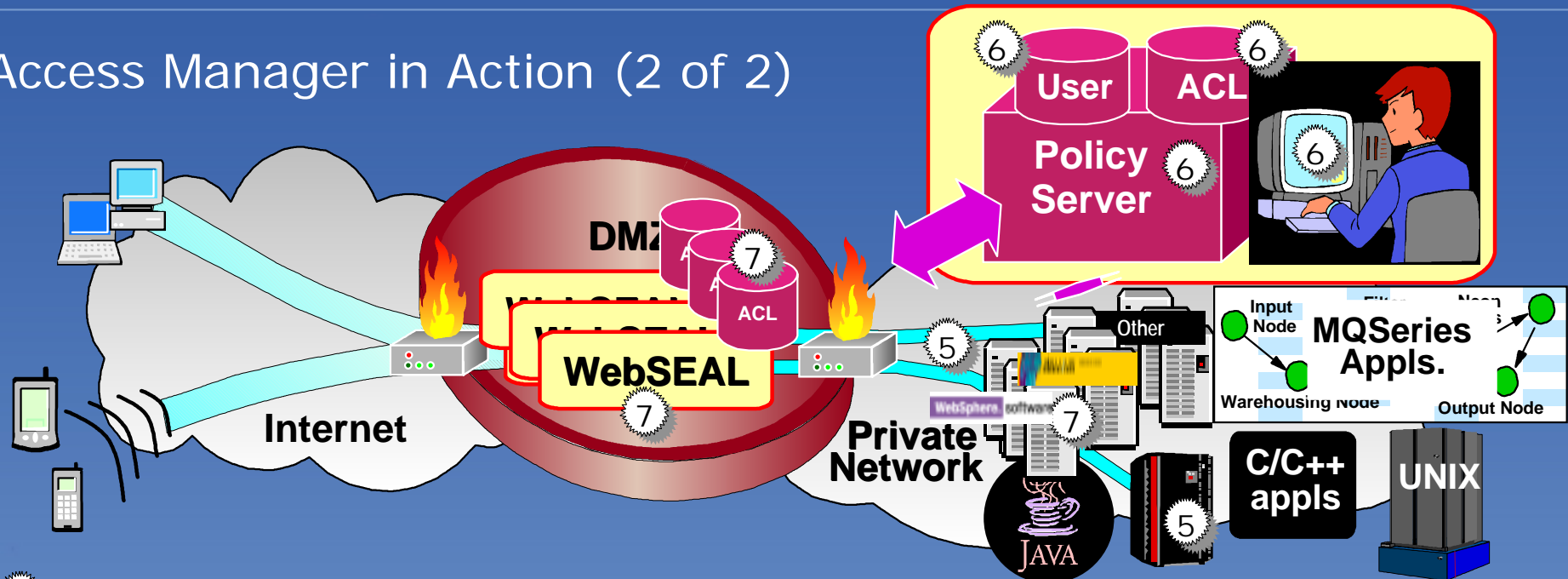
## Access Manager in Action (1 of 2)



- 1 Support multiple means of identity & address Web SSO (single/cross domain)
- 2 Ensure Access Manager's infrastructure is itself secure
- 3 Provide authorization services, with integrated security for WebSphere, Domino, BEA WLS, Siebel, mySAP, BroadVision, Plumtree, Vignette, . . .
- 4 Provide a basis for managing security for a broad range of targets (MQSeries, UNIX systems)

# Tivoli Access Manager

## Access Manager in Action (2 of 2)



- 5 *Provide robust, secure support for 2- and 3-tier transactions, in line with the IBM Framework for e-business*
- 6 *Deliver robust management tools*
  - *Centralized, browser-based, delegated administration*
  - *Support for multiple registries* (SecureWay, Netscape/iPlanet, Domino, AD)
  - *Single protected object namespace* (for multiple, heterogeneous resources)
  - *Comprehensive, policy-based audit*
- 7 *Ensure high availability and scalability* (via replication/caching/load balancing)



# TCO

- T.C.O. = Total Cost of Ownership
  - It's the TOTAL cost of running
    - a set of "stuff" to provide some "service"
  - This is how business people traditionally evaluate
    - HOW to do things
  - Implies that somehow somebody
    - decided that something is to be made/had
  - KEYS: "HOW" based just on alternatives TCOs

## Mission Critical Service

- Much better defined by the
  - Total Cost of NOT HAVING IT
  - when you need it
- In other words, something that despite
  - having a (well known?) TCO
  - may prove too much more significantly
    - painful & expensive "NOT TO HAVE"
- Keys: TOTAL costs of NOT having

# Business Users do NOT care what you do with your PLANNED down time

- as much as they care NOT to have ANY
  - UN-PLANNED down times during "biz time"
- Business users can plan around PLANNED un-availability of mission critical systems
- What Business Users can NOT usually accept
  - is having to have both Planned and UN-Pl'd
  - YOU CAN NOT REDUCE BOTH TO ZERO
    - on an individual component basis
- Key: "individual component basis"

## Never begin asking for budget...

- ask for preference/adversion
  - acceptable time of UNplanned downtime
  - against money to prevent them
- Have the user KEEP updated a contingency "Plan B" for alternative/manual processing, so they realise how much mission critical their system really is...
- TEST their plan B (fire drill :-)
- Ask again for the "TC of not Having"
- Ask again for "Not Having Adversion"

## High Availability

- My petty own TWO definitions
  - Historical = (ex-post)
    - the FACT that a service has been available
      - in the past
  - Predicted = (ex-ante)
    - a "PERCEPTION" in terms of Probability
      - that a service will be up
      - when it will be needed in the future
- KEY: do NOT extrapolate past availability



# Strategic Planning:

- My petty own definition (borrowed from many: -)
  - Analyze possible future scenarios/events, their value and impact to you
    - What can go wrong, and how much will it cost me/my entity NOT to have the service
  - Estimate the "a priori" / "pari passu" probability of these events
  - Analyze, decide and take actions TODAY that will improve the probability of the desired events and scenarios actually happening
- Keyword of this slide is TODAY

# There is no such thing as "THE BEST" practice as absolute recipe

- Does it make sense to ask ?
  - Will the server be up tomorrow?
  - NO SLA will make it happen...
    - at most you will get damages/penalties
- It makes sense to Actively Plan & Design:
- **WHAT CAN I DO TODAY to IMPROVE the probability or likelihood that a Service will be perceived as available when needed?**

## The (pre) Works

- You must apply generally agreed Best Practices
  - for making the *individual* items more reliable
  - Examples:
    - Clean your network of unwanted traffic
    - Deploy Storage & IO sensibly, i.e.
      - <http://www.Lotus.com/Performance>
    - Automate the deployment customizations

# Summary of Lotus New-licensing information

- You must get
  - the most updated Q&A PDF document
  - from Lotus
  - and ask
    - your IBM Business Partner
    - or IBM rep
  - what that means to you
  
- This is our best guess to decode the Lotus provided info: -)
  
- On an "incremental (delta) analysis basis"

# Summary of Lotus New-licensing information

Existing Server Offerings	Existing License w/ maint (1st yr) PA Level A - SVP	New Server Offerings License w/ maint (1st yr) PA Level A - SVP	Comments
Domino Mail Server; mail, C&S, 1-4 CPU's	\$894/server	Domino Messaging Server; messaging and calendaring, partitioning; \$894/processor	Move to processor
Domino Application Server; mail, C&S, custom applications; 1-4 CPU's	\$2,308/server	Domino Enterprise Server; applications, messaging, calendaring, partitioning, clustering; \$2,308/processor	Move to processor
Domino Enterprise Server; mail, C&S, custom applications; 5-8 CPU's; partitioning, clustering	\$6,423/server		
Domino Advanced Enterprise Server; mail, C&S, custom applications; 9+ CPU's; partitioning, clustering	\$25,713/server		
Domino Extranet CAL; non employee applications only; unlimited CPU's; partitioning, clustering	\$5,353/server	Domino Utility Server; clustering, partitioning, unlimited user access to applications (no messaging); no CAL requirement; \$11,750/processor	Move to processor
Lotus Communications CEO	\$150/user	Lotus Communication CEO, \$150/user	Unchanged



## Licensing Issues:

- A user is a user is a user (is this a tautology or what :-)
  - A clustered user costs = as a non clustered user (since R4.01)
- Most NEW server licenses are priced by CPU or by User
  - So if in order to support your load you needed "n" CPUs
  - Then the cost of the license per CPU is linear
  - Regardless of how you group the CPUs into Boxes/Servers
- Most NEW server licenses include "clustering"
  - It used to be the case that "Enterprise"
    - was so more expensive
    - was the only one supporting Clustering
  - Now ye old Application Server - renamed "Enterprise"
  - AND the NEW Utility Server: both include clustering.
- Incremental Administratrivia:
  - You probably need ZERO delta dollars/yens/euro/coins of the realm
  - Because your infrastructure will be Licensed for Cluster Already!

# Notes Clustering is Active-Active

- Which means that you ARE using all the power you bought
  - You do not have stand-by-idle resources
  - As the name indicates, you can "load balance" access to all servers
  - You have embedded multi platform fault tolerance.
  - Check what the "i" stands for in the Definition of RAID (inexpensive)
- You can afford to do MORE server CONSOLIDATION
  - *Measure with micrometer, mark with chalk, cut with axe* "method"
  - Define Benchmark, prototype expected performance
  - Calculate Load (somehow), expressed in CPUs for total users
  - Total Numbers of CPUs you need + 10%, plus one or two :-)
  - Divide by how many CPUs per box = Boxes
- Example:
  - With this load and OK response, a one CPU box takes XXXX users
  - We have YYYY users, means  $Z = \text{YYYY} / \text{XXXX} = \text{Number of CPUs}$
  - Say  $Z = 10$ , add 10% plus one = 12 CPUs
  - Say you then buy 3 four-way boxes.....yes this a trial & error "art"

## Portfolio techniques / Sizing heuristics

- There are always 2 practical limits:
  - Lower:
    - at LEAST how many you need to reduce risk
  - Upper:
    - at MOST how many can you manage effectively
  - Tip: Start with 3 or 4, fine tune afterwards
    - but please
      - do NOT start with 2 or 6
      - The limit is no longer six !!!

# Six no longer a limit, but.... don't do "this" !

```
Lotus Domino Server: Srv001.T
> sh server

Lotus Domino r Server (Build H12_02042002 Pre-release 1 for Hindows/32) 23/04/2002 18:55:42

Server name:                Srv001.TheConifers.Con/Srv/TheConifers
Server directory:           c:\Data\Server01
Partition:                   c:\Data\Server01
Elapsed time:                03:53:30
Transactions/minute:        Last minute: 19; Last hour: 19; Peak: 24
Peak # of sessions:         10 at 23/04/2002 16:09:12
Transactions: 3542           Max. concurrent: 20
ThreadPool Threads:         40
Member of cluster:          MegaCluster
Availability Index:         100 (state: AVAILABLE)
Mail Tracking:               Not Enabled
Mail Journaling:             Not Enabled
Shared mail:                 Not Enabled
Number of Mailboxes:        1
Pending mail: 0             Dead mail: 0
Waiting Tasks:               0
Transactional Logging:       Not Enabled
Hosted Organizations:        Not Enabled
Fault Recovery:              Not Enabled
Activity Logging:             Not Enabled
> sh cl

Cluster information:
Cluster name: MegaCluster, Server name: Srv001.TheConifers.Con/Srv/TheConifers
Server cluster probe timeout: 1 minute(s)
Server cluster probe count: 3960
Server cluster default port: *
Server availability threshold: 0
Server availability index: 100 (state: AVAILABLE)
Cluster members (20):
Server: Srv001.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv002.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv003.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv004.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv005.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv006.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv007.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv009.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv008.TheConifers.Con/Srv/TheConifers, availability index: 100
Server: Srv010.TheConifers.Con/Srv/TheConifers, availability index: 100
```



## Class of services: Example

- Say, for the purpose of example, you have "3"
  - "whatevers": OSs, Sites, Servers, Routers, ISPs
  - say you name the 3 elements as A B and C
- With 3 elements you can define the following
  - Classes of Service:
    - Top, simultaneously present in A+B+C
    - Middle, present in either: AB, AC or BC
    - Single, present just in A or B or C
- Homework: Try the combinations for 4 units,
  - $C(4,4) + C(4,3) + C(4,2) + C(4,1)$



## If you have a Cluster of more than TWO:

- You can afford to negotiate with your users "classes" of SLA
  - for example: Cluster of 4 boxes (say a,b,c,d)
  - System Files: (names, etc), deployed in a+b+c+d
  - Optionals: (as-is-as-available. if-available :-)
    - deployed in ONE (a or b or c or D)
  - Std Clustered, deployed in a pair of servers:
    - ab,bc,cd,da,etc (use round robin or striping)
  - Mission Critical, deployed in 3 servers
  - Ultra Mission Critical: deployed as system files, in all four servers
  - BEWARE: if you do not have tight process-control: DONT DO THIS!
    - a crash in an application due to bad logic/data combo will = ...

## High Availability ("Business Approach")

- Something that is "likely" to be available...
- Must be architected and run as such
- "Architected" implies with "HEURISTICS",
  - most of which are "difficult to quantify"
  - It's easier to measure Sq Feet of Grass to Mown
  - than quantifying "Garden Landscaping Work"
- "Run" requires having meaningful WYPIWYG

# The HUMAN Factor: WYPIWYG

- WYPIWYG is actually W.Y.P.I.W.Y.G



- "What You **Print** **Pay** Is What You Get"
  - If you measure the wrong things...
  - you WILL get wrong behaviours and output

## Dilbertian Examples or WYPIWYGs



- IF you Pay people to keep the UPTIME
  - of individual machines (stress on individual)
- They WILL schedule + preventative maint time
  - They will NOT apply patches a.s.a.p./available
  - They will NOT down a service EVEN when at risk
  - 99% of hacked/virused machines were
    - "already well known vulnerabilities"
- It will cost you much MORE money and troubles
  - and you will get LESS value for your money

SLAs are as useful to prevent damage as  
insurance/assurance [ :-) ]

- Make you feel better about evil things  
OUTCOMES
  - but they do NOTHING TO prevent evil things
  - from happening in the first place
- Some "Dilbertian" examples:
  - I will insure my house in order for it
    - NOT to go on fire, when you'd better
      - buy insurance in case of disaster BUT ALSO
      - get a smoke detector (detection)
      - get fire extinguishers (response !)
  - I will ask people to sign NDAs...

## Portfolio Principles

- ***"there is nothing wrong with putting all your eggs in one basket, just watch that basket"*** Henry Ford
  - don't put all your eggs in ***one*** basket cause you can't watch ***it*** close enough
  - don't put all your eggs in ***too many*** baskets cause you can't watch ***them all*** close enough
- If you have/had money to invest...
  - Would you invest everything in the latest fad/dotBomb/whatever OR diversify risk (economy of portfolio analysis)



## Portfolio techniques

- reduce risk by using stuff that will fail eventually BUT with negative or zero correlation
  - Win32 code-streams have a huge in-built-correlation, so do UNIX's/Linux's
  - Lower Correlation between Win32, Linux, etc
  - Lower Correlation between AS400/iSeries / rest
- Use this to weight how you "spread" stuff

# SPOFs = Single Point of Failure

- Definition:
  - A single point of failure is a anything that is not redundant enough and whose failure will cause damage to the availability of a service
- I will NOT repeat here the trivial ones
- Some "hidden SPOFs":
  - check bill of materials for anything that has1
  - mouse/keyboard/Switch ==> IMPLY SAME RACK
  - UPS/ISP/Site:
    - you may have to consider multi site/homed

## The HUMAN Factor: WTPIWTD

- WTPIWTD is actually W.T.P.I.W.T.D.
- "What THEY Pay Is What THEY Demand"
  - Make sure the BizSponsor pays by BILLBACK
    - a class of service with expected resilience
    - a % of your fulfillment platform
    - Never let a user "own" a box that you run
      - easier to say than to do, but try :-)
      -

## Have apps "spread" among servers...

### ■ Now what?

- a) we need to define how we will synchronize
  - Bad News:
    - Scheduled replication not good enough...
    - Some apps must be cluster aware enabled!
  - Good News:
    - NATIVE Event/Queue Driven = CLREPL =
      - (aka Almost Real Time)
    - Most apps will automatically work better
- b) we still need to spread the load/access.

# The beauty of Notes/Domino: Secure Replication

- Deploy to more than one site enabled by
  - Replication of databases
    - scheduled replication
    - event driven replication
    - both
- Tips:
  - do NOT deploy by OS copy nor FTP, use replica
  - Hardcode Cluster OU in ACLs ie.  
    \*/Srv/<whatever>
  - [Names]: Add to prevent pull replication issues

## Cluster Mates: (Mate is an industry UnPIC std term)

### ■ Definition:

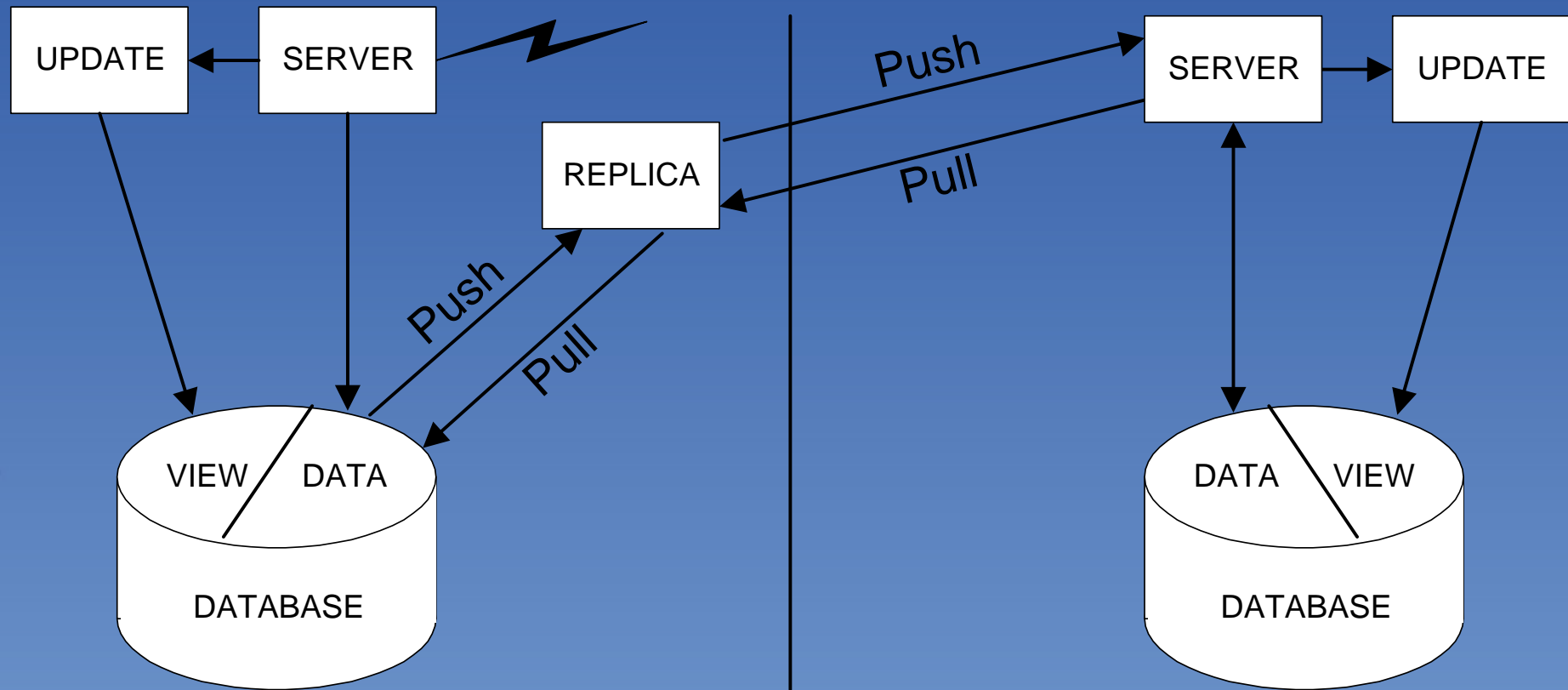
- A cluster of something is composed of mates
  - logically siblings among them (no master)
- Domino Wise, a Cluster Mate can be:
  - Available (normal)
  - Busy ( $\text{Server\_Availability\_Index} < \text{Server\_Availability\_Threshold}$ )
  - Unavailable (or unreachabeable/perceived as such)
  - Restricted (Temp=1 or Perm=2)
  - Invalid (never contacted)



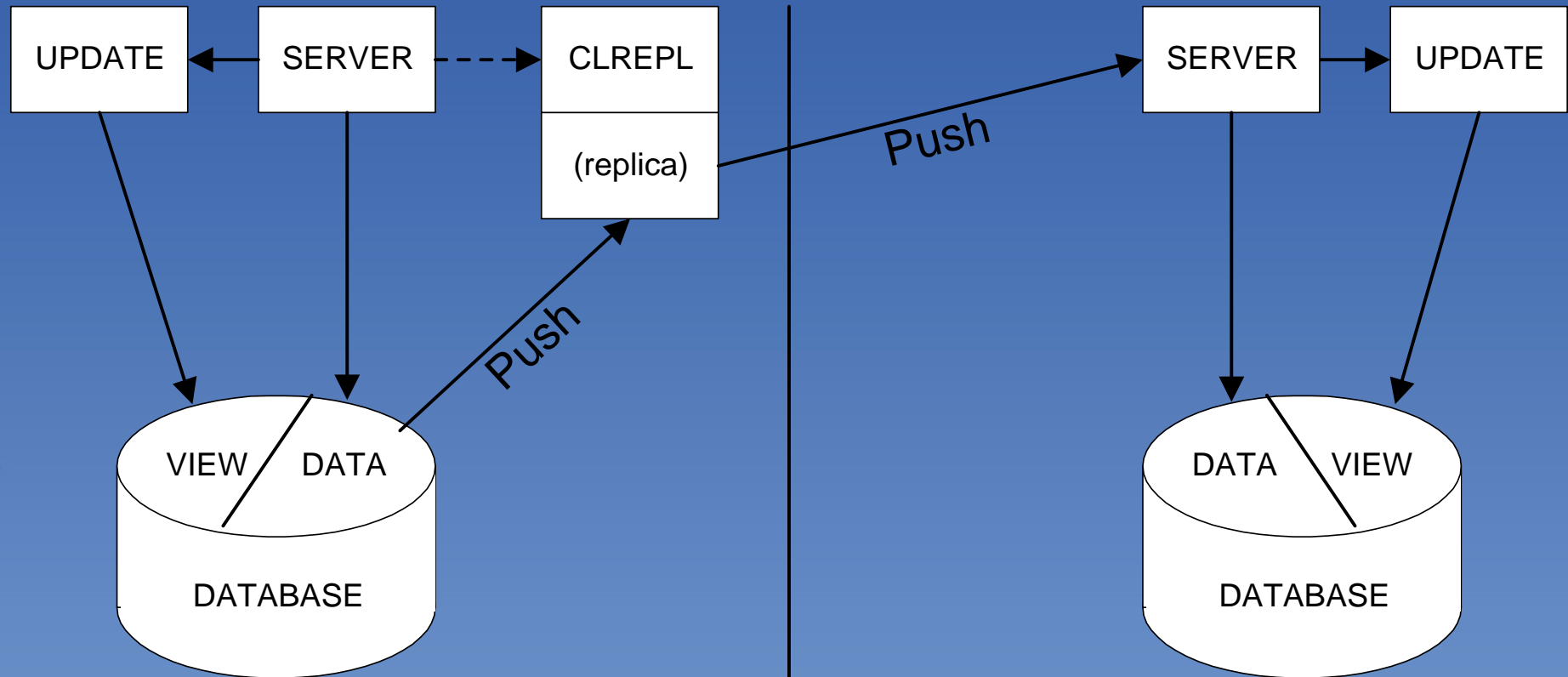
## CIDbDir

- It's a Notes Database, similar to catalogue,
  - Cluster Specific (RepId depends on ClusterName)
- Maintained by a server task of the same name
- Contains info about databases deployed in a cluster
- Is used by Notes/Domino Cluster Aware modules
  - to know where to push what
  - and for "failovers"
- Tip: Beware limit 8000 dbs (sometimes)

# From LKB: How Push-Pull (std) Replica works

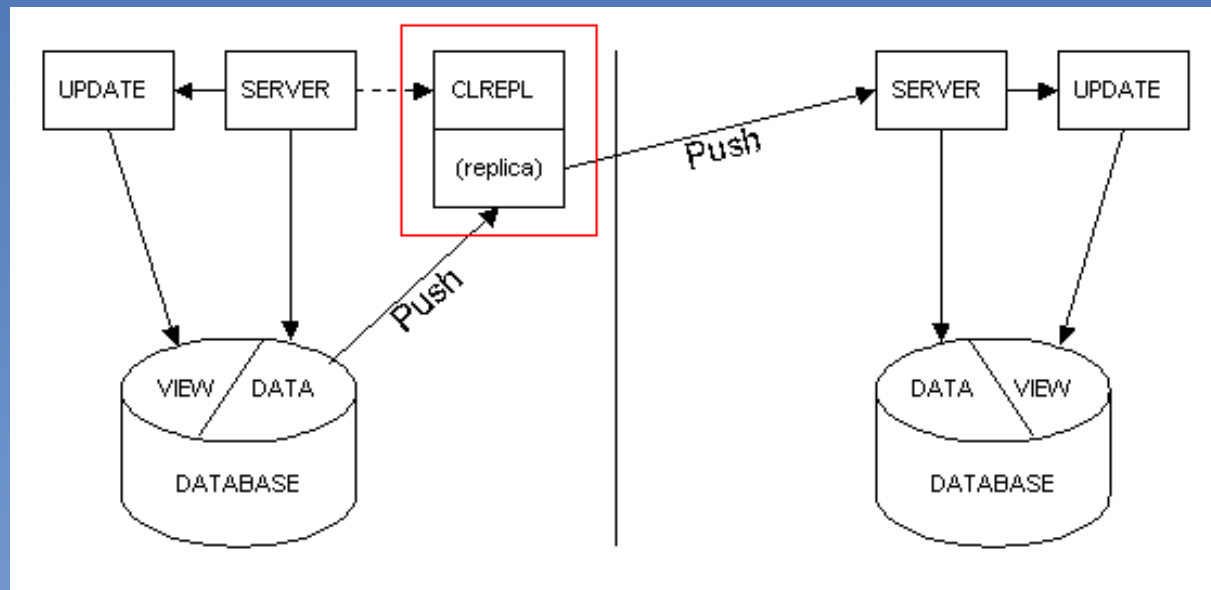


# From LKB: How Push Cluster Replica works !



# How does Cluster Replication work

- Document changes are captured and trigger the cluster Replicator via a message queue
- Cluster Replicator reads message queue and pushes changes to other all other replicas in the cluster regardless of replication settings (aka almost "real time" replication)



# Servertasks involved in Cluster Replication

- **cladmin** Servertask in R5 ( D6: integrated into the server) takes care about administrative things
- **clbdbdir** Servertask takes care that **cluster directory** is up to date
- **clrepl** Servertask pushes changes to other replicas based on information from **cluster directory**
  - logs periodically into replication log (manual: tell clrepl log)
- **replica** Servertask should still be active
-

# Server regularly check state of their Cluster Mates

- API Level call **NSPingServer**
  - gives back a list of cluster mates and the availability

- You can check this information via

> **show cluster**

Cluster Information

Cluster name: nsh-cluster, Server name:  
nsh-dus-02/Srv/NashCom/DE

**Server cluster probe timeout: 1 minute(s)**

Server cluster probe count: 185

Server availability threshold: 0

**Server availability index: 100 (state: AVAILABLE)**

Cluster members (2)...

server: nsh-dus-02/Srv/NashCom/DE, availability index: 100

server: nsh-dus-01/Srv/NashCom/DE, availability: 42

■

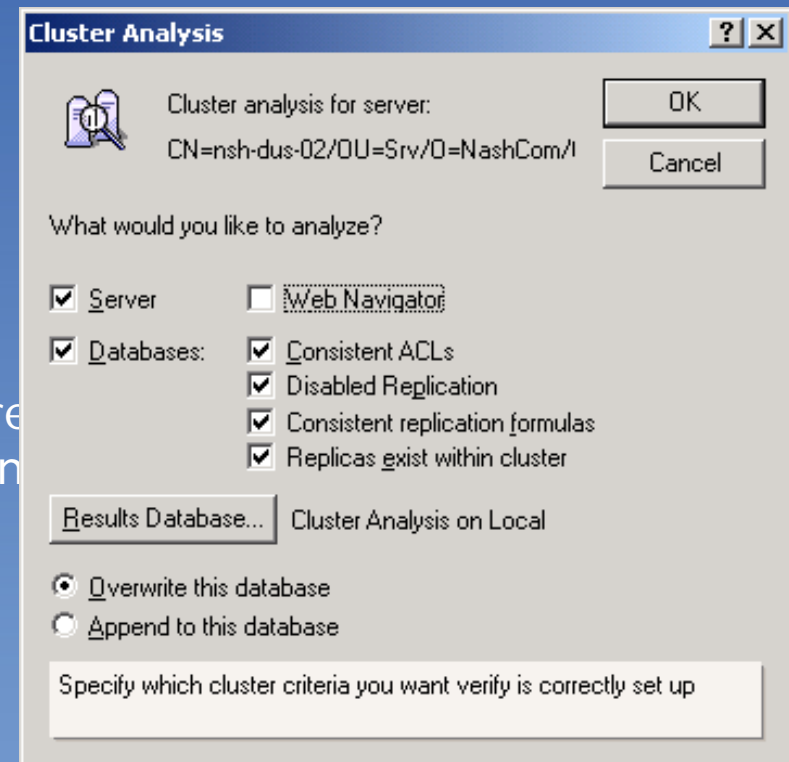


## How does failover work?

- **Cluster.ncf** contains information about cluster members
- Client uses this information to find another cluster mate in case the current server goes down
- Example Cluster.ncf  
Time=27.01.2003 00:06:24 (C1256CBA:007EEDC0)  
NicEMEA  
CN=extranet04uk.lotus.com/OU=Srv/OU=LotusEmea/O=Net  
CN=194.196.39.11/OU=Srv/OU=LotusEmea/O=Net
- Server uses cluster directory to find replica of the database to open by ReplicaID and redirects to the right server

# Run Cluster Analysis regularly

- Cluster Analysis is a great feature to figure out about problems in your cluster
  - It's part of the Admin Client and (Server / Analysis / Cluster ...)
  - Run it to find problems with ACL, Replication, not existing databases, ...
- Tips
  - Run it, print it and sign off all warnings you find
  - Use FT Search to remove multiple occurrences of similar or already fixed problems until DB is empty
  - Run Analysis again to see you addressed all problems



# Cluster Replicator Performance & Statistics

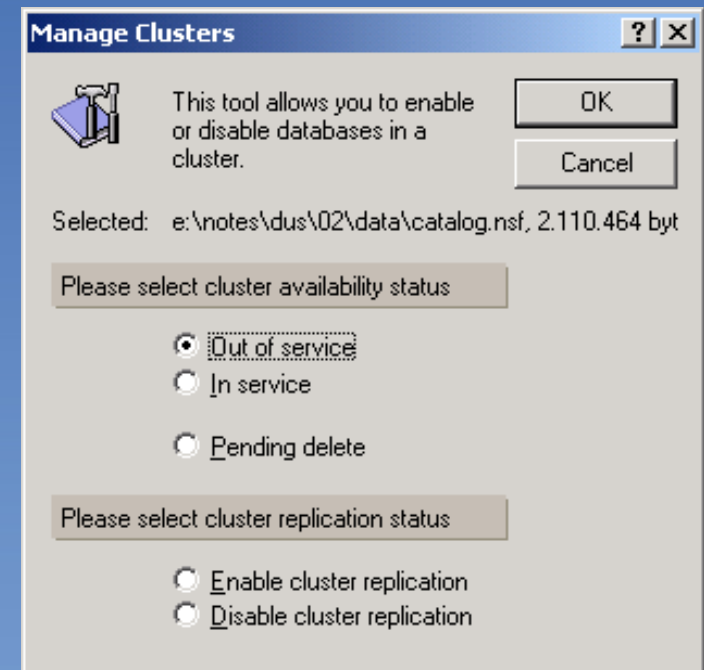
- General Rule: number of clrepl = cluster members -1
  - R5: `servertasks=events4, repl, router, clrepl, clrepl, clrepl, ...`
  - D6: `Cluster_Replicators=n`
- Check if clustering works properly via
- **Show Stat Replica.Cluster.\***
  - `Replica.Cluster.WorkQueueDepth` should be less than 10
  - `Replica.Cluster.RetryWaiting` should be less than 5
  - `Replica.Cluster.Failed` should be zero if possible
  - `Replica.Cluster.SecondsOnQueue.Avg = 10 -> should be << 15!`
- **Show Stat Server.Cluster.\***
  - `Server.Cluster.OpenRedirects.xxx.Unsuccessful = 0`
  - check for unsuccessful redirects!

# Cluster Replication & Database Quotas

- There are issues with Database Quotas before R5.0.10
- Good news:
  - New option in R5.0.10 **CLREPL\_OVERRIDE\_QUOTAS=1**
  - Domino 6 overrides quotas by default
  - you get the old behavior with **Clrepl\_Obeys\_Quotas=1** (DDT)
- Bad news:
  - If you already have this problem you need to delete replication history and CutOff Date to resolve existing replication problems
  - Lotus Script can clear the replication history
    - **Set rep = db.ReplicationInfo , Call rep.ClearHistory() , Call rep.Save()**
    - But not remove the CutOffDate (in most cases not needed)

# Maintenance of Servers or single databases

- Restricting a server
  - Notes.ini **Server\_Restricted =1** or 2
- Take single databases out of service
  - via Admin Client Files/Database/Cluster ...
- Client will automatically failover to another replica of the requested DB (cluster.ncf, clbdbdir.nsf)



# Troubleshooting Settings

- Only use those settings if you really need to
- They will log a LOT of information
- It really helps to understand how replication works ;-)
  
- Log Options
  - RTR\_Logging=1
  - LOG\_REPLICATION=4
  
- Debug Options
  - DEBUG\_REPL=2
  - DEBUG\_REPL\_ALL=1



# Best Practices for Cluster Replication

- Ensure you have full manager access for **LocalDomainServers** as a Server group or better **\*/Srv/Org** as Manager of type Server in all ACLs
- Make sure all applications provide roles to give access to documents with reader fields
- Give Servers all rights and roles to "see" all documents
- Don't use replication formulas for clustered databases
- Have a scheduled replication in case some events in the clrep-queue get lost or the server is down...
- Add startup replication documents to ensure databases are up to date after server restart
- Schedule replication to the Name of the cluster instead of single server names (load balancing & failover)

# Developing Cluster enabled Applications

## Some general rules & tips

- Never use NoteID always use UniqueID (UNID)
- Open all databases with failover
- Use "Unprocessed Documents" only for performance reasons
  - use a field in the document to check the status instead!
  - you never know if an agent might need to run on a different server or the agent-design changes...
- Don't use hardcoded server or database names if possible
- Don't assume to find databases in the same directory on the same server
- Have a reasonable "on error handling" for catching errors and resume
  - You cannot always recover automatically if a server goes down
- Scheduling agents for failover is extremely difficult - you might have to make some trade-offs ...

## "Automagic Clustering Experience"

- The art of doing something "automagically" to improve the perceived performance of the cluster, usually by making intelligent usage of idle resources.
- Proactive:
  - Load Spreading
- Reactive
  - Performning Load "re-"Balancing by trying to fail over to less busy clustermates

# Failover

## ■ Definition:

- Server Initiated
  - due to reactive Load Balance or failures
- Client Initiated
  - server is dead *or perceived* as dead
  - requires client to know how to connect to cluster mates without server assistance!
  - Tips: insert the address in name:
    - CN=<FullyQualifiedDomainName>/Whatever
    - CN=194.196.39.11/Srv/LotusEmea/Net`

# Cluster Aware "1352" Notes Clients. a.k.a. Cluster-READY clients

- Definition:
  - A Notes Client is said to be cluster-aware when it will perform custom logic to transparently and automatically fail-over from one server to another, upon server directive or LACK of reply
- QUIZ:
  - what % of Notes Clients are CLUSTER Aware?
  - hint: what was the first version of Cluster Aware Notes client?
- If I told you Notes 4.01 was the first one...

Cluster.NCF (max 2x40 entries, LKB 185700)

--> Cluster\_Name\_Cache\_Size=nnn (notes.ini)

- Time=22/12/2001 14:26:46 (80256B2A:004F5AD8)
  - Cluster/NotesWeb
    - CN=Notes2/O=Notesweb
    - CN=Notes1/O=Notesweb
- Time=03/01/2002 16:18:24 (80256B36:0059935B)
  - TheConifers.com
    - CN=dotNSF.TheConifers.com/O=TheConifers
    - CN=Linux.TheConifers.com/O=TheConifers
    - CN=WebSphere.TheConifers.com/O=TheConifers
    - CN=Win2k.TheConifers.com/O=TheConifers
    - CN=www.TheConifers.com/O=TheConifers




## Native Notes Access:

- Summary of what we did for PIN for Lotus EMEA since 1995
- Self - Registration
  - Signed documents compiled anonymously
  - Filled by formulas that find relevant info at users
- WorkFlow
  - to validate
    - Entitlements
    - Naming Conventions
  - to CrossCertify
    - sometimes a low tech-solution does the job faster and better.
- Why this is still relevant:
  - because it has been working for 8 years
  - because it's reasonably secure and easy to run with few admins
  - because it saved Lotus itself several million U\$S !!!

# Server Configured in 1996 (still up!)

**What Clustering/Advanced Services/NPN means to you...**


NPNs, the Notes Public Networks , use a special version of Notes, also known as CARRIER GRADE NOTES, that allows them to provide some extra functionality, particularly in balance loading, failover recovery and billing.

**We also use it. Thus...**

**You may see in your log messages similar to this one,**

```
23/04/96 06:20:49      Failover on replica ID (XXXXXXXX:YYYYYYYY)
                        from server 194.196.39.10/Srv/LotusEmea/Net
                        to 194.196.39.11/Srv/LotusEmea/Net
23/04/96 06:20:49      Starting replication with server 194.196.39.11/Srv/LotusEmea/Net
```

**or in the replicator page**

	Today 07:23	with 194.196.39.11/Srv/LotusEmea/Net (194.196.39.10/Srv/LotusEmea/Net unavailable) 0 Received, 0 Sent
-------------------------------------------------------------------------------------	----------------	----------------------------------------------------------------------------------------------------------

BP 2001 Forum

## Cluster Aware Web Client:

- Definition:
  - A Browser is said to PERFORM cluster-aware when it CAN BE TOLD to perform custom logic to transparently and automatically fail-over from one server to another, upon server directive or LACK of reply
- Quiz:
  - Does Microsoft Explorer Support this ?
    - Hints: "301" and "multihomed" and "DNS"

# "Spraying Sessions"

## ■ Definition:

- A technique to scatter/assign
- traffic/load/sessions/whatever
- to one out of a set of possible "mates"
  - Simple: Round Robin or just dup A
    - bad for Load Balancing (Sticky/cache/etc)
    - but OK for client failover! See Ms Kb Qs
    - 154442 +182644/168321/140859/139334
  - Content/Load/Origin/Net/Latency Aware
    - more complex but powerful: ie: Olympics

## Session Spraying... and failover

- Session-Spraying is a technique that is better described and understood with a methaphor:
- Dialogue - At a Restaurant:
  - -Customer:
    - Can I have a table for 2, please
  - -Restaurant "Rep":
    - Here is your table, and this is <x> your waiter who will take care of you
  - Customer interacts with <x> SAME waiter
- Session is said - in this case - to be "Sticky"
  - as opposed to pure stateless
  - as defined in the original http protocols

## Session Spraying (cont'd)

- Customer continues to talk to "waiter/mate"
  - until
    - "mate" is no longer available or equiv'.
    - or "mate" redirects client to other mate
    - or customer is fed-up of bad service and initiates "Client Based Failover"
    - i.e. call restaurant/rep/maitre again to escalate/complain and asks to be served by another different "mate" waiter



## How to distribute "load" among ClusterMates

- First thing you need to understand is where you are regarding the overall topology
- Interesting questions
  - Who provides DNS ?
    - and how is that cached ?
  - How many Subnets you have ?
  - Are you using Proxies
    - (stay tuned, more slides coming...)

# Proxies can be a tricky stuff

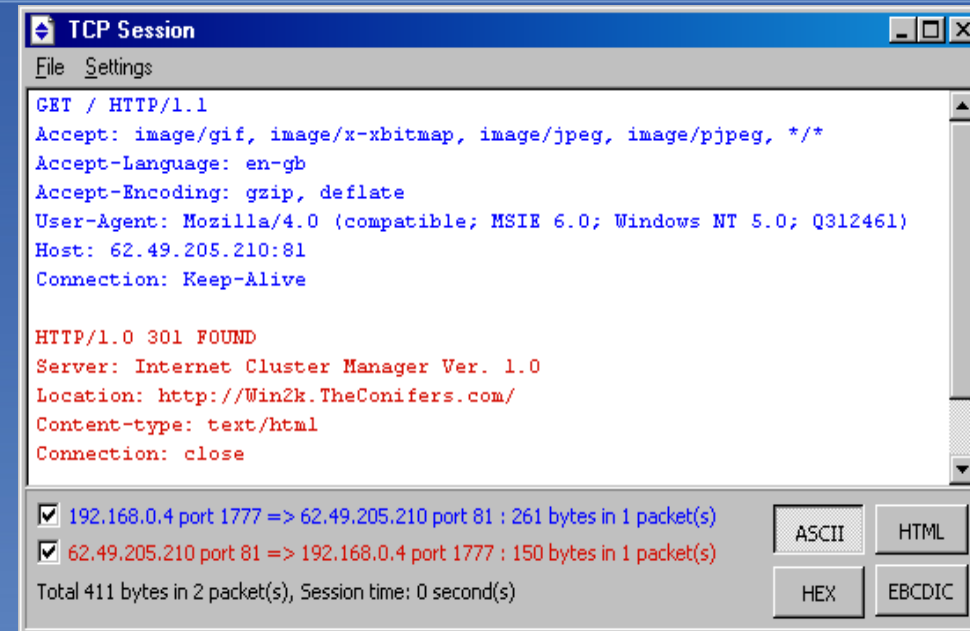
- Proxies can be:
  - Forward Proxies
    - with or without cache
    - with or without security plug-ins
    - transparent or declared
  - Reverse Proxies
    - by definition you do NOT declare them
    - browser THINKS he's talking TO the back end servers
    - "back end" is relative, because it could still be "outside"
    - can be with or without security plug in
    - can be with or without caching
    - can be with or without load balancing
    - can be with or without "junctions" (more later!)
    - can be a pretty complicated thing to set up & debug!

## ICM = Internet Cluster Manager

- It does SOME intelligent
  - http/https spraying
  - it works via "301 Redirect"
  - useful for session spraying
  - many users will find this is OK for them

## Example of ICM Session Spraying

- GET / HTTP/1.1
  - Accept: \*/\*
  - User-Agent: Mozilla/4.0
  - Host: 62.49.205.210:81
  - Connection: Keep-Alive
- HTTP/1.0 301 FOUND
  - Server: Internet Cluster Manager Ver. 1.0
  - Location: <http://Win2k.TheConifers.com/>
- Content-type: text/html
- Connection: close



```
TCP Session
File Settings
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Host: 62.49.205.210:81
Connection: Keep-Alive

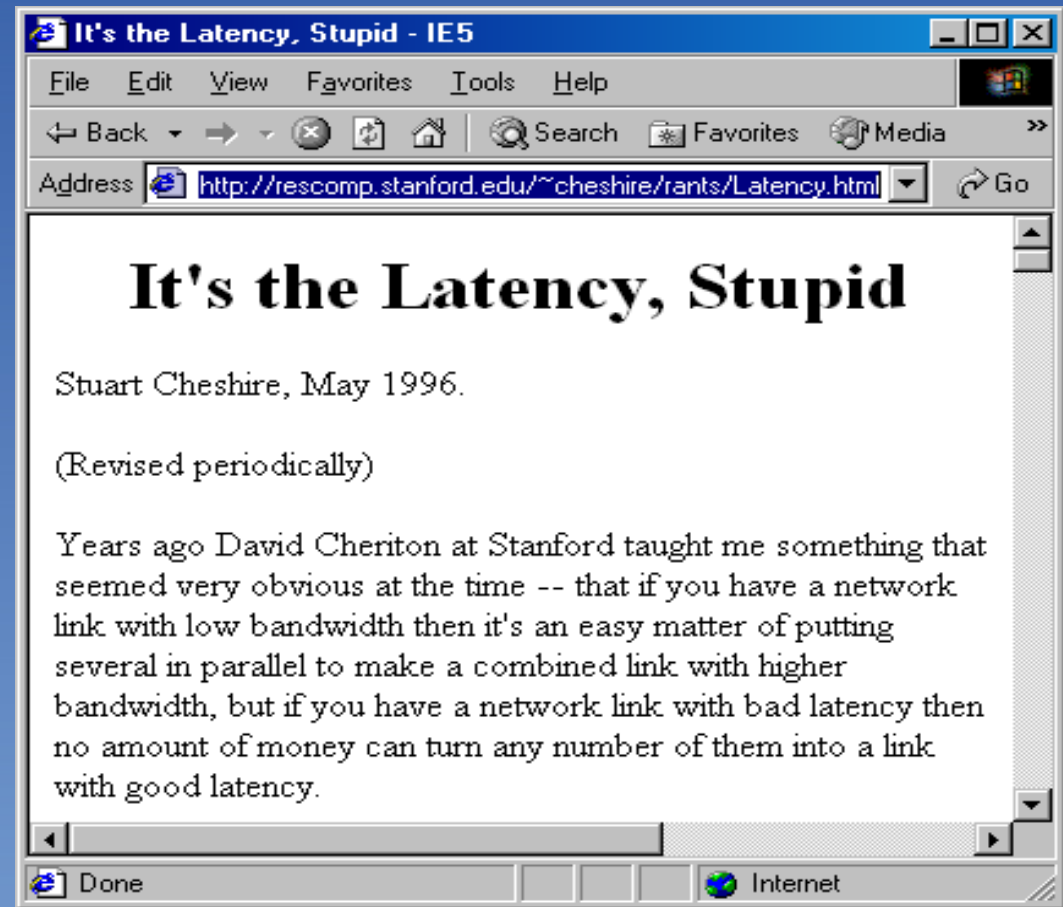
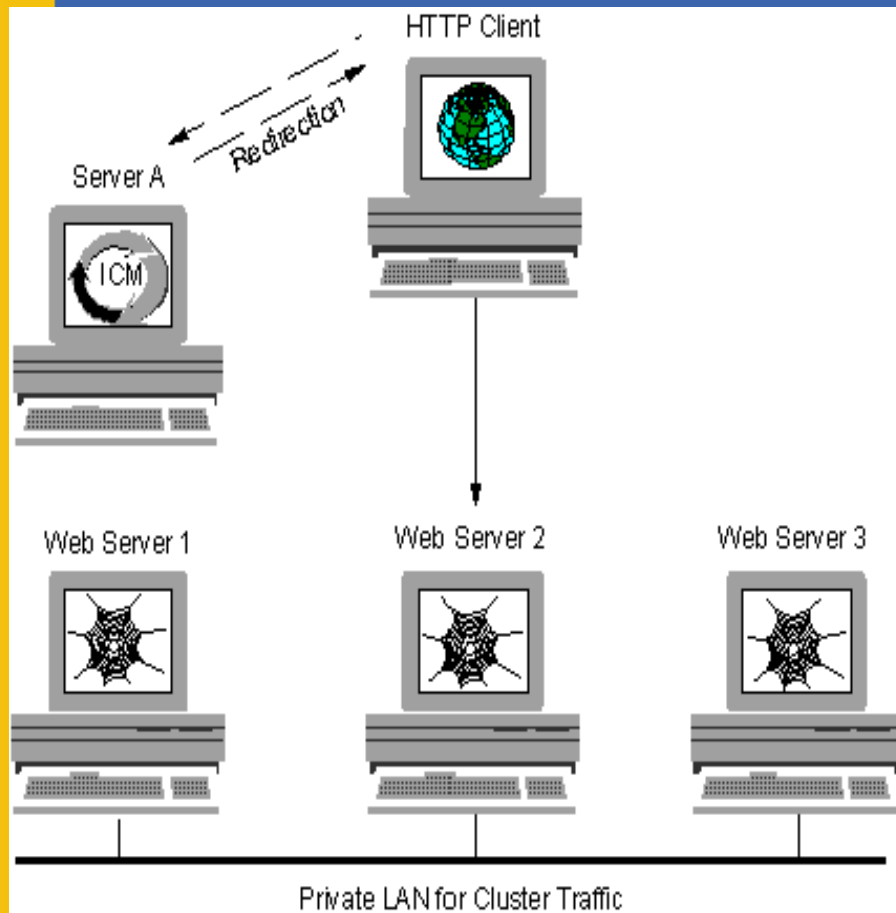
HTTP/1.0 301 FOUND
Server: Internet Cluster Manager Ver. 1.0
Location: http://Win2k.TheConifers.com/
Content-type: text/html
Connection: close

 192.168.0.4 port 1777 => 62.49.205.210 port 81 : 261 bytes in 1 packet(s)
 62.49.205.210 port 81 => 192.168.0.4 port 1777 : 150 bytes in 1 packet(s)
Total 411 bytes in 2 packet(s), Session time: 0 second(s)
```

## If you spray with just ICM

- Tips:
  - Spray "write" sessions = STICKY
    - but you can combine it with...
  - Spray "fulfill=read" via non sticky
  - Whatever you do, in your apps:
    - in LS: OpenWithFailover when possible
    - ALWAYS use relative paths in URLs
      - a relative path begins with a dot, not "/"
      - if you can't, use /\_\_replicaid.nsf

# Latency & Redirects: LKB 170830





## In order not to make ICM a SPOF

- Configure at least TWO of them
  - you can run them IN the ClusterMates
    - using a different IP Address
- Round-Robin them via DNS (multiple A)
- Nota Bene:
  - DDT n "CNAMES" as said in LKB178867
  - DO n "A"s because of MsKb Q154442

# You must understand what you WANT to happen at client based failover

- BECAUSE this will impact on the amount of cluster aware design your application must have
- You must treat the following cases:
  - App was reading (no problem)
  - the transaction is still in the CIRepl queue...
  - App was writing: either you have or you don't have the last transaction performed against the old mate; when failover happened and you connect to new-mate, since old-mate can be kaput or just unavailable to the user, to the new mate or both... or.. it's a complex thing

# You MUST let the user know how you are handling the failover

- You can NOT catch "client initiated" failovers
  - when site unavailable, or unreachable
  - never exclude routing tables and DNSs
- You MAY have a FRAMESET where the user only sees the address of the main "cluster" in his/her browser and sessions happen within FRAME transactions are redirected within Frames, and...
- You ALWAYS have on screen instructions...

# What about other protocols ?

## Sametime, QP, etc ? LKB 189266

- There are many good reasons for complementing Domino with other best of breed IBM Networking applications (some "just branded" Websphere)
  - You will find some hints in KnowledgeBase
  - You will find some great IBM RedBooks
  - You will find White Papers and other stuff
  - You will find a lot of info at the IBM site
  - If Domino alone will not do it, you can bet
    - Lotus will officially support the IBM solution
    - i.e. Quickplace, Sametime, etc

# How to complement this with some other cool IBM Stuff

- ND a.k.a. Network Dispatcher
  - The most powerful tool available for the job
  - You MUST consider this stuff !
    - it does very smart Level 3/4 LSB and more
    - extremely customizable (java advisors)
- Included in IBM Websphere Edge Server
- Also bundled with Tivoli Access Manager for e-Biz
- formerly known as IBM WS Performance Pack
- formerly known as IBM SecureWay Net Dispatcher
- formerly available standalone as IBM Net Disp.





## Technologies behind Net based LSB:

- Much more powerful and complex stuff
- Approach is Java based, multiplatform code
- Extremely efficient, runs in dedicated tiny hw
- Intelligently "massaging" network packets
- Based on TCPIP, per protocol "cluster" of servers
- Each Protocol has custom "Advisors"
- You define the loads/heuristics and weights
- You can define stickyness or not
- It works by DSR = DIRECT SERVER RETURN
- When latency counts, much more efficient.

## DSR - you need to know some prereq's

- Efficient way of implementing fulfillment of LSB
- Each Cluster has a "shared" Cluster Address
- The Cluster Manager "binds" the Cluster Address as an alias of its NFA = Non Forwarding Address
- Each ClusterMate has LoopBack Driver configured
- and ClusterAddress BOUND as ALIAS to the lookback driver 127.0.0.1
- All machines accept traffic FOR cluster address
- BIG TIP: You will have to fine tune static routes anyhow, learn ROUTE PRINT/ADD/Delete

## DSR - you need to know a little about how/why it works

- ND Cluster Manager receives traffic for the cluster address, via the "physical card" adapter alias
- ND figures out to which clustermate to send it
  - this is not a one liner, it's **EXTREMELY** complex
  - You MUST architect the affinities properly
- TCP Headers are conveniently hacked or "massaged" and re-sent over the (back) wire...
- with the MAC address of a selected clusterMate to that clusterMate but with the IP address STILL pointing to the cluster address

## DSR - At the ClusterMate (simplified) IN

- The Cluster Mates sees traffic in TCPIP "Funnel"
- for ClusterAddress WHICH IS ON THE LOOPBACK
- but the traffic is received via the NETWORK CARD
- The masagged traffic appears to have been re-routed to it
- The masagged traffic "fools" the tcpip stack
- It just works! (grossly over simplified !)

## DSR - At the ClusterMate (simpl'd) OUT

- The ClusterMate dilligently replies
- DIRECTLY TO THE USER
- The user receives a DIRECT reply from "a" ClusterMate that has a different MAC address than the ND Cluster Manager, but from the correct IP, as if the packet had been re-routed to the user
- Who cares, it works....

## What can you cluster with Net SLB ?

- You can cluster anything you are "listening to"
- You must understand `netstat -an | find "0.0.0.0"`
- If you bind addresses you will listen just that
- Beware of multiple domino tcpip ports/addresses, IF you use them (please DOCUMENT WHY) then list FIRST the loopback address in the TCPIP= List
- If you do this, it will work as a ClusterMate but NOT as a standalone server
- BECAUSE you are binding your listen
  - JUST to <ClusterAddress>:<Protocol>
  - instead of to all addresses \*: <Protocol>



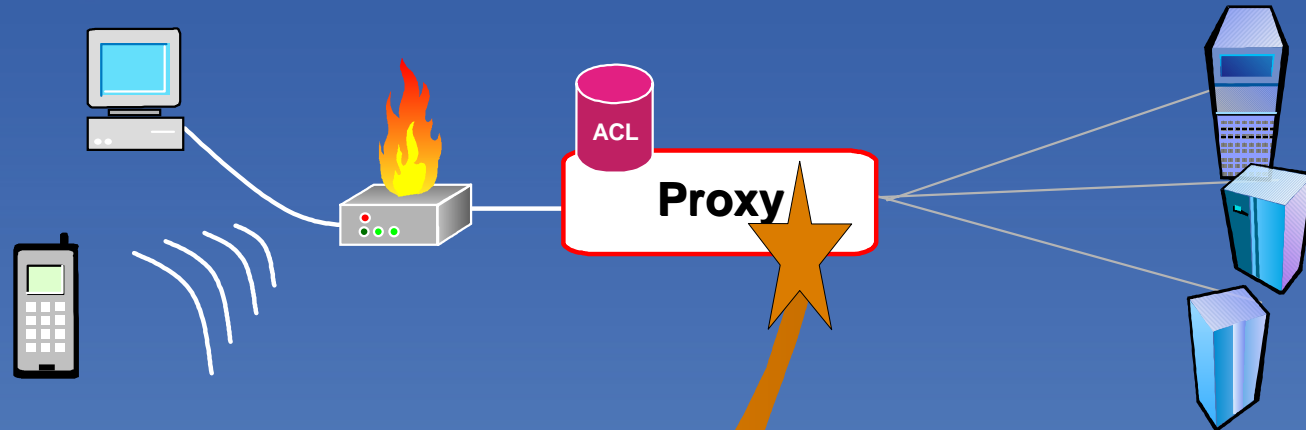
# If this seems complex, in order not to make ND a SPOF...

- You can and should configure
- a pair of them in High Availability Mode
  - with heartbeat + the works
- The HW is minimal
- The SW is (not cheap)
  - but VERY good value for money

## How to debug/test this stuff

- Ping is USELESS, don't even bother...
- You need a protocol analyzer/consultant
- You will NOT succeed to do this with a proxy
- You MUST test all possible failures
  - just unplug cables one by one
  - or tell tasks to quit
  - and dump the failover/dialogues
- You must debug BEFORE enabling firewalls
- You must test again after the firewall is up

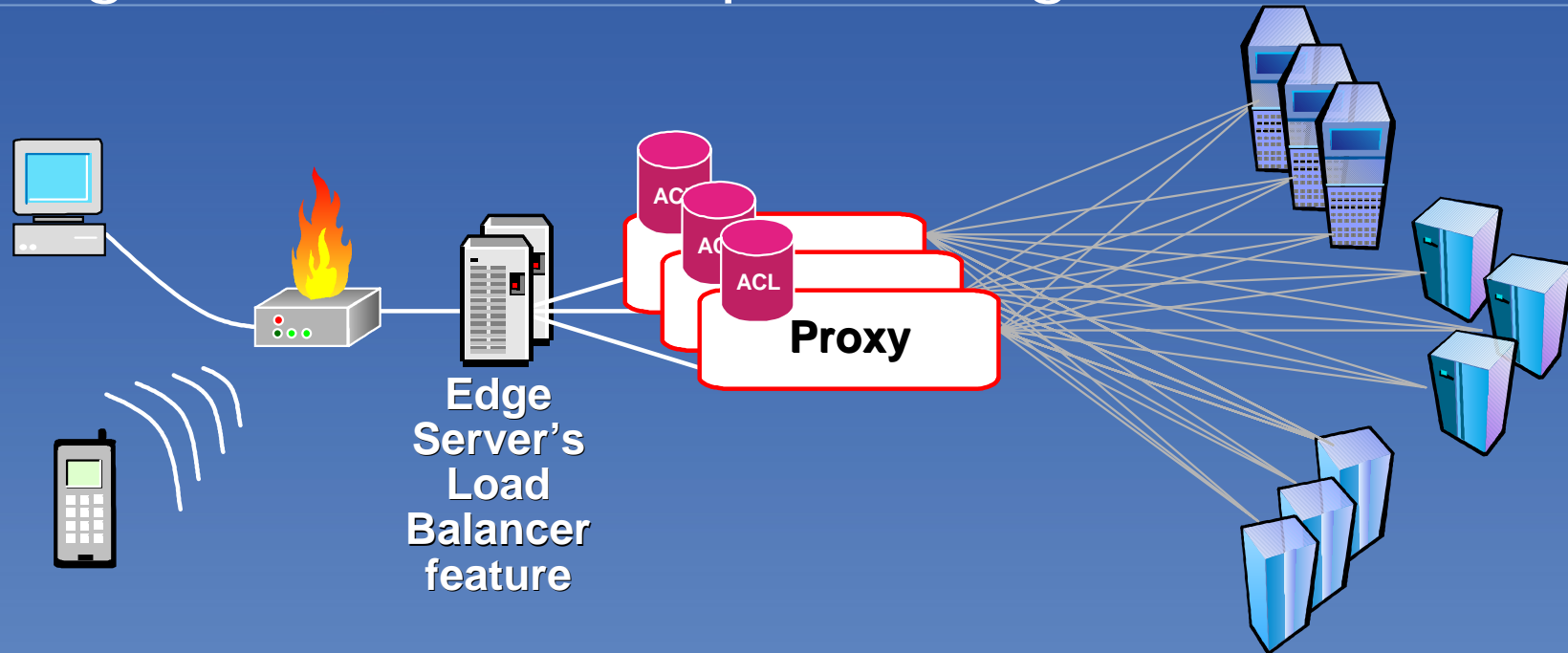
# Integration with Reverse Proxies



*Proxy can be WebSEAL or WebSphere Edge Server Caching Proxy configured to use the AM Plug-In for Edge Server*

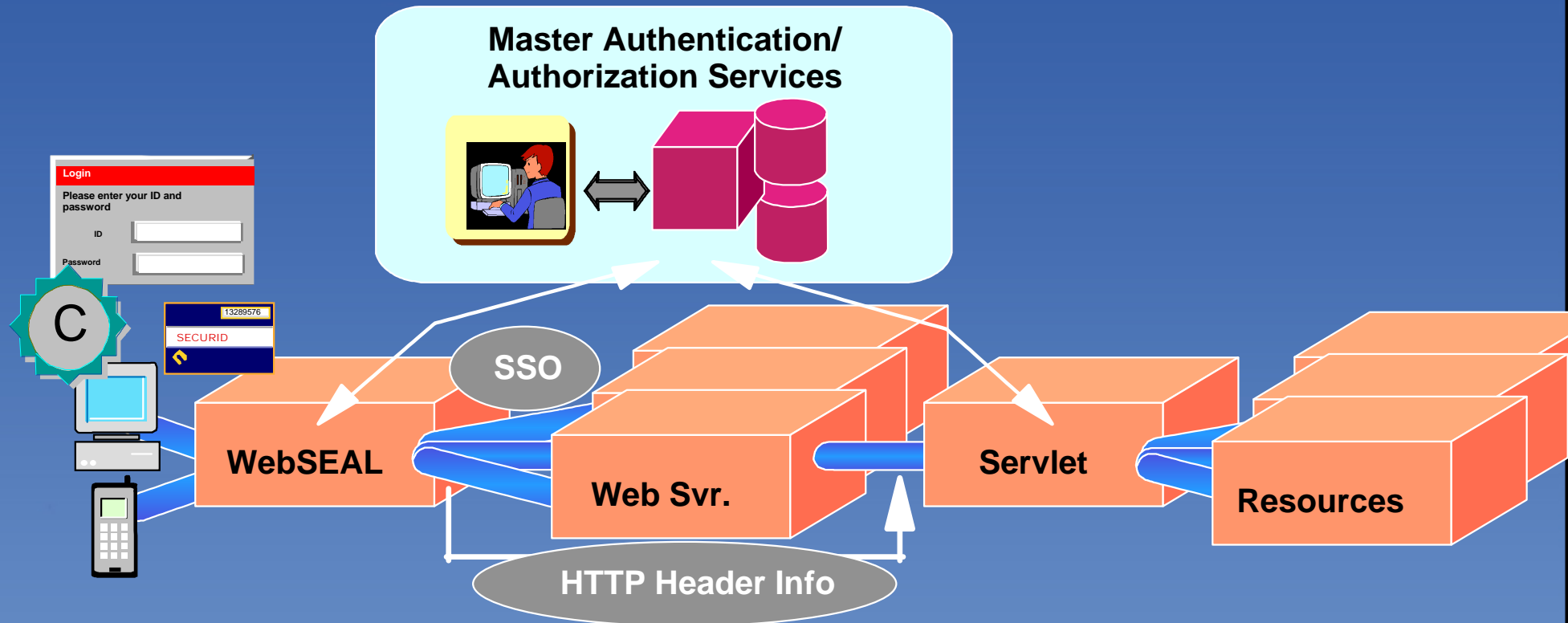
- **Caching Proxy features:** Caching, Content-based routing, virtual hosting, forward/reverse proxy, hardware crypto acceleration
- **Security:** Edge Server Caching Proxy works with Access Manager services
- **URL mapping to back-end servers**
- **Virtual hosting:** Associates multiple domain names with single Web server
  - Multiple certificates on the same Caching Proxy machine

# Integration with WebSphere Edge Server



- WebSEAL or WebSphere Edge Server Caching Proxy works with WebSphere Edge Server's Load Balancer feature
- WebSEAL can in turn balance the load across target Web application servers

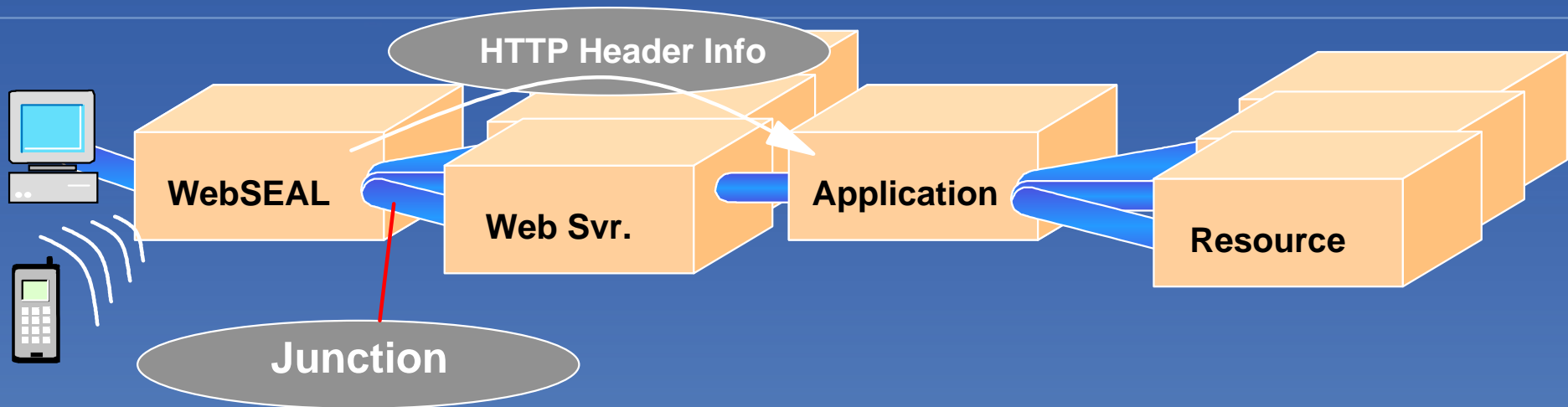
# Access Manager Operational Concepts



## ➤ Applications

- WebSEAL (Robust Authentication/ Credential Support, Web/URL SSO, High Availability/Scalability)
- Java application (EJBs/servlets use 100% Java 2 / JAAS security calls)
- C, C++ application (Using the aznAPI from The Open Group)

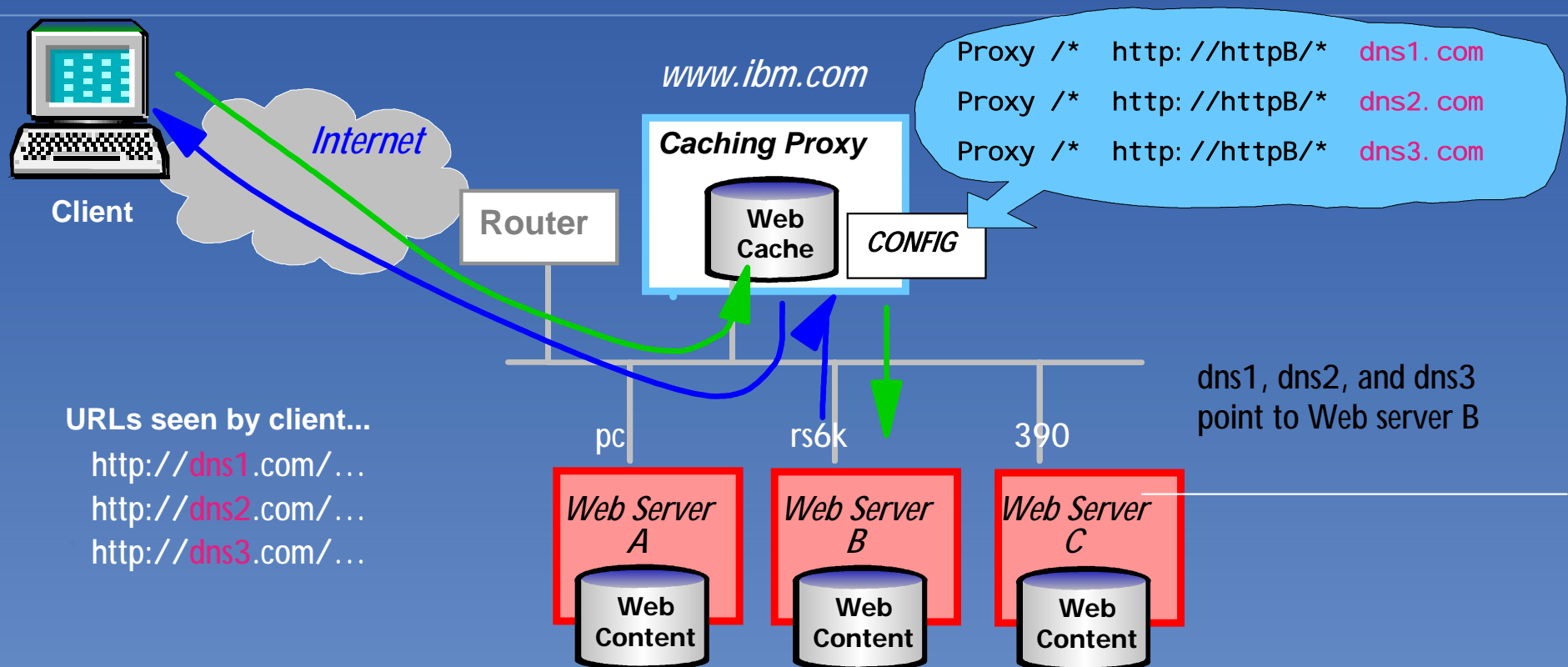
# Junctions Specify Info → Application



- Determines what gets sent to the back-end application
  - Nothing
  - Credentials from the Lock Box
  - User & group information (iv\_user, iv\_groups)
  - EPAC (“Dossier” – iv\_creds)
  - LTPA token
  - Supplemental user information (e.g. credit limit, social security number, e-mail address – tag\_value)
  - Entitlements information, for building a custom personalization service (PD\_PORTAL)

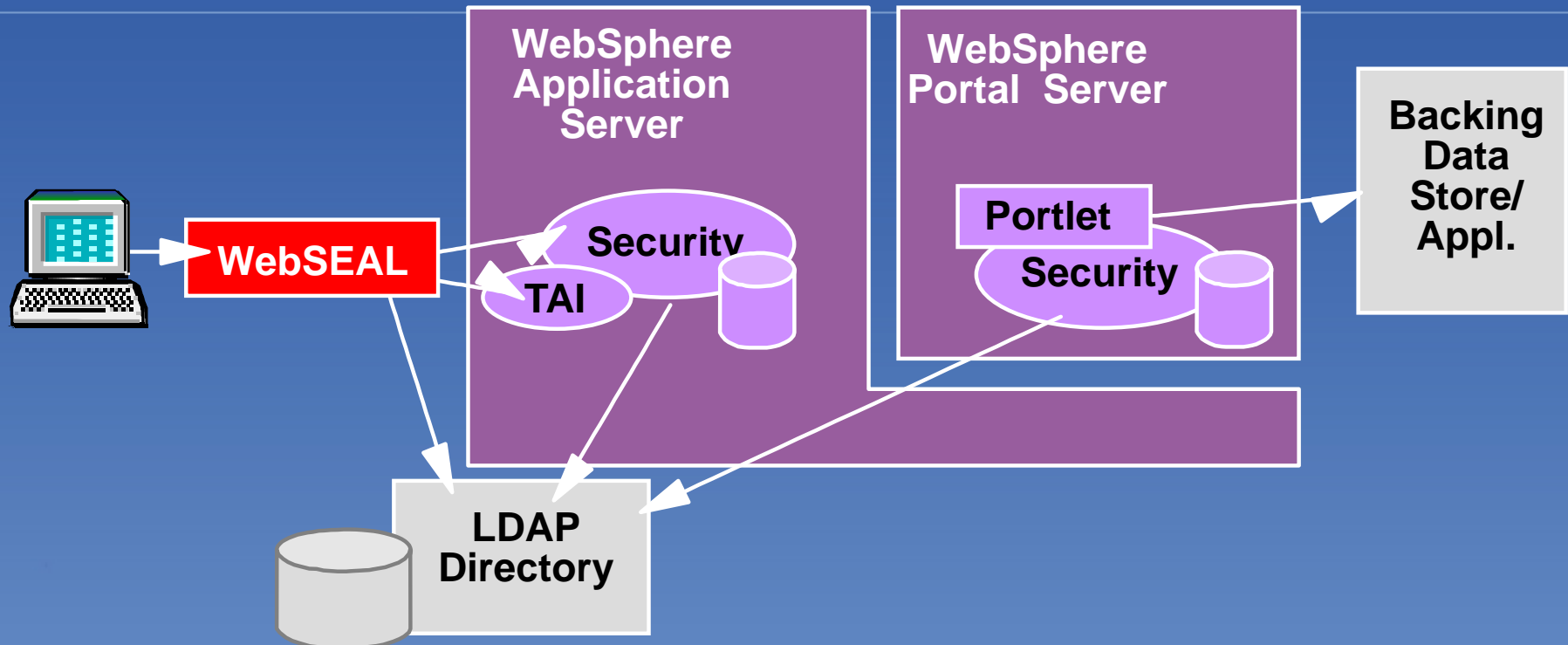


# Integration with WebSphere Edge Server



- **Caching Proxy features:** Caching, Content-based routing, virtual hosting (shown above), forward/reverse proxy, hardware crypto acceleration
- **Security:** Edge Server Caching Proxy works with Access Manager services
- **URL mapping to back-end servers**
- **Virtual hosting:** Associates multiple domain names with single Web server
  - Multiple certificates on the same Caching Proxy machine

# WebSphere Portal Server

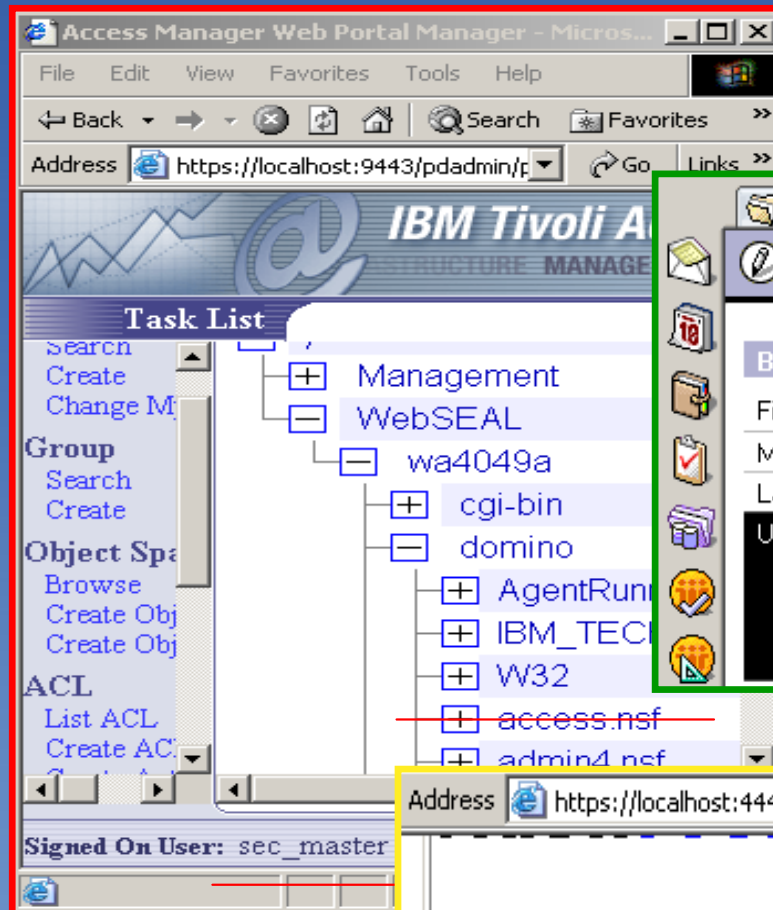


- Leverages Access Manager/WebSphere integration
  - Sharing user info in LDAP
  - Web SSO (via LTPA or Trust Association Interceptor)  
Browser ↔ WebSEAL ↔ WAS ↔ Portlet ↔ Content Server
- Direction (1H02)
  - Access control of portlets, pages and portal resources
  - Secure vault SSO as a portlet service

## dotNSF's TAI for Domino Web SSO

- dotNSF's Trust Authentication Interceptor for Domino
  - Effectively performs the same role as TAI for Websphere but for Domino mapping the web user credentials to Domino security
  - Reads Contents of iv-user and matches the value with a valid Domino username, alias, shortname, etc.
  - Translates (maps) the iv-user contents and format into a fully canonicalised Lotus Domino "fullname"
  - Authenticates the Web user to Domino using the Domino username, which grants the authenticated user all of the privileges associated with the Domino username including group membership, roles all the way down including to reader and author field access

## Example of Custom code: dotNSF TAI for Domino

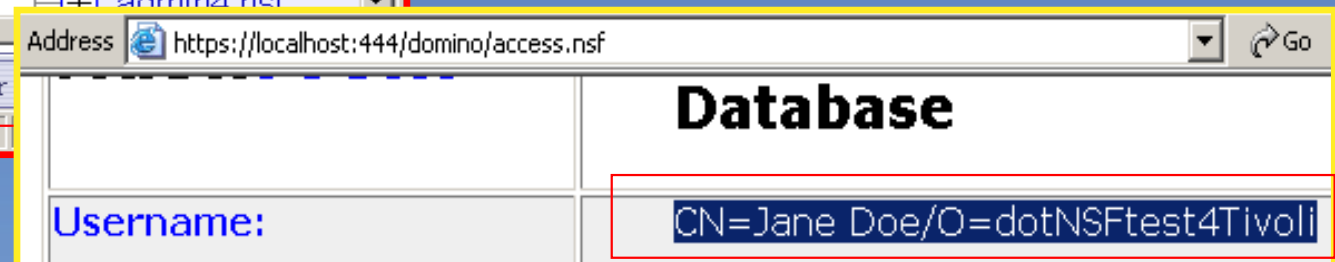


The user of this browser (left) has supplied the sec\_master username & requests an nsf



TAI for Domino matches "sec\_master" with the Jane Doe Notes username

Once authenticated Domino resources accessed using the Notes username



## Example of integration "card" to @Username

```
[25/Oct/2002:16:26:04-0100] The proxy cache is ready
[25/10/2002 16:26:16 1596]
[25/10/2002 16:26:16 1596] — Accepted a secure connection —
[25/10/2002 16:26:16 1596] Entering PreExit Plugin: WTESeal_PreExit()
[25/10/2002 16:26:16 1596] User from 10.1.1.160 submitted request: GET /mail/m12084/mail.nsf/?opendatabase&ui=webmail
[25/10/2002 16:26:16 1596] Looking up domain name: 10.1.1.248:443 -> Itlvm911sb.lvm.de:443
[25/10/2002 16:26:16 1596] Login method for this request is certificate
[25/10/2002 16:26:16 1596] User submitted a client certificate for authentication
[25/10/2002 16:26:16 1596] User's certificate DN: CN=m526008,OU=lvmuser,O=LVM,C=DE
[25/10/2002 16:26:16 1596] Looking up user's certificate distinguished name in LDAP...
[25/10/2002 16:26:16 1596] Found distinguished name for certificate user 'mfjchtest' in LDAP
[25/10/2002 16:26:16 1596] Successfully mapped certificate user to LDAP user 'cn=Marco Foellmer,o=dotNSFtest4Tivoli,c=de'
[25/10/2002 16:26:16 1596] Exiting PreExit Plugin: WTESeal_PreExit()
[25/10/2002 16:26:16 1596]
[25/10/2002 16:26:16 1596] Entering Authorization Plugin: WTESeal_Authorize()
[25/10/2002 16:26:16 1596]
HTTP Headers:
Accept: */*
Accept-Language: en
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705)
Host: 10.1.1.248
Connection: Keep-Alive

[25/10/2002 16:26:16 1596] Creating LDAP identity for user 'mfjchtest'
[25/10/2002 16:26:16 1596] Loading credentials to authorize user 'mfjchtest'
[25/10/2002 16:26:17 1596] Checking operation GET on object /mail/m12084/mail.nsf/?opendatabase&ui=webmail
[25/10/2002 16:26:17 1596] Checking access (x) on ACL string /ESproxy/reverse/Itlvm911sb.lvm.de:443/mail/m12084/mail.nsf
[25/10/2002 16:26:17 1596] Permission was granted to access object
[25/10/2002 16:26:17 1596] User 'mfjchtest' was successfully authorized (return code = 200)
[25/10/2002 16:26:17 1596] Submitted SSO entry 'IV-USER' for user 'mfjchtest'
[25/10/2002 16:26:17 1596]
```



## dotNSF "taim" - "the extension you already know" for Tivoli! dotNSF Tools for (IBM Tivoli) Access and Identity Manager

- dotNSF, Inc. an IBM Lotus and Tivoli Business Partner and ISV, announces at the 2002 Vienna IBM Symposium the first deployment of dotNSF's Tools and extensions for IBM Lotus Domino & IBM Tivoli Access Manager for e-Business
- The previous version of dotNSF tools was Finalist in Lotusphere 2001 Lotus Beacon Awards for Best Utility. **New in this version: Support for Tivoli !!!**
- Architecturally built using official IBM and industry standards APIs, it includes as core functionality a **Trust Association Interceptor for IBM Tivoli Webseal** (Tivoli's secure reverse proxy authenticator) **for Lotus Domino 5 - and 6 -**
- Enables the integration of IBM Lotus Domino databases, privileges, identities and access, and really centralised management of Lotus Domino users, groups and roles from within Tivoli User Manager functions.
- Availability: Immediate, directly from dotNSF, Inc (and/or via IBM Tivoli Sales)
- Prices and configurations: available upon request (configuration dependent)
- Also announced are a Database Object Browser extensions for Domino to perform real time scans - very useful for batch "import" or migration of objects properties and rights into the Webseal security object space.



# Integration with WebSphere Edge Server

## Strengths of the Proxies that Work with Access Manager:

### WebSEAL

---

- Authentication step-up
- Password policies
- e-Community SSO
- URL rewriting

### Edge Server Caching Proxy

---

- Robust caching
- Content-based routing
- Reverse and forward proxy
- URL mapping

### Policy Director and Edge Server Integration White Paper:

[http://mot.tivoli.com/product\\_info/enterprise/policy\\_dir\\_flashes\\_2001.html](http://mot.tivoli.com/product_info/enterprise/policy_dir_flashes_2001.html)

# How to get mad fast: check this table !

Feature	WebSEAL	Web PI	Edge
Easy Install	✓	3Q2003	✗
ADKs			
CDAS	✓	✓	✓
CDMF	✓	✓	✗
Password Strength	✓	✗	✗
Junctions	✓	✗	✗
Authentication <sup>2</sup>			
BA	✓	✓	✓
Forms	✓	✓	✓
Token	✓	✓	✗
Client Certificate	✓	✓	✓
HTTP Headers	✓	✓	✓ <sup>3</sup>
IP Address	✓	✓	✓ <sup>3</sup>
Fail-over Cookie	✓	✓	✓
CDSSO (SAML)	✓	3Q2003	✗
ecSSO	✓	✓	✗

Feature	WebSEAL	Web PI	Edge
iv-headers	✓	✓	✓
LTPA	✗	✓	✓
SPNEGO	✗	✓	✗
Session Indices <sup>4</sup>			
SSL Session ID	✓	✓	✓ <sup>5</sup>
Session Cookie	✓	✓	✓ <sup>5</sup>
BA Header	✓	✓	✓
HTTP Header	✓	✓	✓ <sup>3</sup>
IP Address	✓	✓	✓ <sup>3</sup>
LTPA	✗	✓	✓ <sup>6</sup>
SPNEGO	✗	✓	✗
iv-headers	✗	✓	✓ <sup>6</sup>
Policy			
Step-up <sup>7</sup>	✓	✓	✗
Reauthentication	✓	✓	✗

Feature	WebSEAL	Web PI	Edge
QOP	✓	✓	✗
Multi-Factor Auth <sup>8</sup>	✗	✗	✗
Boolean Rules <sup>9</sup>	✓	3Q2003	✗
Dynamic URI's	✓	✗	✗
MPA <sup>10</sup>	✓	✓	✓
Error Pages			
Custom Error Pages	✓	✗	✓
Macro's	✓	✓	✓
Web Account Mgmt <sup>11</sup>	✓	✓	✓
Serviceability			
Statistics Gathering	✓	✗	✗
Trace	✓	✓	✓
Switch User	✓	✗	✗
POST Data Caching	✓	✗	✓
Redirect on Login	✓	✓	✓ <sup>12</sup>
XKMS (client cert auth) <sup>13</sup>	✓	✗	✗

Feature	WebSEAL	Web PI	Edge
SSO			
BA			
Supply	✓	✓	✓
Filter	✓	✓	✓ <sup>14</sup>
GSO	✓	✓	✗
LTPA Cookie	✓	✓	✓
TAI	✓	✗	✓
IV Headers	✓	✓	✓
Forms Single SO	✓	3Q2003	✗
Fail-over Cookie	✓	✓	✓
Virtual Host Support <sup>15</sup>	✓	✓	✓
Personalization Svc. <sup>16</sup>	✓	✗	✗
Tag/Value	✓	✓	✓
Remote Session Mgmt	✓	✗	✗
Multi-Locale	✓	✓	✓
Multi-Charset (i-mode)	✓	3Q2003	✓
Password Policy	✓	✓	✓ <sup>17</sup>

## Credits:

### ■ Our Teachers

- Lotus/IBM/Iris:
  - too many links, thanx to all !
- Our Partners:
  - Penumbra Partnering Inc.  
<http://www.PENUMBRA.org>
- Our Customers
  - Some names in our site :-)

## Legal Disclaimers and other fine print :-)

- Trademarks:
  - "dotNSF" is a registered Trade Mark of dotNSF, Inc.
  - All IBM Corp's Trademarks acknowledged.
  - All other Trademarks acknowledged.
- License:
  - dotNSF, Inc. hereby grants IBM the non-exclusive license with limited right to use, reproduce, display, perform, and distribute the presentation materials for Lotus' educational, marketing and promotional purposes, attributing dotNSF as the source. It may be placed on Lotusphere CDs, Lotusphere Web Sites, or other media at discretion of Lotus. Like most presentations, this one is best presented by the original authors/speakers, who had access to the raw material summarized here; thus we kindly request communication to us of the effective or intended reuse of this material: dotNSF, Inc - and NashCom - will make best efforts to have this material presented by the original speakers - upon request of IBM - or any other third parties, at very reasonable probono rates.
- Copyright 2000-2003 dotNSF, Inc and its suppliers. All rights reserved

Please contact us for further information:



**the extension  
you already  
know**

**George Chiesa**

George Chiesa <[Chiesa@dotNSF.com](mailto:Chiesa@dotNSF.com)>  
Mobile Phone: [+44 771 85 87 673](tel:+447718587673)  
Tel/Ans/Fax: [+44 1753 830 600](tel:+441753830600)  
Web Site: <http://dotNSF.com>

"dotNSF" is a TradeMark of dotNSF, Inc.  
© MM dotNSF, Inc. All Rights Reserved  
It's about business, not just technology!



**Nash!Com**  
Communication Systems

Daniel Nashed

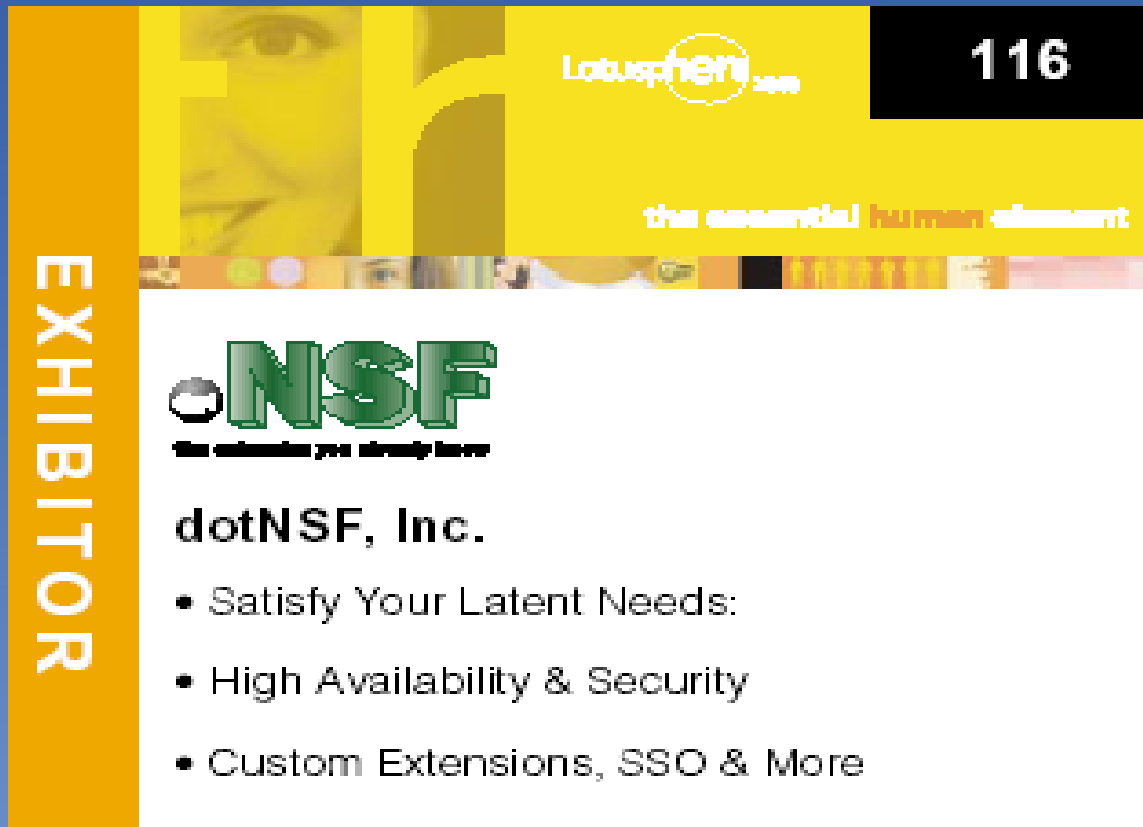
Weidenweg 58  
40723 Hilden  
Germany

+49 172 2141912  
[nsh@nashcom.de](mailto:nsh@nashcom.de)

Lotus/IBM Business Partner/ISV



# Please meet us at our pedestal: 116



**EXHIBITOR**

Lotusphere 2003

116

the essential human element

**dotNSF**  
the extension you already know

**dotNSF, Inc.**

- Satisfy Your Latent Needs:
- High Availability & Security
- Custom Extensions, SSO & More