dominopoint DAY2009

Come farsi licenziare facilmente

Domino Admin and Security Gone Wrong

Autore: Franziska Tanner

Professione: Domino Administrator/Instructor

Chi sono:

- Nata e vissuta in Svizzera, ho vissuto 16 anni in USA, e negli ultimi 3 anni, vivo ai Caraibi
- 13 anni di esperienza su ambiente Domino
  - Gestione, Architetture e supporto
- da 10 a 100,000 utenti, dalla versione 4 alla 8.5
- Ho visto sia il meglio che il peggio, dalla non struttura ad ambienti super strutturati
- Esperienza di istruttore Lotus (e Amministratore)
- Un po' di certificazioni

Come farsi licenziare facilmente

1. Lo stagista pensa che il tuo capo è sovrappagato
   - Gestisci male le ACL

2. Fare il backup non è difficile ma fare backup seriamente lo è…
   - Lavora anche con cose di cui non sei responsabile

3. Condividere informazioni con le persone sbagliata
   - Come tenere gli impiegati licenziati realmente senza accesso

4. Divertisi con un progetto del weekend– ricertificare il tuo ambiente
   - Gestire certificatori e password correttamente

Come farsi licenziare facilmente

5. I tuoi utenti non sanno cosa significa la parola“Schaltfläche Öffnen”
   - Cambia il language pack del DB di posta degli utenti durante la notte
   - Il task DESIGN è una feature potente

6. “Non so perchè il tuo server crasha”
   - Perchè gli utenti non hanno bisogno di mettere le loro applicazioni sul server

7. Chi è abilitato ad eseguire“del c:*.doc /s” sulle workstation
   - Controllare i diritti degli agenti

Come farsi licenziare facilmente

8. Il tuo competitor conosce il tuo organization chart
    - Metti la directory non navigabile da browser web

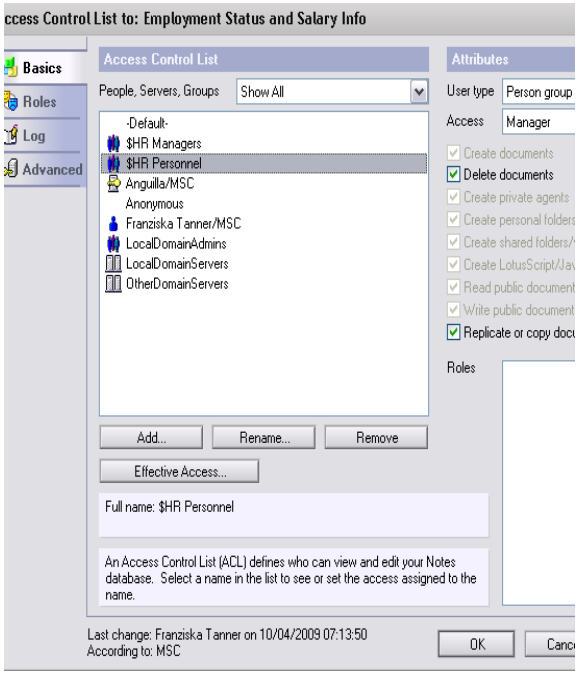
9. Lasciare aperto al mondo a dei task misteriosi
    - Stai fornendo POP3, IMAP ed altri accessi a persone che non dovrebbero averli

10. Chiunque è il benvenuto – ID allegati
    - Tenere I tuoi data in sicurezza

1. Cattiva gestione delle ACL's

Caso tipo:

Il tuo stagista pensa che tu sia sovrappagato. Pensi che l'H.R. apprezzerebbe che lui abbia accesso al database con lo "storico delle retribuzioni"?



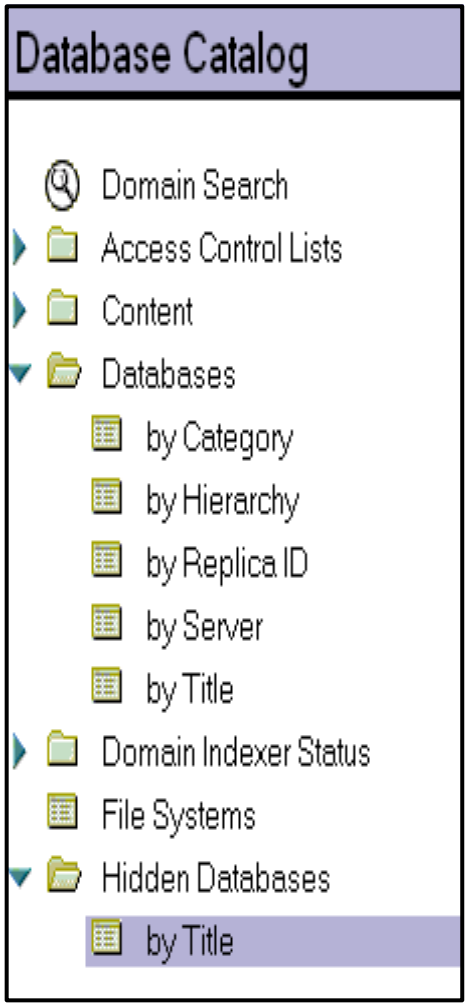
Come succede:

- Inherited environment
  - "all users had Manager rights when I got here"
- ACL's are open to groups by mistake
  - Good nested group management is key
- "Enforce consistent ACL" not implemented
  - Goes along with….
- Lack of pro-active information
  - Do you know for sure what your ACL's are like

1. Cattiva gestione delle ACL's

Fixing it:

1. Audit your environment
2. Identify what's wrong
3. Establish and capture standards
4. Clean up what's wrong
5. Audit periodically



Auditing your environment:

- Your catalog is your best friend
  - Work with one, centrally replicated catalog
  - Include hidden applications
    - View = SELECT @IsAvailable(ReplicaID)& @IsUnavailable(RepositoryType)

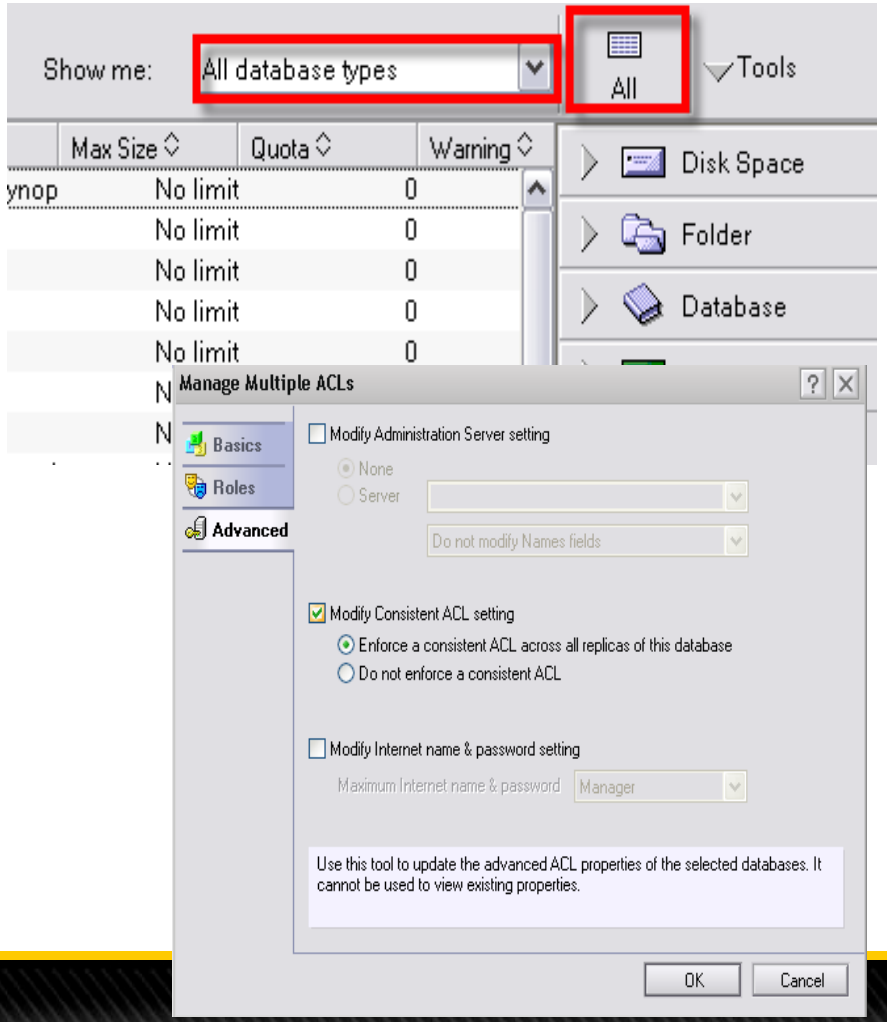
1. Cattiva gestione delle ACL's

Establish and documenting standard ACL's:

- A document library design works well

Mass changing ACL options:

- View all file database types
- Use CTRL+A
- Add [LocalDomainAdmins] to templates
- Enforce consistent ACL's
- Change the Admin server



2. Condividere informazioni con le persone sbagliata

Caso tipo: 80% dei Domino admin non hanno reso effettivi i licenziamenti. Mentre il 100% di loro pensano di averlo fatto correttamente.

Cosa significa:

1. Ambiente ereditato
   - "era così quando sono arrivato e niente si è rotto fino a quel momento"
2. Scarsa comunicazione con HR
3. Documento Server Setting
   - Tab Sicurezza-"Not Access Server"
4. Gruppo e tipo gruppo "Deny Access"
5. Consistenza attraverso tutti I server e protocolli
6. Mito: se non c'è un documento persona, l'utente non può entrare

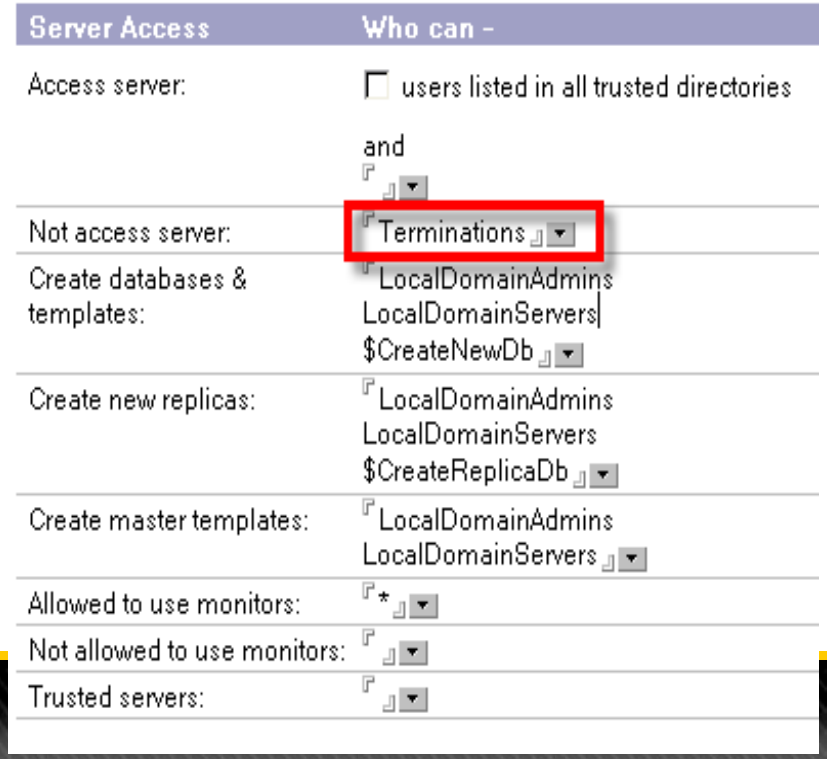
2. Condividere informazioni con le persone sbagliata

Come risolvere:

1. Lavorare con HR per creare un processo di comunicazione a prova di idiota
   - Non fare affidamento su una sola persona
   - Automatizzare se possibile un account per gestire assunzioni e licenziamenti

2. Controllare tutti i documenti server
   - Security tab - Not Access Server

3. Verifica che il gruppo esista
   - Ne rimarrai sorpreso

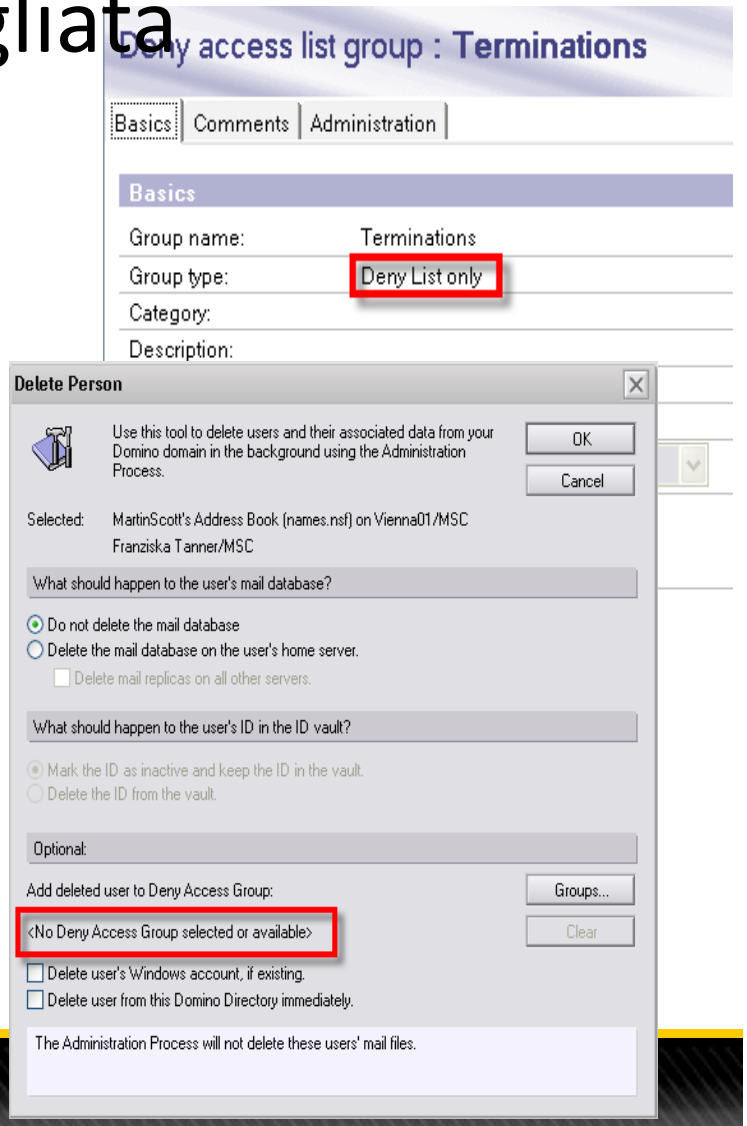


2. Condividere informazioni con le persone sbagliata

Come risolvere:

4. Verifica che il gruppo sia del tipo corretto
   - La Deny List è l'unico tipo di gruppo che l' AdminP non può toccare

5. Verifica che le persone siano state realmente inserite in quel gruppo
   - Default is nothing
   - Once this is set, it'll cache



3. Nessuno deve essere inpreparato

Caso tipo: La maggior parte delle aziende hanno la capacità di fare backup dati. In teoria.

Come succede:

1. “Ma Pippo fa il backup!”
   - Corretto, tranne per il fatto che sei TU a gestirlo

Problemi correlati:

- Le patch del sistema operativo causano crash
- Nessun antivirus nel S.O. o la configurazione dello stesso possono causare problemi a Domino

Come risolvere:

1. Comunicare gli altri team dell’azienda e TESTARE

4. “Qual’era la mia password?”

Caso: Nella tua carriera di Domino admin perderai il “cert.id” o la sua password solo una volta. Te lo assicuro!

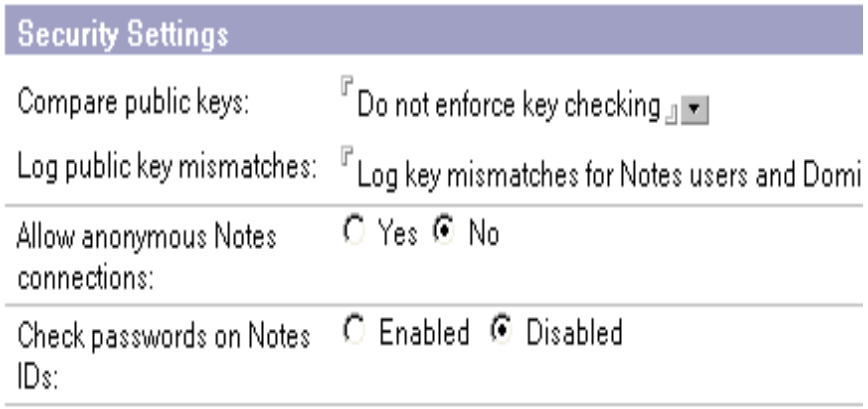
Come ciò accade:

1. Hai spostato il tuo server originale su un altro server
   - I certificatori vengono creati sempre con il primo server
2. Hard-disk dell’Admin rotto
   - Mi auguro che I tuoi cert.id esistano da qualche altra parte
3. Se non usi il metodo di salvare le tue password in più punti ??
4. Turnover mal realizzato o che non doveva essere f

4. “Qual’era la mia password?”

Come riparare (inserire risata isterica):

1. Crea il nuovo certificatore
2. Cross-certificalo con il vecchio
3. Uncheck “check certificates”
4. Ri-certifica tutto
   - Clients, servers, OU’s
5. Una volta fatto,
   re-check “check certificates”
   - Magari loggati prima
6. Valuta di inserire password multiple sul certificatore



Note: CA process and ID Vault managers do NOT get added or removed automatically

5. Cambiare lingua del DB di posta durante la notte

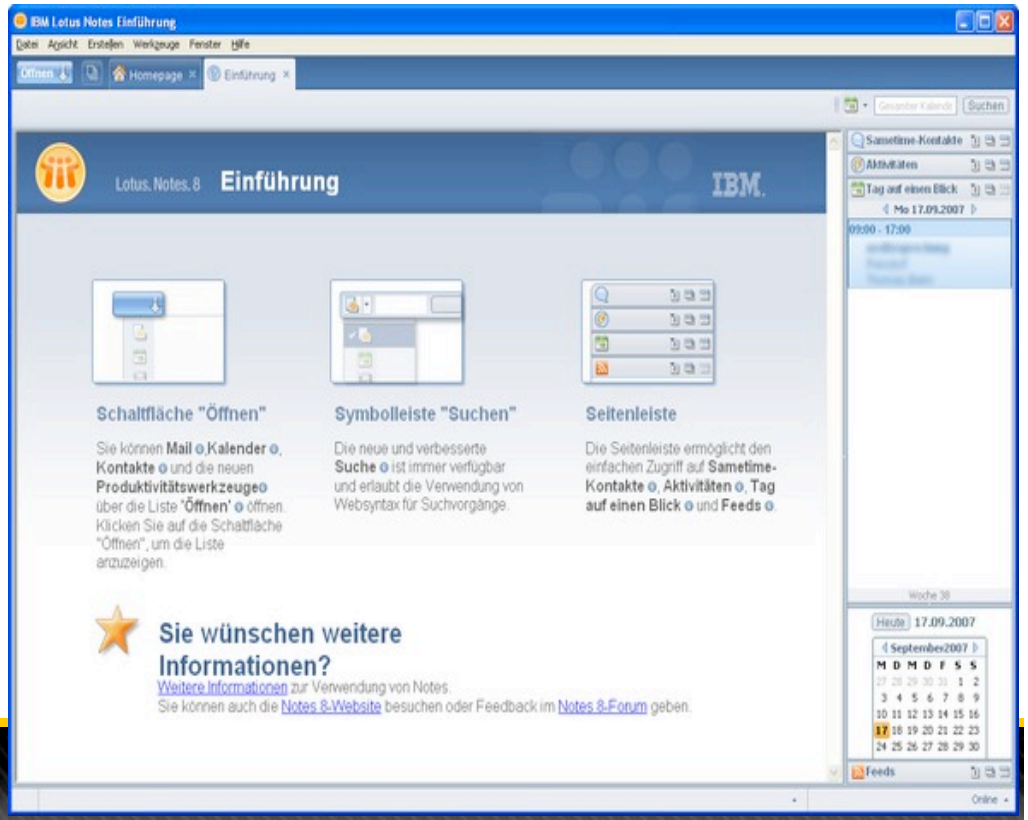
Caso tipo: E' molto probabile che le persone della tua azienda non sappiano il significato di "Schaltfläche Öffnen" e che non apprezzino vederlo apparire in Notes durante la notte.

Come ciò accade:

- Avere più di un template che dichiarano essere Master template
- Aggiungici il Design task
- Aggiungici qualche replica per altro divertimento

Problemi correlati:

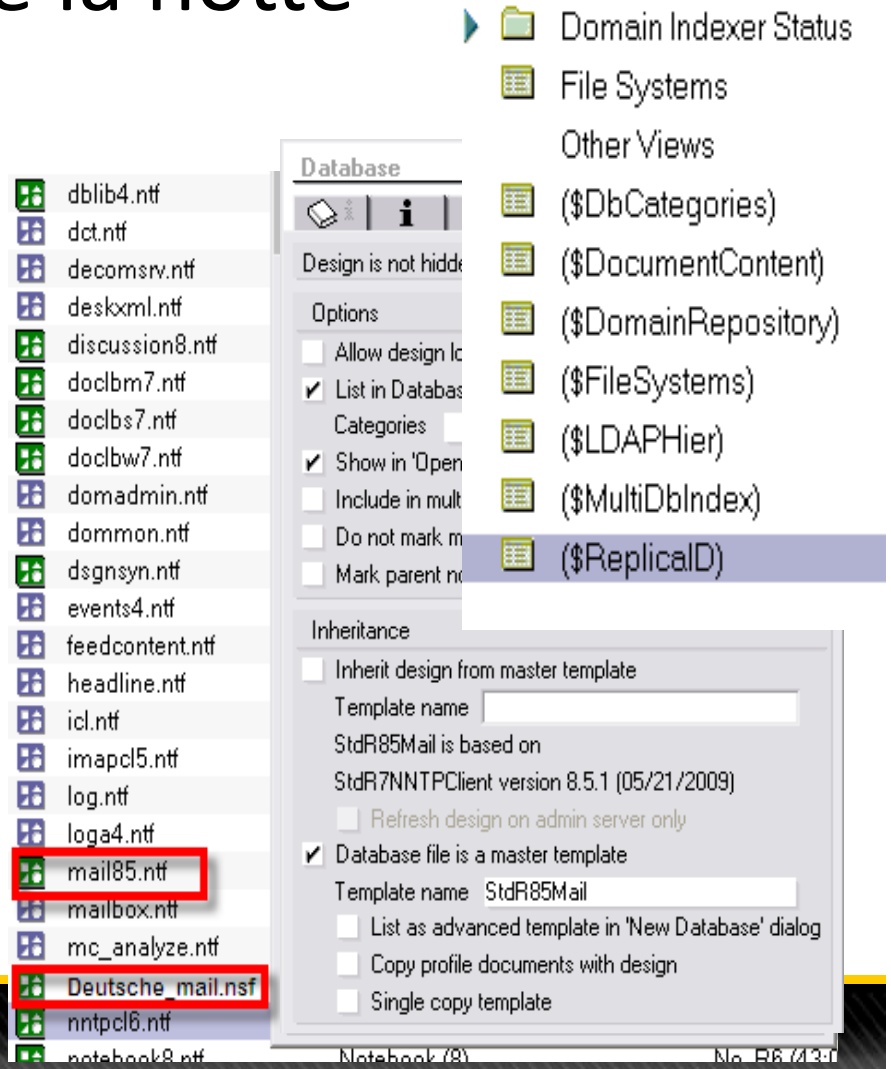
ID di replica duplicati



5. Cambiare lingua del DB di posta durante la notte

Fixing it:

1. Identifica il template "cattivo"
   - Usa le viste nascoste in un catalogo centrale
   - Usa Admin client, Files tab
   - Anche le sottocartelle
2. Sostituisci con il template giusto
3. Load design
4. Rinforza la sicurezza del server
   - Diritti di creazione dei DB sul server
   - ACL dei templates



6. “Non so perchè il mio server crasha”

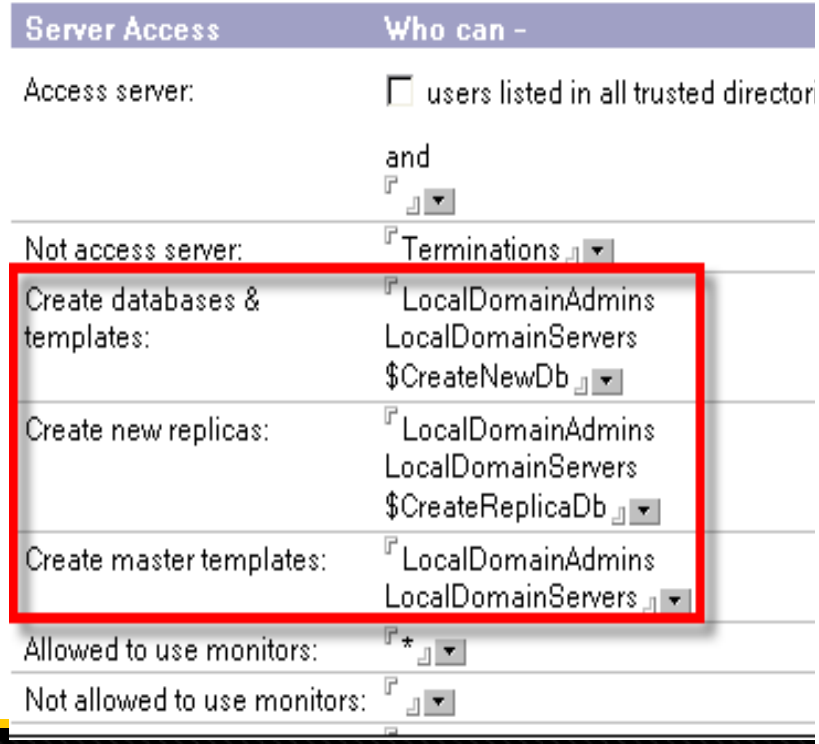
Caso tipo: Nemmeno tutti gli sviluppatori sanno come scrivere un’applicazione che non mandi in crash il server. Perchè consentire ai tuoi utenti di mettere le proprie applicazioni casalinghe sul server?

Come ciò accade:

1. Nessuno si cura di guardare
   - Ambiente ereditato
2. Si forniscono accessi incosistenti
   - I tuoi server sono tutti uguali?

Come risolvere:

1. Aggiungere soltanto Admin e Server
   - Gli sviluppatori testano sul server TEST

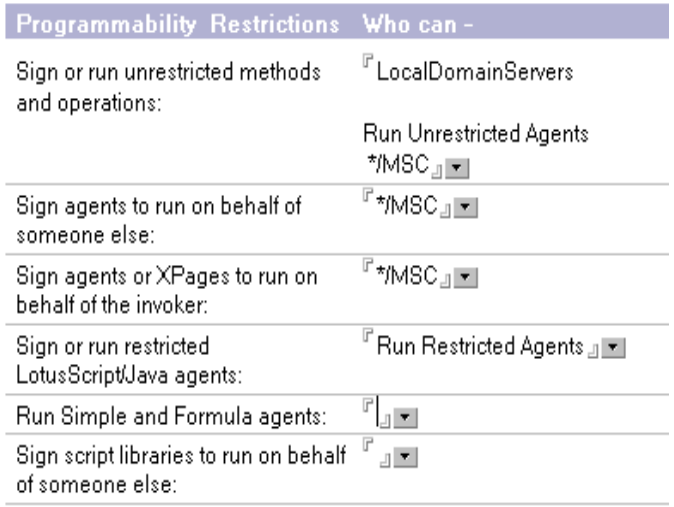


7.Il grande agente “Liberi tutti”

Caso tipo: Tutti I nuovi documenti nel tuo DB “Storico retribuzioni” sono stati inoltrati ad un indirizzo internet. Per l’intero anno passato.

Come ciò accade:

- Diritti per eseguire unrestricted agents sono consentiti a */=O
  - Pensa “chi vuole eseguire run del c:*.doc /s sulle workstation degli utenti
- I documenti server non sono allineati
- Configurazione ereditata



Programmability Restrictions	Who can -
Sign or run unrestricted methods and operations:	LocalDomainServers Run Unrestricted Agents */MSC
Sign agents to run on behalf of someone else:	*/MSC
Sign agents or XPages to run on behalf of the invoker:	*/MSC
Sign or run restricted LotusScript/Java agents:	Run Restricted Agents
Run Simple and Formula agents:	
Sign script libraries to run on behalf of someone else:	

Problemi correlati:

Le ECL’s e firmatari identificati non sono implementati

7.Il grande agente “Liberi tutti”

Come risolvere:

- Inventarsi un insieme di “Restrizione di programmazione” che funzionino
  - Quindi implementarle su tutti I server
  - Be sure to read field help as sometimes nothing = everyone OR nobody
- Capisci le tue ACL e puliscile
- Implementa le ECL e firma le identità per completare il cerchio
- Documenta queste impostazioni COME SI SUPPONE che siano così che tu possa verificarle in seguito
  - Usa i probes DDM per confrontare gli altri server con quello ideale

8. Il competitor conosce il tuo organigramma

Caso tipo: Il tuo competitor(e praticamente qualsiasi hacker là fuori) apprezzano molto la possibilità di scorrere la tua directory online.

Come accade ciò:

- Ereditato da un ambiente Domino esistente– ancora
- Mancanza di testing
  - Questo lo vedo sempre sui siti dei clienti "funziona solo con la VPN"
- Controlla tutti i documenti server
  - Rinforzare la configurazione di accesso al server

Problemi correlati:

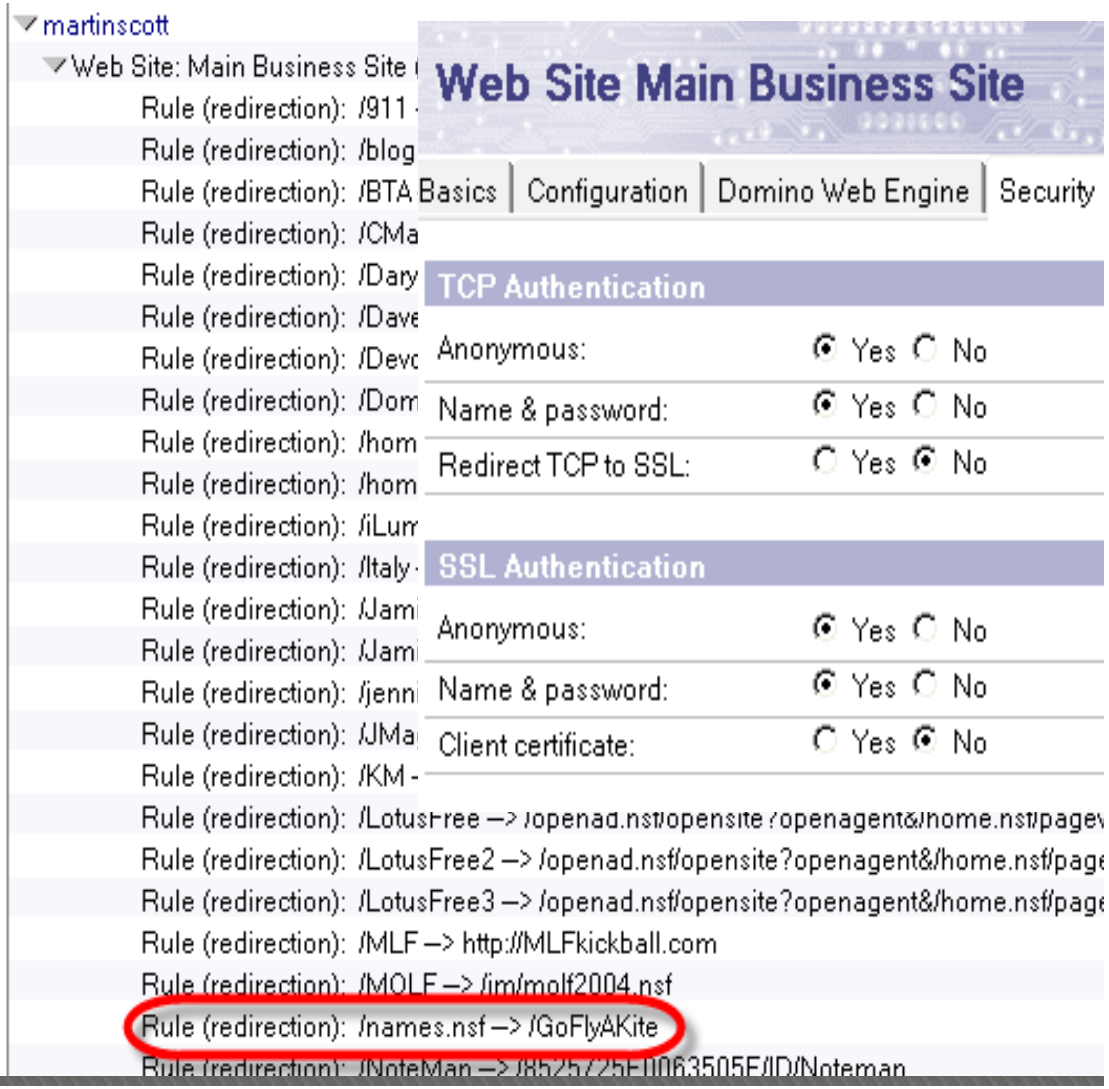
- Eseguire task non necessari, senza eliminare correttamente gli utenti
- Usare "More name variation with lower security"

8. Il competitor conosce il tuo organigramma

Come riparare:

- TEST TUTTI I SERVER per vedere se hai aperto la names.nsf
  - ➢Non soltanto quelli che pensi stiano lavorando su HTTP

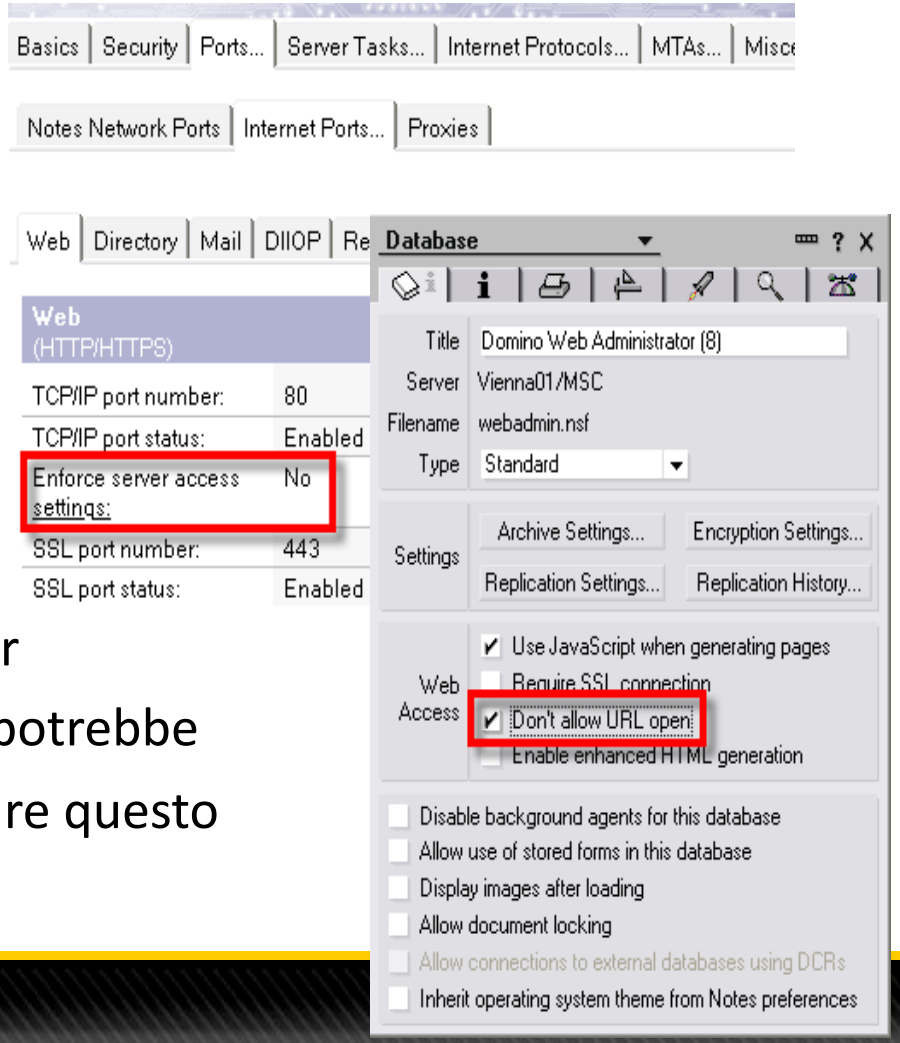
- Usa I documenti internet site I quali sono definiti al tuo sito principale se non si trova un URL.



8. Il competitor conosce il tuo organigramma

Come risolvere:

- Controllare tutti I documenti server e rinforza le impostazioni di accesso al server
- Implementa il redirect SSL dopo l'autenticazione
- Usa proprietà DB"Don't allow URL open"
  - ➢Sends 500 Not Authorized error
  - ➢Suggerimento: Webadmin.nsf potrebbe essere un buon canditato per fare questo



9. Lasciare aperto al mondo task misteriosi

Caso tipo: Il capo del tuo capo potrebbe apprezzare l'accessoPOP3 che tu non sai che stai dando, finquando i gestori della sicurezza fanno un check.

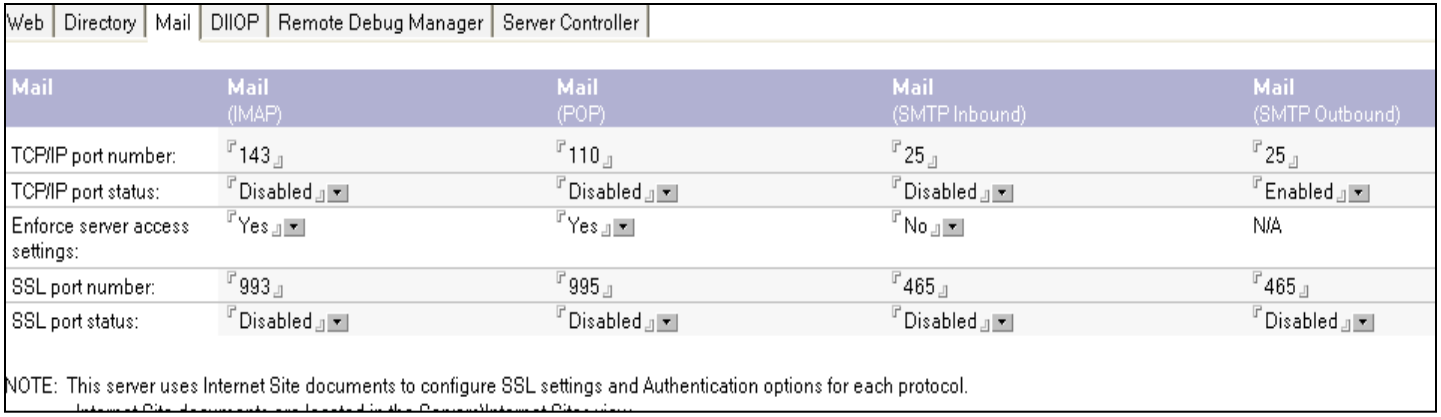
Cosa significa:

- Ambienti ereditati– sei già stanco di ascoltare questa frase?
  - ➢ Stai anche sprecando le risorse del server
- La console dell'admin ti mostra cosa sta girando
  - ➢ Guarda il notes.ini per la lista definitiva
- Di default tutte le porte sono abilitate sul tuo server
  - ➢ I carichi accidentali accadono

9. Lasciare aperto al mondo task misteriosi

Come riparare:

1. Inventario del notes.ini su tutti i server
   - Leggi e confronta i parametri costantemente
2. Rimuovi I Task e le porte non necessarie
   - Già che sei lì*cough ChangeControl cough*
3. Disabilitare tutte le porte non utilizzate in tutti i server document



Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Disabled	Disabled	Disabled	Enabled
Enforce server access settings:	Yes	Yes	No	N/A
SSL port number:	993	995	465	465
SSL port status:	Disabled	Disabled	Disabled	Disabled

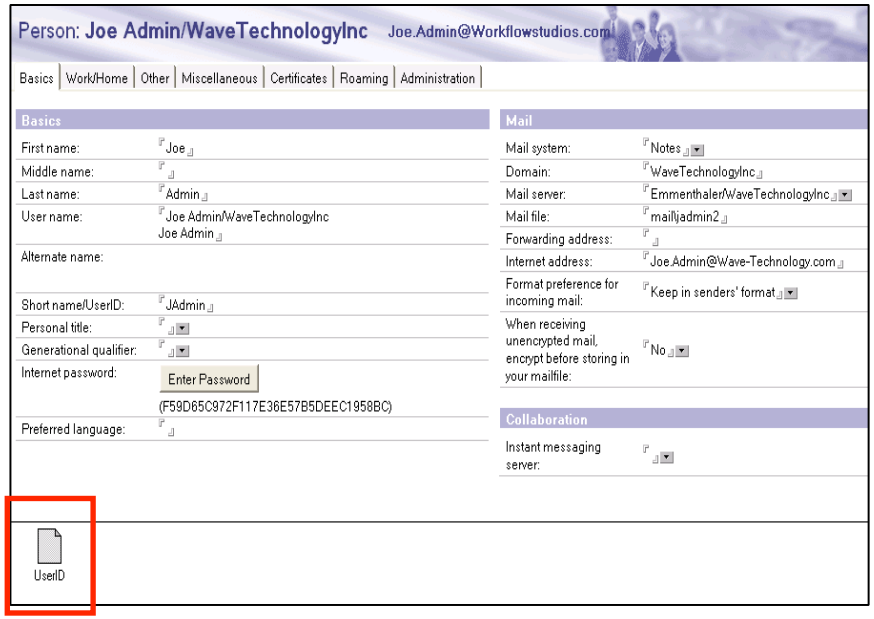
NOTE: This server uses Internet Site documents to configure SSL settings and Authentication options for each protocol.

10. Benvenuti tutti– ID allegati

Fact: Ci vuole tanto meno a creare password standard e lasciare gli utenti scaricare le loro ID, almeno fin quando avrai pulito questo caos

Come accade ciò:

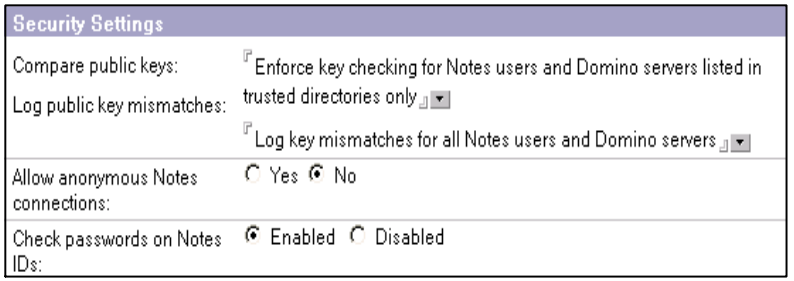
- Le password standard sono usate per comodità
- Il controllo delle password non è mai implementato
  - ➢ Molte combinazioni di id/password possono essere la fuori
  - Il controllo delle password è impostato scorrettamente

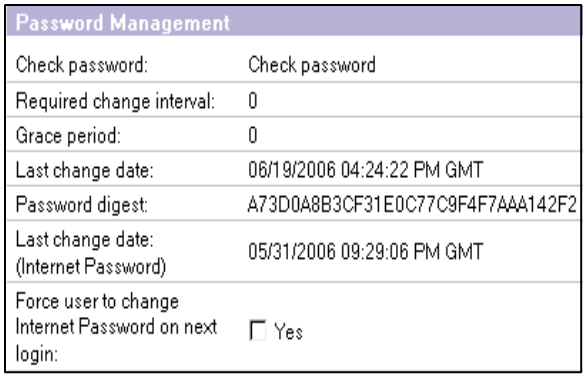


10. Benvenuti tutti– ID allegati

Come riparare ciò:

1. Non utilizzare password standard
2. Utilizzare le policy di sicurezza per forzare il cambiamento delle password
   - Assicurati di sincronizzare con le password internet
3. Implementare il controllo delle password
   - Sia sul client che sul server
4. Rimuovere tutti gli allegati ID's
   - Non dimenticarti delle server.id visto che di solito non hanno una password





Come tenere stretto il tuo lavoro

- A meno che tu non abbia realizzato il tuo ambiente da zero, o l'abbia controllato costantemente, non sai quali siano le configurazioni errate nei tuoi server
- Non pensare"come risolvo questo problema", ma pensa "come posso risolvere e prevenirlo di non succedere ancora"
- Sei tu a gestire il servizio Domino, comprese le cose che gli altri devono curare
- Usa tutti gli strumenti che hai a disposizione, statrep.nsf, catalog.nsf, monitoring tools come DDM and probes, decommission server analysis, event notifications
- Dopo aver riparato, è buono documentare il tuo ambiente creato.

Domande? Commenti?

Contattami: francie.tanner@martinscott.com

Blog: http://www.martinscott.com/blog

Twitter: akafrancie

Skype: franciewhitlock

LinkedIn: http://www.linkedin.com/in/franciewhitlock

Dominopoint Day

è stato possibile grazie a:

Platinum Sponsor

IBM
TREND MICRO
BlackBerry
GSX
Synaptris
Premium Reseller
Lotus. software
IBM Systems
WebSphere. software
Tivoli. software
Rational. software

Gold Sponsor

Ytria
PLANTRONICS. SOUND INNOVATION
Xerum
integra for notes
extracomm