

# Exchange 2003 Service Pack 2

Con il Microsoft Exchange Server 2003 Service Pack 2 (SP2) arrivano buone notizie sia per gli amministratori di sistema sia per gli utenti perché una serie di migliorie rende il lavoro più facile. Vediamo alcuni degli aggiornamenti più importanti

**I**l SP2 di Exchange Server 2003 è costruito sulle solide basi gettate da Exchange 2003 e dal SP1 e dovrebbe essere un aggiornamento benvenuto che a mio avviso le aziende implementeranno rapidamente. Diamo uno sguardo agli aggiornamenti più importanti del SP2 per aiutare a valutare la convenienza ad effettuare l'upgrade.

## Supporto per i dispositivi mobili

Con così tanti dispositivi mobili in uso – dagli smart phone ai PDA – e per il fatto che la messaggistica, l'agenda elettronica e la gestione delle attività sono applicazioni popolari per questi dispositivi, Microsoft ha chiaramente sentito la necessità di integrare questi dispositivi in Exchange. Prima di Exchange 2003, tecnologie di terze parti fornivano i componenti necessari per connettere i dispositivi mobili a Exchange, e compagnie come Good Technology e RIM dovevano una buona parte del proprio business alla loro capacità di connettersi e sincronizzarsi con Exchange.

Sebbene Exchange 2000 Server abbia delle buone capacità in questo campo, Microsoft ha fatto un balzo in avanti con la prima release dei Mobile Services per il sottosistema Exchange in Exchange 2003, riconoscendo l'importanza del mercato dei dispositivi mobili e la rapida crescita delle funzionalità di questi ultimi dedicando molte risorse allo sviluppo di questi servizi.

Il risultato è che i Mobile Services, con il loro ricco insieme di caratteristiche, sono ora una offerta competitiva e a basso costo per il supporto dei dispositivi mobili. Microsoft ha inoltre licenziato la sua tecnologia Exchange ActiveSync ai fornitori di dispositivi mobili come Data Viz, Motorola, Nokia, Palm, e Symbian, così è lecito aspettarsi un maggior supporto per Exchange da parte dei dispositivi e delle applicazioni provenienti da questi produttori.

Prima del SP2, i Mobile Services facevano parte di una categoria di soluzioni mobili preziose e poco costose. Sebbene vengano offerti in bundle con Exchange, soffrono di mancanza di funzionalità in qualche area importante. In congiunzione ad alcune delle migliorie presenti in Windows Mobile 5.0, il SP2 aggiunge:

- Compressione dei dati per connessioni ActiveSync su HTTPS (HTTP Secure) utilizzando gzip.
- Pooling di connessioni che riducono il sovraccarico dovuto alla creazione di connessioni tra i dispositivi e la rete.
- Autenticazione basata sui certificati.
- Criteri di protezione obbligatori
- Ricerca Global Address List (GAL) e convalida degli indirizzi in tempo reale per mezzo della GAL.

## AUTD migliorato

Il meccanismo AUTD (Always-Up-To-Date) viene utilizzato da Exchange per fornire nuove informazioni relative alla mailbox ai dispositivi mobili. AUTD invia informazioni ai dispositivi mobili, ma in alcuni casi è possibile considerarlo un meccanismo di pull in quanto fornisce solo notifiche. Nel tempo, Microsoft ha dotato AUTD della possibilità di inviare più dati (come le intestazioni dei messaggi) al fine di rendere il tool un completo meccanismo di push.

L'autenticazione basata sui certificati è in particolar modo benvenuta in quanto aumenta la protezione identificando univocamente un dispositivo in modo simile a quanto fanno i dispositivi BlackBerry che identificano se stessi alle reti wireless. Utilizzando l'autenticazione basata sui certificati combinata con i criteri di protezione obbligatori che richiedono agli utenti di inserire un PIN per accedere ai dispositivi, si ottiene una autenticazione dual-factor.

Nel SP2, AUTD utilizza connessioni TCP/IP persistenti, piuttosto che SMS (Short Message Service) per inviare notifiche ai dispositivi mobili. Il dispositivo invia una richiesta a Exchange per registrare una richiesta di sottoscrizione per gli aggiornamenti alla mailbox nello stesso modo in cui Microsoft Outlook Web Access (OWA) registra le nuove notifiche per la posta e l'agenda. La richiesta specifica un intervallo di tempo (in genere 15 minuti) e le cartelle che il dispositivo controlla (generalmente Inbox, Calendar, Contacts, e Tasks). Se i dati in queste cartelle vengono modificati durante l'intervallo prestabilito, Exchange invia un pacchetto UDP alla porta 2883 del server front-end utilizzato dal dispositivo mobile, e il server front-end usa la sua connessione HTTP aperta verso il dispositivo mobile per inoltrare la notifica. Dopo che il dispositivo ha ricevuto la notifica, questo stabilisce una richiesta di sincronizzazione con Exchange per recuperare i nuovi dati e impostare una nuova sottoscrizione. Se Exchange non ha aggiornamenti per il dispositivo, invia un messaggio "no data", al quale il dispositivo può rispondere con una nuova richiesta di sottoscrizione.

Se la connessione di rete (come un collegamento wireless o GPRS) viene interrotta dal dispositivo che è stato chiuso o spostato fuori dal raggio d'azione del collegamento, il dispositivo è in grado di ristabilire la comunicazione e riavviare la connessione Exchange. I dispositivi GPRS consumano energia aggiuntiva solo quando trasmettono, così il meccanismo AUTD è più efficiente anche da questo punto di vista rispetto ai dispositivi che interrogano regolarmente Exchange per ottenere gli aggiornamenti. Il tempo di vita dipende dal carico di lavoro al quale è soggetto il dispositivo, ma secondo Microsoft alcuni utenti hanno riportato un incremento oscillante tra il 20 e il 30 per cento

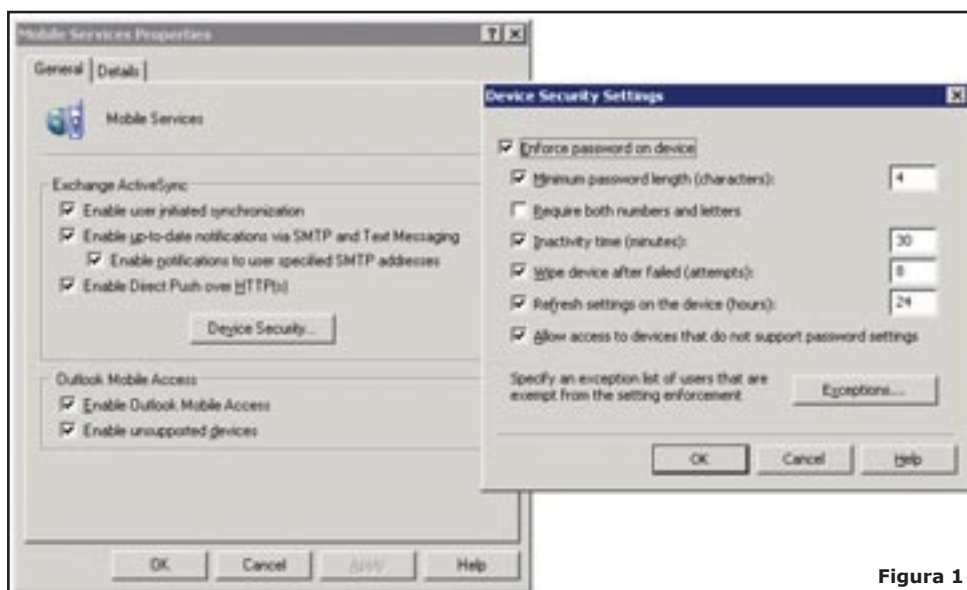


Figura 1

nella durata delle batterie quando hanno utilizzato dispositivi Windows Mobile 5.0.

### Alla ricerca delle GAL

I dispositivi mobili possono utilizzare la caratteristica GALSearch per accedere al server e convalidare gli indirizzi email. Dal momento che la memoria è preziosa per i dispositivi mobili, GALSearch supporta un limitato sottoinsieme di informazioni gestite dalle GAL (al confronto con altri client come ad esempio Microsoft Office Outlook). La Tabella 1 elenca le proprietà che GALSearch supporta e come vengono mappate con gli attributi dell'Active Directory (AD). La caratteristica GALSearch prende una stringa di interrogazione fornita dall'utente ed esegue una ricerca nell'indice ANR (Ambiguous Name Resolution) sul server degli oggetti abilitati nelle GAL. La ricerca ANR, che è simile alla ricerca che effettua Outlook quando cerca le GAL, tenta di restituire fino a 100 risultati che possano soddisfare la stringa di ricerca.

### Protezione dei dispositivi mobili

Nel SP2, i Mobile Services supportano un insieme di protezioni e di caratteristiche di sicurezza, tra le quali:

- Obbligo di utilizzare un PIN (l'utente deve inserire un PIN per avere accesso al dispositivo)
- Impostazione di una lunghezza minima, in caratteri, della password
- Richiesta di utilizzare numeri e lettere nella password
- Tempo di vita del PIN fissato
- Disabilitazione del dispositivo dopo un impostato numero di password errate

In aggiunta, i Mobile Services consentono ai dispositivi di connettersi ad Exchange anche se non supportano le impostazioni relative alle password. Alcuni dispositivi (generalmente vecchi dispositivi come quelli che eseguono Microsoft Pocket PC 2003) non possono rispondere correttamente alle richieste Exchange che scaricano ed

impostare i dati relativi alle policy. Questi dispositivi possono ignorare i criteri relativi alle password e continuare a sincronizzare i dati con Exchange, che è l'approccio che occorre seguire se si deve supportare un misto di dispositivi vecchi e nuovi. È possibile anche creare una lista di utenti che sono esentati dal seguire le policy delle password. Questi utenti possono avere vecchi dispositivi o avere dispositivi che supportano altri meccanismi di autenticazione, come ad esempio la lettura delle impronte digitali. Si accede alle impostazioni relative alle policy delle password facendo

clic su Device Security dalla scheda General delle proprietà delle impostazioni globali per i Mobile Services, rappresentata in Figura 1.

Vedere l'articolo correlato "Impostazione delle policy per i dispositivi mobili" per una spiegazione degli attributi AD che controllano le impostazioni delle policy per i dispositivi mobili.

### Reimpostazione dei dispositivi mobili

Sino al SP2, Microsoft non supportava un metodo per ripulire o reimpostare un dispositivo mobile (ad esempio smart phone o Pocket PC). Altri sistemi concorrenti, come GoodLink Server o BlackBerry Enterprise Server (BES), supportano caratteristiche che consentono agli amministratori di inviare istruzioni ai dispositivi mobili per ripulire il loro contenuto se vengono perduti o rubati.

La funzionalità di pulizia (wiping) fornita dal SP2 è elementare ma efficace. Una pagina Web ad accesso limitato (<https://server-name/MobileAdmin>) consente di ripulire i dispositivi, cancellare i comandi ed eliminare le sincronizzazioni tra il dispositivo e gli utenti. Quando si inizia una pulizia remota, l'applicazione Web invia un comando WebDAV Propatch alla mailbox dell'utente per impostare la proprietà wipeinitiated della mailbox a un valore non zero. I Mobile Services notano che la proprietà è impostata e inviano un comando di pulizia (wipe) al dispositivo, il quale esegue localmente il comando appropriato. Il client quindi rinvia il comando di ritorno al server con una indicazione di successo o fallimento. Un log registra tutti i comandi e lo stato riportato dal dispositivo. Il comando wipe non può, comunque, cancellare dati memorizzati su memory card apposite; i soli dati che il dispositivo può ripulire sono quelli relativi alle impostazioni specifiche dell'utente. Queste migliorie non sono gratuite, così se si vuole trarre vantaggio dalle migliorie offerte dal SP2, occorre effettuare l'aggiornamento dei dispositivi mobili con il Windows Mobile 5.0 Messaging and Security feature pack (vedere all'indirizzo <http://www.microsoft.com/windowsmobile/business/5/default.aspx> per i dettagli).

Diversi produttori hanno differenti approcci per l'ag-

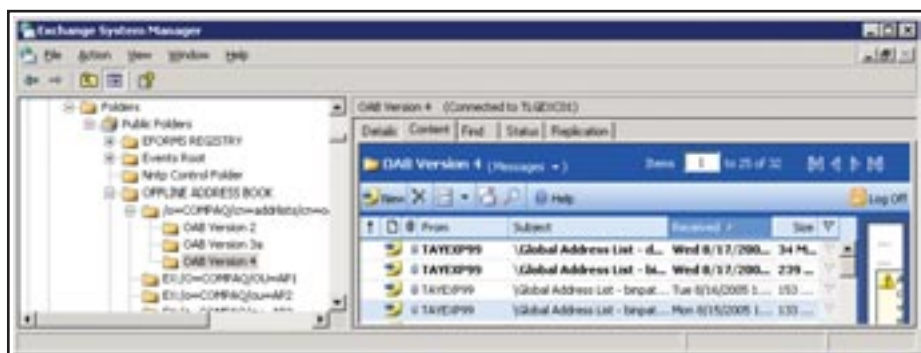
**Tabella 1: Proprietà Mobile GAL**

Proprietà ActiveSync	Attributo ADAD attribute
DisplayName	displayName
Phone	telephoneNumber
Office	physicalDeliveryOfficeName
Title	Title
Company	Company
Alias	mailNickName
FirstName	givenName
LastName	Sn
MobilePhone	Mobile
EmailAddress	Maildevice

giornamento (e il testing) alle nuove versioni di Windows Mobile, così occorre controllare presso il proprio fornitore quali criteri di aggiornamento adotta e quali dispositivi supportano Windows Mobile 5.0.

### Continua la guerra allo spam

Microsoft ha aumentato la capacità di Exchange di scartare la posta indesiderata. La versione originale di Exchange 2003 supportava un miglior filtro sulle connessioni ed i recipient (i contenitori dei messaggi di posta), e la capacità di restringere l'accesso ai gruppi di distribuzione. Il SP1 aveva risolto alcuni problemi, come ha fatto la prima versione dell'Intelligent Message Filter (IMF), che è basato sulla stessa SmartScreen Technology che Microsoft utilizza per proteggere il suo servizio



**Figura 2**

MSN Hotmail. Il Junk E-mail Filter di Outlook 2003 inoltre utilizza una variante di IMF. Fondamentalmente, IMF esamina un flusso di messaggi di posta in entrata e imposta un valore di probabilità di spam (SCL, Spam Confidence Level) per ogni messaggio. Se questo valore è più alto rispetto a un valore prefissato dall'amministratore, Exchange scarta immediatamente il messaggio; viceversa, questo viene passato all'utente. Il Junk E-mail Filter di Outlook quindi valuta il messaggio e lo passa o lo rifiuta, a seconda delle preferenze impostate dall'utente. Per esempio, alcuni indirizzi potrebbero essere in una lista particolare dell'utente e in questo caso Outlook non sopprimerà i messaggi provenienti da questi indirizzi, neppure se hanno un alto valore SCL.

Il SP2 parte da queste solide fondamenta aggiornando diverse componenti antispam e includendo una nuova release di IMF. Per esempio, il SP2 ora esamina le connessioni SMTP in entrata per assicurarsi che il partner connesso

stia inviando messaggi correttamente formattati così che utenti maligni non possano trasmettere messaggi che includono caratteri a 8-bit nel flusso RFC2821 (una tattica comunemente usata per difendersi dai filtri). Inoltre, il SP2 risponde ai comandi SMTP VRFY, che corrispondenti remoti utilizzano per verificare gli indirizzi di posta, ma Exchange non fornisce informazioni in quanto gli spammer utilizzano spesso questi comandi per ottenere la conferma che l'indirizzo email sia valido. Exchange non supporta il comando SMTP EXPN, che interroga un server riguardo alla membership delle liste di distribuzione (DL, Distribution List).

Se il messaggio passa il test di connessione e viene accettato, Exchange può allora applicare il recipient filtering al fine di prevenire che i messaggi vengano recapitati a determinati indirizzi. Il recipient filtering può fermare i messaggi inviati ad indirizzi inesistenti, ma gli spammer potrebbero cercare di costruire una rubrica di indirizzi inviando i messaggi ad una serie di indirizzi e monitorando i risultati per verificare quali di questi sono validi. Il SP2 supporta una tecnica denominata SMTP command tarpitting, la quale consente di configurare Exchange in modo da implementare un delay (ritardo) in secondi nella risposta a un comando "Rcpt To:" se un utente remoto cerca di raccogliere indirizzi. Come risultato, gli spammer troveranno i propri attacchi rallentati al punto da non ottenere alcun risultato, e si dirigeranno probabilmente verso un bersaglio più facile.

La grande notizia per l'aggiornamento di IMF è il modo in cui può rilevare e sopprimere messaggi che contengono attacchi phishing (NOTA: Il phishing è un

tipo di frode che si attua tramite posta elettronica allo scopo di rubare i dati di identificazione di un utente. Viene attuato tramite invio di false email che invitano l'utente a ri-effettuare una registrazione consegnando di fatto i propri dati identificativi a qualcuno che non è quello che appare - un istituto di credito, in genere). L'IMF aggiornato ora contiene test che misurano se un messaggio ha caratteristiche di phishing e imposta un valore di Phishing Confidence Level (PCL), che si può utilizzare come parametro per accettare o scartare i messaggi. Più alto è il valore PCL, e più il messaggio ha origine dubbia.

Il valore PCL, e più il messaggio ha origine dubbia.

L'IMF inoltre supporta Sender ID, una architettura standard che è progettata per contare lo spoofing email dei domini nei quali uno spammer genera messaggi che sembrano essere originati da un dominio legittimo come Microsoft.com.

Sender ID dipende dai record DNS dell'organizzazione con i dettagli relativi ai server di posta che trasmettono messaggi per il proprio dominio; i server che supportano Sender ID possono utilizzare questa informazione per controllare se un messaggio proviene da una fonte legittima. È possibile decidere se cancellare i messaggi illegittimi, rifiutarli e inviare un nondelivery report (NDR), o accettarli con uno status che fa sì che IMF incrementi il valore SCL per il messaggio. L'impostazione di default è Accept, ma qualsiasi messaggio ricevuto che viene marcato come proveniente da sorgente illegittima ha un valore SCL calcolato

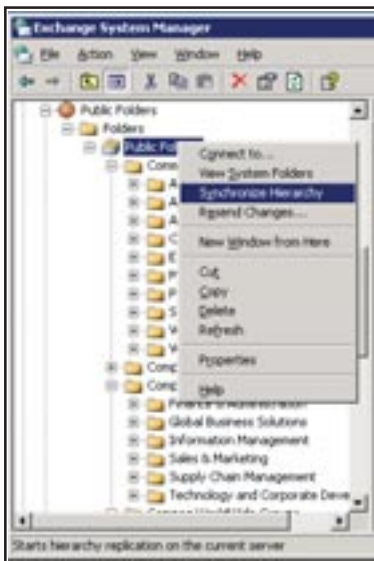


Figura 3

dall'IMF molto alto e verrà soppresso in ogni caso, probabilmente dal filtro junk-mail del recipient. Per maggiori informazioni riguardo all'architettura di Sender ID vedere all'indirizzo <http://www.microsoft.com/mscorp/safety/technologies/senderid/default.aspx>.

L'IMF non supporta gli ambienti clusterizzati, ma questo non è un gran danno. La maggior parte dei server che partecipano alle operazioni di "igienizzazione" sono server

standalone e non fanno molte altre cose oltre al filtrare i messaggi di posta in entrata alla ricerca di spam e virus, mentre invece i cluster tendono ad essere usati per i server di posta. Per fare un confronto, la ridondanza e la disponibilità di un server di pulizia per i messaggi di posta è generalmente accompagnata da un bilanciamento del carico tra sistemi multipli.

### Il nuovo OAB

Per molte aziende, il nuovo formato Offline Address Book (OAB) introdotto in Exchange 2003 opera molto bene con i client Outlook che vengono eseguiti in cached mode. Ad ogni modo, le organizzazioni più grandi hanno incontrato difficoltà che potevano rallentare i server con le richieste dei client per il download degli OAB, così il SP2 introduce un formato OAB rivisitato (OAB v4) e un nuovo meccanismo di aggiornamento che rileva lo stato di carico dei server.

I client Outlook richiedono un download completo dell'OAB se è stata modificata una percentuale dell'OAB maggiore di un dato valore. Questo valore è impostato di default al 12,5 per cento, o un ottavo, delle voci presenti nell'OAB. Ad ogni modo, anche una piccola modifica come l'aggiornamento di una singola cifra in un numero di telefono potrebbe far sì che Exchange consideri il record modificato.

Ogni azienda che effettua l'aggiornamento da Exchange 5.5, consolida i server, aggiunge o rimuove gruppi amministrativi, od esegue tipiche operazioni sulla posta elettronica (come spostare mailbox tra i server, modificare fisicamente gli uffici, aggiungere un nuovo SMTP o altri indirizzi di proxy per la posta), genera un largo numero di modifiche all'OAB. In questi casi, il valore di soglia del 12,5 per cento può essere sorpassato facilmente, causando molte richieste di download completo da parte dei client e di conseguenza sovraccaricando i server.

Le piccole aziende generano piccoli OAB, così i loro server hanno meno probabilità di incorrere in questi problemi, ma le larghe organizzazioni devono porre maggior attenzione a questo, e perlopiù devono evitare di implementare Outlook 2003 in Cached Exchange Mode.

La risposta di Microsoft è stata quella di introdurre una compressione LZX per velocizzare il trasferimento dei dati OAB tra il server e il client (questa è la stessa tecnologia che i client utilizzano per scaricare gli aggiornamenti di Windows dal Web) e un meccanismo denominato Binpatch, che utilizza la Binary Delta Compression (BDC) per applicare gli aggiornamenti ai file OAB dei client. In aggiunta, i client ora generano il loro proprio ordinamento per gli ANR e i file ricercati basandosi sulle impostazioni locali impostate sui PC piuttosto che dipendere da quelle locali supportate dal server. A causa della modifica dei client, solo i PC che eseguono Outlook 2003 SP2 possono scaricare od utilizzare i file OAB v4; i client che eseguono Outlook 2003 o Outlook 2003 SP1 continueranno ad usare il formato OAB v3.

Durante il processo di generazione dell'OAB, i server SP2 generano due nuovi file denominati Binpatch.oab e Data.oab ed archiviano questi file nella cartella pubblica di sistema OAB v4, come mostrato dalla Figura 2.

Ogni file Binpatch.pab contiene le modifiche effettuate dall'ultima generazione dell'OAB, od ogni modifica alla GAL avvenuta durante il giorno. Le precedenti versioni di OAB modificavano i file che contenevano record completamente aggiornati, anche se questa modifica era stata minima, ma i nuovi file contengono le patch binarie che i client Outlook 2003 SP2 possono utilizzare per creare un aggiornato OAB.

Per esempio, il file OAB v3 completo mostrato nella Figura 2 è di 66 MB, e l'aggiornamento del 17 agosto è di 1003 KB, mentre le versioni OAB v4 misurano rispettivamente 34 MB e 239 KB. Il risultato è che ora Outlook ha bisogno di scaricare un minor numero di dati rispetto alle versioni precedenti.

Microsoft si aspetta che il nuovo formato OAB e il SP2 possano ridurre considerevolmente il numero di volte che un client effettua una richiesta di download completo. Questi ultimi dovrebbero avvenire solo quando i file OAB non esistono sul client, quando sono danneggiati, o quando il client non ha scaricato aggiornamenti per più di un mese. Un problema minore è rappresentato dal fatto che sebbene il nuovo formato riduca il carico di lavoro del server, dà invece al client un lavoro maggiore nel decomprimere ed applicare i file binari di aggiornamento. Se il proprio PC è già sovraccarico non si noterà questa difficoltà extra e si noterà un rallentamento durante il processo degli OAB.

### Incremento dello Store Size Limit (Standard Edition)

Prima del SP2, il limite per la dimensione delle mailbox nella Standard Edition di Exchange 2003 era di 16 GB. Questo limite era stato fissato ancora con Exchange Server 4.0, così era ovviamente diventato obsoleto ed inappropriato in un mondo nel quale la dimensione media dei messaggi di posta è diventata più grande, la dimensione media dei dischi è aumentata, e il costo per gigabyte è calato enormemente. La risposta di Microsoft è stata quella di incrementare questo limite con il SP2 portandolo a 75 GB.

Nel tempo, Microsoft aggiornerà anche la versione di Exchange inclusa in Microsoft Small Business Server (SBS) 2003 per supportare il nuovo limite, probabilmente con un service pack che verrà rilasciato diversi mesi dopo il rilascio del SP2 di Exchange Server 2003. Avere un limite molto più alto per l'archiviazione è una buona cosa, ma anche l'incre-

## Exchange 2003 Service Pack 2

mento di 59 GB non è rapportato alla nuova dimensione media dei messaggi di posta. Nel 1996, un messaggio in media pesava 10 KB, mentre ora 100 KB o più. Come risultato, giusto per proporzione, Microsoft avrebbe potuto incrementare il limite portandolo a 160 GB o più. Si potranno trovare alcune discussioni interessanti riguardo ai nuovi limiti all'indirizzo <http://blogs.technet.com/exchange/archives/2005/09/14/410821.aspx>.

### Modifiche alla gestione delle Public Folder

Le Public Folder (o cartelle pubbliche) rappresentano per tutti la parte favorita di Exchange.

Alcune aziende trovano che le cartelle pubbliche facciano un buon lavoro per quelle che sono le proprie necessità, ma altre hanno scoperto che esistono opzioni migliori. Per esempio, Microsoft SharePoint Portal Server e i SharePoint Team Services sono popolari alternative per le organizzazioni che cercano strumenti di collaborazione.

Microsoft si sta chiaramente allontanando dalle Public Folders, ed eventualmente lascerà questa caratteristica probabilmente non appena si potranno avere strumenti di migrazione solidi per spostare tutti i dati gestiti tramite le cartelle pubbliche verso le nuove piattaforme. Nel frattempo, il SP2 cerca di risolvere alcuni dei problemi che angustiano gli amministratori. È possibile ora utilizzare Exchange System Manager (ESM) per arrestare e riprendere l'attività di replica dei contenuti (ma solo su server che eseguono almeno il SP2), forzare la replica della gerarchia delle public folder (come mostrato nella Figura 3), ed aggiornare i permessi sulle cartelle, ottenendo la propagazione di questi attraverso tutta la gerarchia di cartelle. Exchange registra la cancellazione delle cartelle pubbliche nell'Application Log, così che si possa determinare chi ha cancellato una cartella eventualmente scomparsa.

### Modifiche benvenute

Il SP2 non introduce altre modifiche di tipo immediato, ma include molte altre migliorie che renderanno la vita più facile agli amministratori di Exchange, ed anche agli utenti. L'aggiornamento è semplice da applicare e questo consentirà una rapida implementazione. Come sempre, occorre assicurarsi di avere del tempo per testare il SP2 nel proprio ambiente di produzione prima di implementarlo in tutta l'organizzazione. Buon divertimento.

L'autore

**Tony Redmond** è un contributing editor di *Windows IT Pro*, un senior technical editor di *Exchange & Outlook Administrator*, vice presidente e CIO di *HP Services*, e autore di *Microsoft Exchange Server 2003 with SP1* (Digital Press).

### Impostazione delle policy per i dispositivi mobili

Exchange archivia le impostazioni relative alle policy per i dispositivi mobili nell'attributo `msExchOmaExtendedProperties` nei propri dati di configurazione nell'Active Directory (AD). L'attributo è una stringa multivalore che include un blob XML

che contiene gli elementi di policy da applicare ai dispositivi mobili (il blob XML è un formato compreso dai dispositivi mobili). Ogni volta che un dispositivo mobile cerca di eseguire un comando `ActiveSync`, questo invia la sua policy key nell'istanza `HTTP` della richiesta. Exchange confronta la policy key del dispositivo con il proprio valore (che viene archiviata nella porzione `PolicyKey` di `msExchOmaExtendedProperties`), e se i due valori non corrispondono, allora Exchange restituisce un codice `HTTP 449` che fa sì che il dispositivo prenda le impostazioni di policy aggiornate e le applichi prima di continuare la sincronizzazione. È possibile far sì che i dispositivi aggiornino le loro impostazioni di policy in modo regolare impostando un valore per il parametro `Refresh settings in the device (hours)`. Exchange mantiene le impostazioni relative alle policy (in minuti: l'interfaccia grafica mostra il valore in ore) nella stringa `PolicyDataRefreshInterval` nell'attributo `msExchOmaExtendedProperties` e la marcatura relativa al momento in cui la policy è stata inviata con successo al dispositivo nella mailbox dell'utente. Se si imposta una policy di refresh, provare ad impostare un valore come 144 (una settimana) che non causa continui tentativi di aggiornamento di policy non modificate.

L'attributo `msExchOmaExtendedProperties` inoltre include una impostazione denominata `Policy DataSalt`, in cui alcuni byte casuali sono codificati in formato `base64`. Exchange usa questi byte per creare un hash della marcatura relativa all'ultimo aggiornamento riuscito ed archivia questo valore assieme alla marcatura nella mailbox dell'utente. Gli utenti non conoscono quali byte sono stati usati, così non possono scrivere applicazioni che reimpostino la marcatura nella propria mailbox poiché non sono in grado di rigenerare l'hash.

È possibile, inavvertitamente, far sì che Exchange ripulisca (wipe) il dispositivo rispondendo ad una richiesta di digitazione di PIN. Per esempio, alcuni dispositivi reimpostano se stessi per risolvere problemi hardware o software e richiedono l'inserimento di un PIN prima che il dispositivo possa riconnettersi ad Exchange. Se la reimpostazione avviene quando il dispositivo è in tasca, probabilmente non si noterà che sta richiedendo un PIN, e se non si è bloccato il dispositivo medesimo, il movimento di questo nella tasca causerà la pressione di vari pulsanti, digitando PIN errati e causando una serie di tentativi che non avranno successo. Un'altra situazione comune che può causare la reimpostazione è dovuta a quando un bambino lo prende per giocare, senza naturalmente avere la cognizione di cosa sia un PIN, ma semplicemente per premere i tasti della tastiera. Exchange per questo motivo include una impostazione `CodeWordFrequency` che è impostato a metà del valore di `DeviceWipeThreshold`. Quando il dispositivo raggiunge un numero di PIN falliti equivalente al valore `CodeWipeFrequency`, effettua una richiesta per una parola in codice. Una parola in codice non è un codice, ma solo una richiesta per l'utente di digitare il valore mostrato dal dispositivo per confermare che sta realmente cercando di inserire un PIN. I tasti premeuti inavvertitamente non possono generare il codice corretto, e la maggior parte dei bambini non sono analogamente in grado di farlo, così il meccanismo previene il fatto che Exchange possa ripulire o cancellare il dispositivo a meno che non sia necessario.

**Tony Redmond**