

RE: Sendmail – IMAP–UW – Cyrus–SASL2 – SMTPAUTH problems

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2006-02/msg01852.html>

- *From:* "Greg Groth" <ggroth99@xxxxxxxxxxxx>
 - *Date:* Sun, 19 Feb 2006 12:43:03 –0600
-

First, thank you for your reply.

Second, I have figured out the problem of not being able to delete IMAP folders in Thunderbird. Apparently this is a client–side issue, not a server one. The answer is to unsubscribe the trash folder in Thunderbird. After unsubscribing, it still appears and operates normally, and you are then able to delete folders. I found the answer in forums regarding older versions of Mozilla Mail, which is why nothing turned up on a search for Thunderbird. Not sure of the exact cause, or if this indeed a bug or just something I missed in the documentation, but it works now.

From: "Ted Mittelstaedt" <tedm@xxxxxxxxxxxxxxxxxxxx>
To: "Greg Groth" <ggroth99@xxxxxxxxxxxx>, <joe@xxxxxxxxxxxxxxxxxxxx>
CC: <freebsd-questions@xxxxxxxxxxxx>
Subject: RE: Sendmail – IMAP–UW – Cyrus–SASL2 – SMTPAUTH problems
Date: Fri, 17 Feb 2006 04:11:15 –0800

Hi Greg,

It is true there's a lot of software available but I have found over the years that a lot of the packages are good, and will work equally well on the back end. Most of the older ones have matured to the point that a rather common selection criteria is "I chose that because that's what all my friends are running"

You really won't know what works the best unless you try all of the packages, and nobody has the time for that. So what you have to do is just pick one based on whatever sketchy research you turn up and spend some time on it, after a few months you will know if it's going to work for you or not. Most times it will work OK for you so your choice becomes one of which is better: knowing a few packages well, or a lot of packages not very well.

A hobbyist/amateur is better off knowing a lot of packages not very well, because their fun is in trying out new things and learning how different things are done. But a manager of a production system is in the other boat, they need to know a few packages very, very well. You need to be aware of which kind of person your taking advice from.

RE: Sendmail – IMAP–UW – Cyrus–SASL2 – SMTPAUTH problems

IMHO RedHat isn't much good unless you go the full meal deal and buy a support contract from RedHat. If you are upgrading from old 7/9 RH and you want to keep the RH universe, and you don't want to buy into support, then go to CentOS.

RedHat was becoming a pain to deal with. It seemed to me, and this is just my opinion and worth the paper this email is printed on, that a lot of the software had been tweaked to where common solutions to common problems didn't work, and solutions had to be found for the specific version of RedHat I was using. Not that there's anything morally wrong with RedHat doing this, I just found it a pain when looking for answers to problems.

Frankly I feel that one of the big problems with Linux right now is they are missing the boat on SATA RAID big time, and I mean really, really big time. Most server-quality motherboards these days come with RAID0/1 SATA chipsets, and disk drives are so cheap now that even people putting together little crummy servers are going mirrored SATA disks. But Linux has ignored this, claiming it's the responsibility of the manufacturers to write drivers, and most of them haven't. The Linux people all seem to think it's perfectly OK to go buy an Intel motherboard with onboard ICH7R RAID and disable that and drop \$200 into a 3ware RAID card and plug that into the motherboard if you have the nerve to run RAID on anything other than a Real SCSI RAID array. Fine, let them delude themselves, it just puts Linux further and further away from the server arena. Most Linux distros have terrible or nonexistent support for Promise RAID cards as well, once again, really short-sighted.

I don't know much on this subject I'm afraid, but I'm about to get into this because KnoppMyth apparently has issues running a SATA drive as a primary boot device. (Off the subject, but I tried getting MythTV running on RedHat FC4, and ran into too many issues getting it running to continue on that route).

Anyway, getting back to your situation. We run SSL imap and pop3, with uw–imap. I recommend this route since it allows people to hit their mailbox with both pop3 and imap and not get a lot of funny messages about popping down the placeholder message. uw–imap used to have a problem with really big e-mails years ago, it would swap itself to death building the tempfiles, this was fixed years ago.

I did solve my SSL problem by recompiling UW–IMAP and Sendmail without SSL, and installing stunnel. Everything is working the way I want it configured. Hopefully there won't be any scalability issues, but I don't expect any in our tiny environment.

We run SMTP AUTH but we don't run SSL SMTP. Why? Because way too many customers out there still run elderly versions of e-mail clients that can't handle SSL SMTP. If I was doing up a mailserver for a corporation I might consider SSL SMTP, but frankly, I think the idea that someone's going to sniff your password is highly overrated. Most people set their e-mail clients up to permanently save the password so there goes your security right out the window. And your foolish if you let people use the same userID and password for the mailserver. What I'm doing these days is setting up the users with full name userIDs. For example userID ted.mittelstaedt, password goglafrich. Or some such. e-mail addy then becomes ted.mittelstaedt@xxxxxxxxxxxxx. Needless to say this userID is only present on the mailserver and nowhere else, same with the password. A cracker already can get the targets full name by calling the companies directory assistance line or off their business card, so they gain no new information item by breaking this userID. And these userIDs and passwords are too long to be susceptible to a spammers dictionary attack. Particularly if the employee is popping the mail off the server, if the attacker gets the userID and password they are generally going to only be able to get a few pieces of mail out of the server.

Decision makers above me decided that SSL is a "good thing", and I can't really argue with that. I doubt that sniffing is that big of a deal as well, we used POP–before–SMTP for the last 6 years without a problem (knock on wood). I'm not going to argue with "the powers that be" though, but I'm not going to kill myself getting Microsoft to work correctly. Internally we are switching to Thunderbird, not because of the SSL issues, but due to the lack of filtering rules for IMAP in Outlook Express. Outlook was discarded as an option because it did way more than we needed it to do, and proved to be confusing to our end users. My only other issue is a handful of accounts that connect remotely, and I believe use Outlook Express. They do not understand, and don't care to understand, technical issues revolving email, and will be quite satisfied on ports 110, 143 and 25.

You can argue it however you want but today with ethernet switches being as cheap as they are, even a malevolent employee on a corporate network is going to have a hard time sniffing passwords on a decent net. Anything they do to convince the switches to stop being switches is going to bring the network to it's knees and attract a lot of attention quick. I discount most of those scenarios as provable in the lab, but useless in real life.

I'm the only one in the office that knows that a switch is something other than the thing to turn the lights on and off, so it's not really an issue.

RE: Sendmail – IMAP–UW – Cyrus–SASL2 – SMTPAUTH problems

In real life the preferred attack vector is to insert a keyboard logger on the users desktop, which is rediculously easy, all you have to do is wait for Microsoft's patch tuesday, reverse engineer the patches to see what they patched, and write a worm to take advantage of that hole, and drop a keyboard logger when it infects. That buypasses all the SSL horseshit and if you want to get fancy you can scan the users system for the outlook files and extract the saved password from outlooks ini files, it's not like Microsoft encrypts it or anything. The worm leaves a back door and you scan the internet looking for the back doors. You will find plenty to keep yourself busy. We see customers that have had this done to them almost every day. By contrast I've never once seen a customer with an employee who wasn't a network administrator that knew what a packet sniffer was and how to use it. As far as WEP is concerned the trade rags constantly claim how insecure it is and how easy it is to brute force crack and obtain keys – once again, this is laboratory stuff, it's not visible in the real world. In the real world there are so many unsecured wireless networks in the average city that a cracker that turns on a wireless promiscuous sniffer is going to see 3–4 networks, 3/4 of which are wide open, no matter where they go. What incentive is there to crack? And that's just the people dumb enough to leave SSID broadcasting turned on.

Again not an issue, half the users can't plug in a phone, much less a keyboard logger.

Anyway, one last note for you. No matter what you use, just about all the instructions out there tell you to create a self–signed certificate for imap/ssl smtp/etc. do not do this! The Microsoft e–mail clients can't handle this. What you want to do is create a root certificate, then create certificates for all your https servers, your secure imap and pop servers, your ssl smtp, you name it. Sign all of them with the root CA. Then, insert the root CA into the list of trusted root CA's in the Microsoft browser on the client, and from that point on the Microsoft clients don't think you are running self–signed certificates anymore and do not whine, bitch and complain and you don't have to fumble around inserting a bunch of self–signed certificates for every little service you run into all your clients. That is for example how you get Outlook to speak SSL without paying Verisign. A lot of people fooling with self–signed certs have discovered to their dismay that only outlook express can have a self–signed cert installed, regular outlook from ms office cannot.

You may not care for this, but I did use a self–signed certificate. Thunderbird has no problems, and my Outlook Express users aren't going to use SSL anyway. By having SSL as an option using stunnel, and still leaving the standard ports open, I have been able to fulfill the needs and desires set by those above me and should avoid any issues with MS products.

RE: Sendmail – IMAP–UW – Cyrus–SASL2 – SMTPAUTH problems

Ted

Again, many thanks for your insight. It's difficult to find practical advice for noobs like myself that doesn't immediately jump into arcane technical discussions that I have difficulty following.

Now, off to do battle with Mailscanner.

Best regards,
Greg Groth

Express yourself instantly with MSN Messenger! Download today – it's FREE!
<http://messenger.msn.click-url.com/go/onm00200471ave/direct/01/>

freebsd-questions@xxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>
To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"