

CERN COMPUTER NEWSLETTER

Volume XXXIX, issue 1

September–October 2004

Contents

Editorial

CNL changes with the times 1

Announcements & news

CERN Courier gains a new computing section 2

IT bookshop caters for our computing needs 2

CERN bookshop and library plan book fair for October 2

Recruitment process goes electronic 3

Three software support contracts are currently being reviewed 3

Restrictions apply to software for personal and professional use 3

Desktop computing

Accessing NICE from outside CERN 4

Outlook 2003 offers new benefits 6

Technical brief

CERN has some new recipes for fighting growing volume of spam 7

Internet services & network

Alternative SMTP server on port 2525 will use CERN mail servers remotely 9

Reverse-DNS configuration of the IP server is crucial 9

Information corner

Questions and answers from the Helpdesk 10

Recent changes to CERN's IT services 10

Calendar 10

Editors Nicole Crémel and Hannelore Hämmerle, CERN IT Department, 1211 Geneva 23, Switzerland. E-mail: cnl.editor@cern.ch. Fax: +41 (22) 7677155. Web: cerncourier.com (link CNL).

Advisory board Wolfgang von Rüden (head of IT Department), François Grey (IT Communication team leader), Christine Sutton (CERN Courier editor), Mick Draper (group leader, User and Document Services).

Produced for CERN by Institute of Physics Publishing
Dirac House, Temple Back, Bristol BS1 6BE, UK. Tel: +44 (0)117 929 7481.
E-mail: chris.thomas@iop.org. Fax: +44 (0)117 920 0733. Web: iop.org.

Published by CERN IT Department

©2004 CERN

The contents of this newsletter do not necessarily represent the views of CERN management.



CNL changes with the times



The new machine room in the basement of CERN's computer centre.

For the past 38 years the IT Department has been publishing the CERN Computer Newsletter (CNL), which covers topics of interest to the department, to CERN users and also to a wider sphere of IT professionals and computer scientists.

As part of an effort to improve the communications between the department and users around the world, a plan for improving the content and layout of CNL and for increasing its readership was proposed to the management.

The decision was:

- to include a new section, "Computing News", in alternate issues of *CERN Courier*, starting in September 2004;
- to provide a new online version of CNL with a downloadable PDF (this newsletter).

The "Computing News" section in *CERN Courier* will contain short or medium-sized articles to address scientific computing in the broadest sense, or more specific articles on Grid projects such as the LHC Computing Grid (LCG) and EGEE.

The new online version of CNL will be more technical and CERN IT specific, but we still wish to include some scientific computing articles that will be of general interest to CERN users.

For both publications the technical work will be done by the publisher of *CERN Courier* and the online version of CNL will be available from the website at <http://www.cerncourier.com/>.

We hope you enjoy the first issue of this new version of CNL. We will be very glad to receive your comments, which should be e-mailed to the CNL editors (e-mail: cnl.editor@cern.ch).

**Nicole Crémel and Hannelore Hämmerle, CNL editors,
IT/Communication Services**

CERN Courier gains a new computing section

The articles that are listed below have been published in the September 2004 issue of *CERN Courier*, which contains the new Computing News section. Full-text articles can also be found on the *CERN Courier* website at <http://www.cerncourier.com>.

Computing News

● Newsletter changes with the times

Robert Aymar, CERN director-general, about the new computing section in *CERN Courier*.

● CERN's computer centre gets ready for LHC

Status and plans concerning the upgrade of the CERN computer centre.

● D0 goes offsite for more power

Re-examining huge amounts of collision data at several remote sites.

● Farm offers real-time event reconstruction

Physics analysis at the Belle experiment.

● The Grid gains new dimensions

Recent developments in the LHC Computing Grid project and CERN openlab.

● CERN prepares for Linux changes

Repercussions of a new distribution policy of RedHat.

● Co-operation aims to ease digital divide

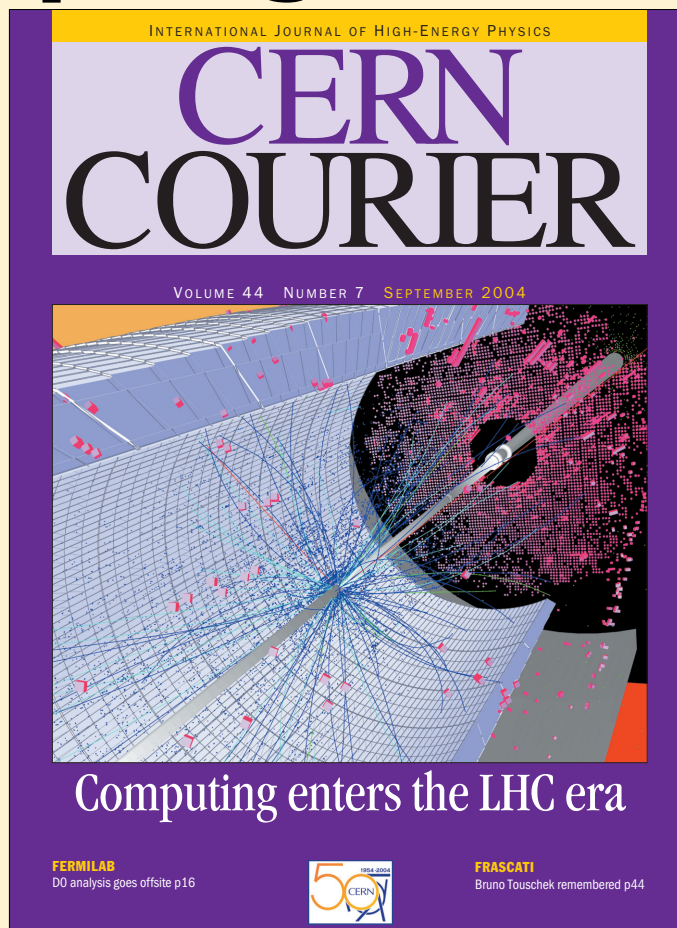
Launch of SEE-GRID project for South-Eastern Europe.

● GridPP collaboration enters a new phase

Following the second stage of the UK's contribution to the LHC Computing Grid.

● Rewind

35 years ago – multitasking CPU.



New IT Products

Calendar of Events

Spam Dossier

● The plague of spam today

Louis McCaul, chief of the Information and Communication Technology Service at the UN in Geneva, is interviewed by Jean Michel Jakobowicz, editor of *UN Special*.

● Alleviating spam's effects

Emmanuel Ormanecy and Alberto Pace of CERN's Internet Services Group describe new spam filter options (see extended version on p7 or CNL online).

Viewpoint

● Going public: a new paradigm

For David P Anderson, project leader of SETI@home, the future of scientific computing is public.

IT bookshop caters for our computing needs

Remember that the CERN IT Computing bookshop moved to a new location earlier this year.

The shop is now situated in Building 513 R-047. CERN users can buy both books and CDs there at discount prices. The service is open on weekdays from 8.30 a.m. to 12.30 p.m. and it can also be contacted by e-mail or phone (e-mail: Bookshop@cern.ch; tel: 74050).

Books are purchased from some 15 publishing houses and the bookshop's catalogue offers a selection of documentation aimed at the range of computing utilities that are currently available at CERN. The service welcomes suggestions from the user community for new acquisitions.

The bookshop's most recent acquisitions are:

● The CD for **Windows XP** and the CD for **Office 2003** (25 Swiss francs each). These are only available while you remain at CERN and a small licence agreement needs to be signed.

● **The Latex Companion** (2nd edition). This book contains a CD for TeXlive, which runs on a PC. This edition has been completely reworked.

● The new **Inside Out Series** of Microsoft books on Office XP tools.

● **C++ for Java Programmers**.

● **The Macintosh Panther Bible**.

● **High performance MySQL**.

● **The Unified Modeling Language Reference Manual**.

● Lots of new pocket editions from the **O'Reilly Series**.

● **OpenGL** reference manual (new edition).

● **Java for Engineers and Scientists** (new edition).

● **Enterprise Java Beans** (new edition).

● **Computer Networks** (new edition).

● **Advanced Unix Programming** (new edition).

The complete list, with all of the relevant information, is compiled regularly and is made available on the CERN network at <http://cdsweb/tools/itbook.py>. This is now integrated into the CERN library system.

Roger Woolnough, IT/UDS

CERN bookshop and library plan book fair for October

The CERN central library, in conjunction with the IT Computing Bookshop, is organizing a bookfair on 28 and 29 October. Some 12 major publishers will be represented and copies of their latest books will be on display, as well as their "key" titles that may

interest CERN. The major topics covered will be computing, physics, technology, mathematics, engineering and popular science.

The following have been invited to this event: Alpha Science, Cambridge University Press, E-books Corporation,

Elsevier, Institute of Physics, McGraw Hill, Microsoft Press, O'Reilly, Oxford University Press, Pearson, Springer, Wiley and World Scientific.

The fair will take place in the main building (Building 60). We look forward to your support of this initiative.

Recruitment process goes electronic

Since January 2004, all vacancy notices from CERN have been made available on the new e-Recruitment website (<http://ert.cern.ch>).

The e-Recruitment Toolkit (e-RT) covers recruitment for CERN staff and for all of the research programmes: technical and doctorate students, fellows and associates.

The Human Resources Department (HR) usually handles around 6000 job applications annually. For some specific recruitment exercises, like the Fellows and Associates Selection Committee, all copies of applications being handled around CERN can represent up to 15 000 pages of paper. This is now fully electronic.

e-RT comprises two main interfaces: the front office, where applicants can register their details, search and apply for vacancies; and the back office, where CERN staff can



Geraldine Ballet, Recruitment Services, prefers e-RT to mountains of paper.

search for candidates, make comments on applications and make selections.

This fully electronic system allows candidates to check the status of their application on a regular basis and e-mails are sent when a candidate has

reached a certain step in the recruitment process.

e-RT is based on iCams, a product developed by Hireserve (<http://www.hireserve.com>) of Fleet, Hampshire, UK. It was chosen after a market survey and call for tender, and was customized by IT-AIS-HR along with the HR Department.

The product is based on Oracle, PL/SQL packages and Java – well known technologies used for years by IT-AIS. It also uses Oracle Intermedia's features to help to search and index thousands of CVs and application forms. So far e-RT has proved very stable, able to cope with a large number of concurrent users (up to hundreds) and easy to maintain.

After only 10 months, e-RT already contains 8500 registered users, of which about 4700 have submitted 13 000 applications to various jobs.

Francois Briard, IT/AIS

Three software support contracts are currently being reviewed

The maintenance support contracts for IRIS Explorer will be cancelled from the beginning of January 2005. Please note that users will still be able to use the currently installed version of IRIS Explorer.

The NAG C library support contract (for sites outside CERN) was terminated in July 2004. This is a support contract only and will not affect the currently installed libraries.

The termination of the TGS OpenInventor contract is also currently under discussion.

For further information, please e-mail: sdt.support@cern.ch. Details of all supported tools can be found on the CERN website at <http://cern.ch/product-support/sdt.html>.

Pete Jones, IT/PS

Restrictions apply to software for personal and professional use

A growing number of computer security incidents that are detected at CERN are caused by software that has been installed for personal use.

Some of the popular "free" software that is available on the Web, for example, can introduce significant security problems, either at the time of installing the software (e.g. when adding spyware or adware) or later as a result of a lack of updates to close security holes.

Software that is not required for a user's professional responsibilities introduces an unnecessary risk and should not be installed or used on computers that are connected to CERN's networks. This includes any computers that are connected to CERN remotely (e.g. via VPN).

Three kinds of non-secure software that violate CERN's Computing Rules, and which are therefore not permitted on CERN's computing or network

facilities, are described below:

- KaZaA and other Peer-to-Peer (P2P) file-sharing software (e.g. Aimster, Bearshare, BitTorrent, Edonkey2000, Eetee, Emule, Gnutella, KaZaA, Limewire, Morpheus, Napigator, Napster, Poisoned, Soulseek and WinMX). For further information, visit <http://cern.ch/security/file-sharing>.

- Skype P2P telephony. The privacy policy of Skype violates CERN's Computing Rules by bypassing firewall protections and offering services to others. For further details on Skype restrictions at CERN, see <http://cern.ch/security/skype>.

- Versions of instant messaging software not configured in CERN's distributions, such as ICQ and so-called "free" downloads, which contain spyware or adware (e.g. Gator and Hotbar) and have introduced privacy violations and/or security exposures.

Caution must be taken when

considering the installation of any software that is not available from CERN's officially supported distributions. You must check the security and legal (e.g. licensing) aspects of the software, including assurance of a timely mechanism for obtaining security updates as well as compliance with CERN's Computing Rules.

A list of some software that is known to cause security or network problems is available at <http://cern.ch/security/software-restrictions/list>.

In addition to security problems, software that has been installed for personal use often creates support problems. The additional software can make problem analysis even more difficult.

Even if the initial installation appears not to have any impact on the correct running of the system, it can cause problems for changes to the system at a

later date. Removing additional software may also require a complete reinstallation of the system from scratch to allow for recovery from all of the changes that were made to the system as a result of the installation.

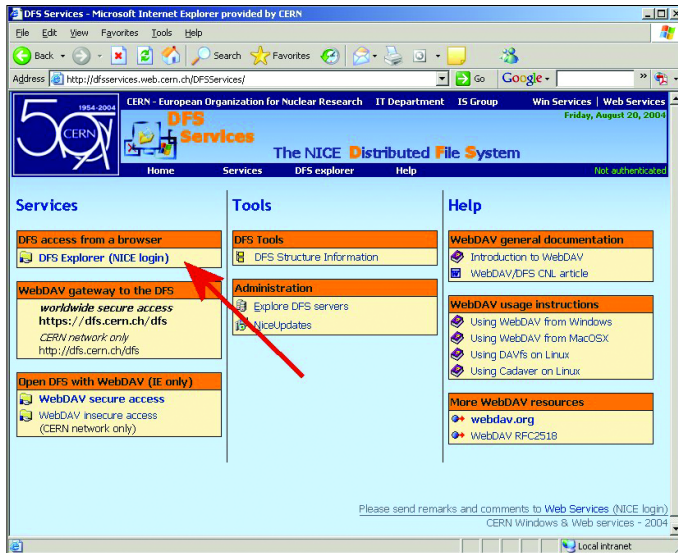
CERN's Computing Rules require users to protect their accounts and computers from unauthorised access. The risk of a break-in to a computer is related to the software installed and how securely it is maintained.

To keep your computer secure:

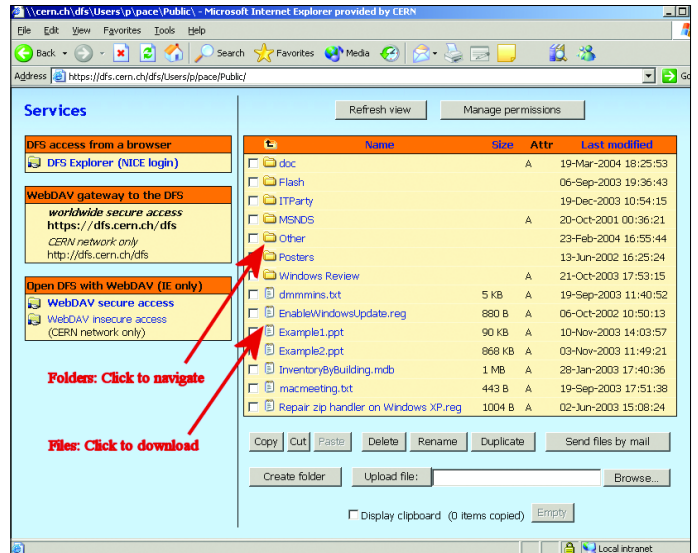
- use a CERN centrally managed system;
- restrict the installed software on the computer to those applications that are required for your professional duties;
- ensure that the operating system and all applications are configured securely and regularly maintained with security updates.

Denise Heagerty, IT/DI and Lionel Cons, IT/CS

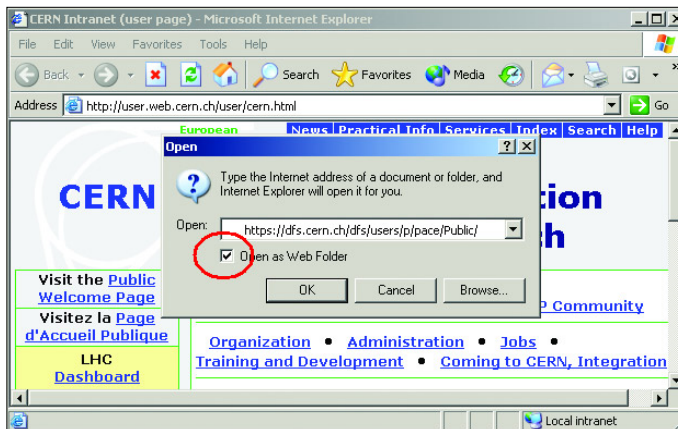
Accessing NICE from outside CERN



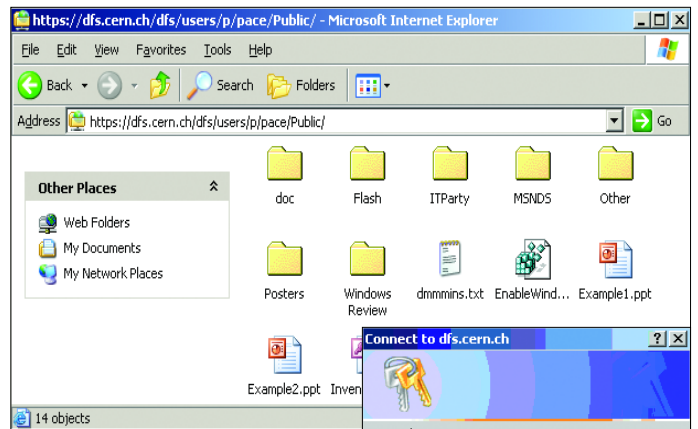
The <http://www.cern.ch/DFSservices> homepage.



The DFS explore, which gives access to DFS files from the Web.



Accessing the DFS files system using Webdav (Windows).



Webdav access from Windows.

Users at CERN were previously using several mechanisms, like ACB or VPN, to access files stored on the NICE Distributed File System (DFS) when they were outside CERN at a distant laboratory or at home. However, complicated set-ups are no longer necessary, and the only requirement today is a Web browser with an Internet connection. Just point your browser to <https://cern.ch/dfs>. You will be redirected to the DFS Services website.

This website provides Web access to the DFS file system in two ways: via the Web browser and the via the WebDAV client.

The browser method

Web browser access is available either by following the DFS Explorer link on the DFS

homepage or by typing the directory name in the address bar, starting with <https://dfs.cern.ch/dfs> (the “s” in https is mandatory – without it you will not be able to connect).

For example <https://dfs.cern.ch/dfs/users/p/pace> is the Web address of the DFS directory, [\\cern.ch/dfs/users/p/pace](https://cern.ch/dfs/users/p/pace).

The user interface is self-explanatory and it allows you to perform all sorts of file manipulations, including deleting, copying, moving and renaming files. It has an embedded clipboard that allows you to copy/cut/paste files within the Web server and to upload small files (up to 3 MB) from the client to the DFS.

To upload a file, first click on “Browse” to select a local file, then click on “Upload this file”

to start the upload process. Larger files can be uploaded with WebDAV (see later).

The webpage also allows you to download files from the DFS to the local computer. To do so, just click on the name of the file that you wish to download and save it to your local disk. Note that the behaviour is slightly different if you click on the name of a folder instead of a file: in this case the folder is opened and will become the new working folder.

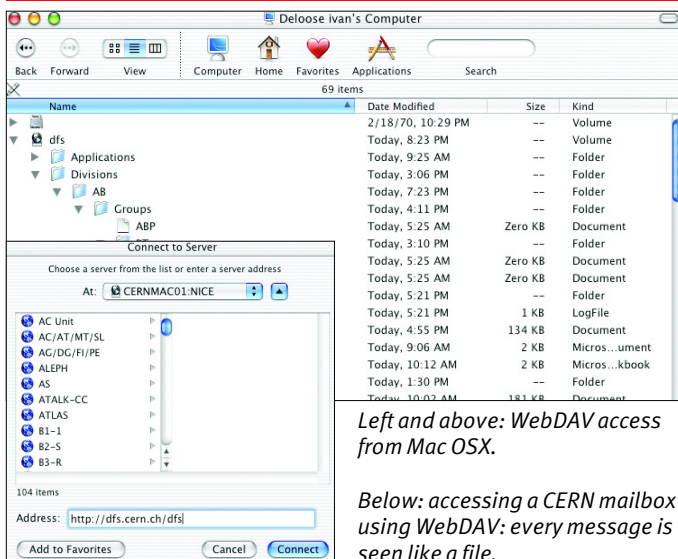
“Send files by email” is a useful tool when you are connected using a slow Internet link (e.g. modem, GSM). It allows you to send a file to a third party without having to download it locally then upload it again to send it by email.

Finally, the “Manage

permissions” button is directly connected to the “Trustee manager”, which allows you to change access permissions to all files and directories for which you have permission control. This makes all required functionalities available to all platforms because the only requirement is a Web browser.

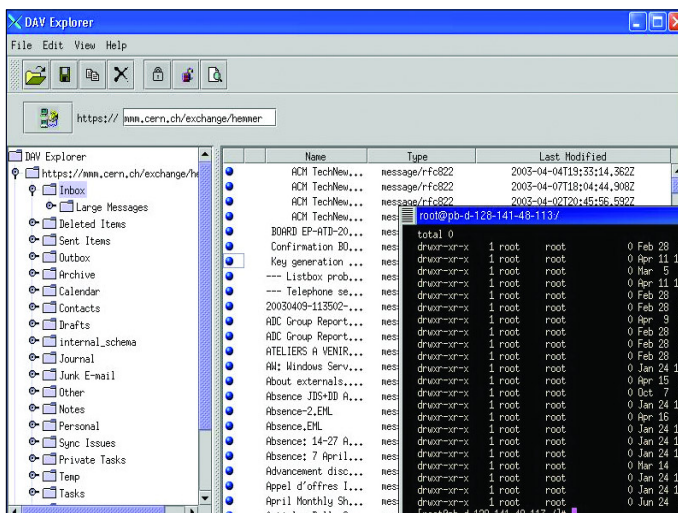
Described above is the maximum that you can do using a simple Web browser. However, for some years now, all major browsers and/or operating systems that have browsers have supported the http extensions for distributed authoring and versioning (WebDAV).

Desktop computing



Left and above: WebDAV access from Mac OSX.

Below: accessing a CERN mailbox using WebDAV: every message is seen like a file.



Using WebDAV

In addition to supporting the normal HTML Web user interface, the site at <https://dfs.cern.ch> also offers a complete implementation of WebDAV. This means that you can mount the entire DFS file system to your local computer outside CERN.

If you are using Windows, the way you achieve this is with the Internet Explorer. Select "File" and then "Open", then tick the "Open as web folder" option after typing the URL of the folder that you want to open.

After the required authentication (with the usual NICE username and password) you can see your DFS files in read/write mode from anywhere in the world. You can drag and drop files and folders from DFS to your local file storage in a seamless way, just as you would copy them from a CD, floppy disk or your home directory. You

can also drag and drop files and folders from your local disk and upload them to the DFS.

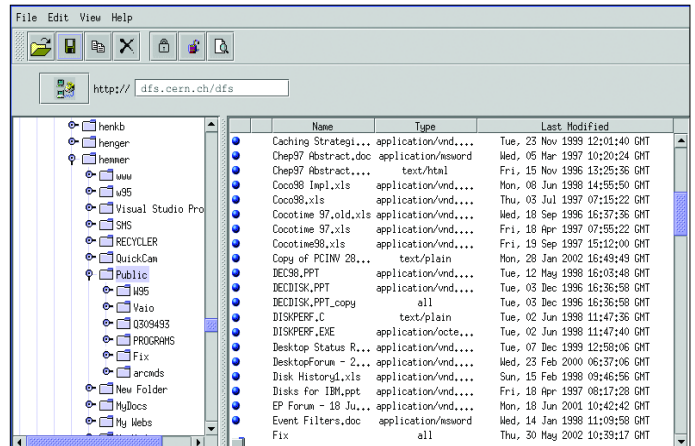
In a similar way you can access the DFS file system through WebDAV from a Mac (using OSX) and from Linux (using DAVExplorer, Cadaver or any other DAV client).

Once the WebDAV file system is available locally you can easily do aggregate operations like copying entire directories with a single mouse click.

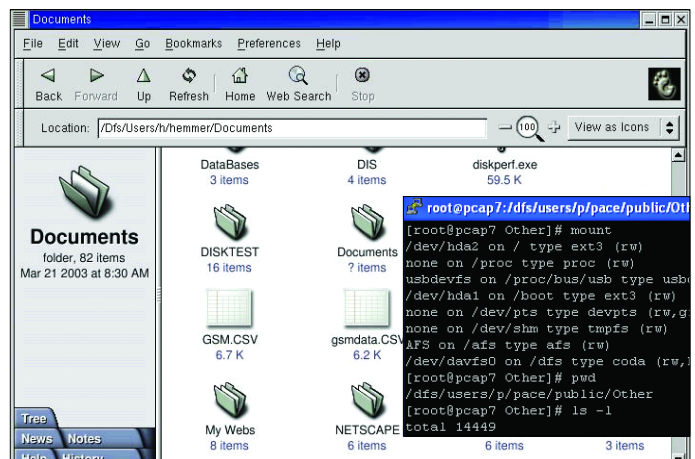
The DFS Services pages at <http://www.cern.ch/dfs> will provide you with some documentation about using WebDAV from different platforms.

Native file access for scripting

There is even more that you can do: mount the DFS file system into the local file space using WebDAV. There are native file system drivers for Windows,



Dav access from Linux using DavExplorer.



Native file access on Linux accessing a WebDAV-mounted DFS file system.

Mac OSX and Linux that allow you to do this.

In particular, Windows XP built-in WebDAV redirector and DAVfs on Linux allow you to mount DFS file systems. This gives you access to the DFS file system natively. The fact that it is mounted as a file system allows you to access files even from the XP command line or the Linux shell. This allows the manipulation of DFS files from scripts (e.g. Perl, VBscript) for any kind of automation.

Having said that it is possible to crossmount the DFS file system into your local file space, be aware that there are some (severe) limitations:

- The current Windows XP WebDAV redirector and the DAVfs driver for Linux support http only – they do not support SSL. Given that only SSL is offered outside CERN, this solution currently works only for computers located on the CERN internal network. However, we do not see any reasons why these drivers should not support

SSL in the near future.

- When a remote file system is mounted, some operating systems start to create indexes of the remote files. In the case of DFS, this could take several days and eat up all of your network bandwidth.
- If the goal is to access DFS from inside CERN, then there are better and faster protocols available (e.g. CIFS/SMB). These are available for Windows, Linux and MAC OSX. Why use http when the native CIFS/SMB is faster, therefore?

Web access is not limited to DFS files – it is also possible to use WebDAV to access all of the files stored on the central Web servers and all mail messages stored in the central mail servers. This opens up several additional possibilities, such as mail clients that read and write mail using simple file access instead of the traditional SMTP/POP/IMAP/MAPI protocols.

Alexandre Lossent, Rafal Otto, Alberto Pace, IT/IS

Outlook 2003 offers new benefits

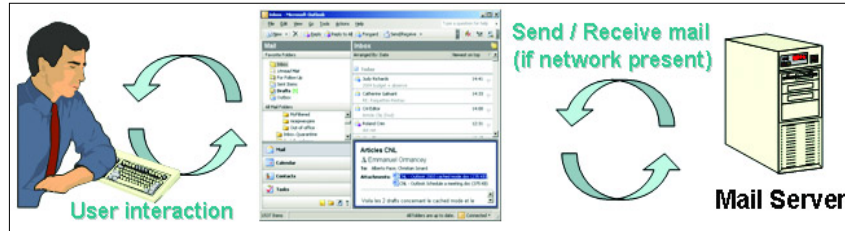


Outlook 2003 is part of the new Microsoft Office 2003 suite. It offers new and enhanced functionality that can improve efficiency and make it easier to collaborate with colleagues.

If Office 2003 is not installed on your machine, check the Win Services page at <http://cern.ch/win/docs/office2003>.

One interesting feature of Outlook 2003 is the cached mode, specially adapted for laptop users, which can replace the offline mode of Outlook XP – not always easy to use.

When Outlook is configured for cached mode, you enjoy better online and offline messaging because a copy of your mailbox is stored on your computer, along with a copy of the address book. The cached mailbox and address book are updated periodically from the CERN mail servers as soon as the



In cached mode, user interaction and message fetching are asynchronous and both independent processes.

network connection is restored.

The principle benefits of using cached mode are:

- it shields the user from troublesome network and server connection issues;
- it facilitates switching between online to offline;
- it automates CERN e-mail address resolution, even offline;
- e-mail messages, agenda and tasks are all available offline.

By caching the user's mailbox and the address book locally, Outlook no longer depends on ongoing network connectivity for access to user information. In addition, users' mailboxes are kept up to date, so if a user disconnects from the network

(e.g. by removing a laptop from a docking station), the latest information is available offline.

In cached mode, user interaction and message fetching are asynchronous and independent processes.

To configure Outlook 2003's cached mode (see box, below):

- log into your Nice account;
- ensure that Outlook 2003 is closed;
- in the Start menu, select Control Panel and then Mail;
- click Show Profiles;
- select Default Profile;
- click Properties (1);
- click E-mail Accounts (2);
- select View or Change Existing E-mail Accounts and

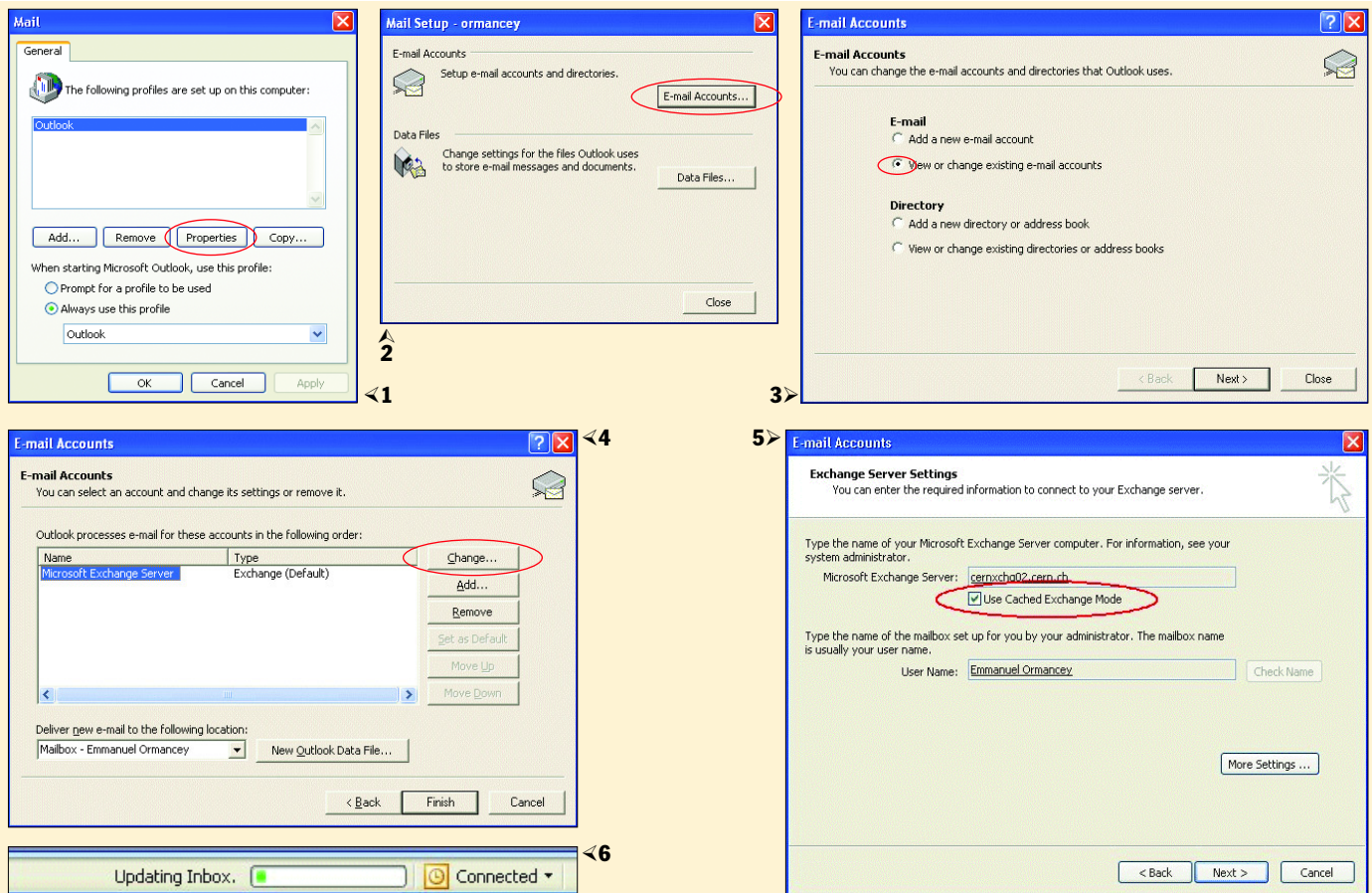
click Next (3);

- select Microsoft Exchange Server and click Change (4);
- check Use Cached Exchange Mode (5);
- Click Next and then Finish.

Once you have configured the cached mode, Outlook 2003 will work as usual but will build a cache in the background. Switching between online and offline is transparent (6):

- if you are connected to CERN's network, Outlook will connect automatically to Mail servers and synchronize the cache;
- if you are disconnected from the network, Outlook works as usual but using the local cache.

Emmanuel Ormancey, IT/IS



CERN has some new recipes for fighting growing volume of spam

Spam Fight

Select the filtering level:

Off

No Spam filtering, all incoming mails will be delivered without filtering.

Low

Obvious Spam mail will be detected and moved to the Cern Spam folder, but some will still arrive in your Inbox.

Medium

Obvious and more "intelligent" Spam mail will be detected and moved to the Cern Spam folder.

High

Nearly all Spam mail will be detected and moved to the Cern Spam folder. Some commercial mailings might be assimilated as Spam, you'll need to check the Cern Spam folder to identify and whitelist them.

UltraHigh

ALL mails will be moved to the Cern Spam folder except:

- Mails with negative score (inside Cern or whitelisted)
- Mails matching whitelist (contacts can be added*)

You'll need to check the Cern Spam folder everyday.
* MMM contacts available with Outlook XP or Webmail.

Recommended

Expiration

Keep spam filtered mails for : 1 month

Move mails to Cern Spam based on character sets:

If you receive mail in foreign character sets (i.e. Chinese), you may want them to be treated as Spam. Note that for example Italian or German languages are part of the "western" character set and can therefore not be filtered.

Chinese mails

Korean mails

Japanese mails

Russian mails

Save

Switch to: [Simple mode][Advanced Mode]

The spam fight configuration tool, available for every CERN mailbox.

In principle, the best approach to tackling spam would be to use newer and more secure mail-transfer protocols that would ensure the traceability of e-mail messages (e.g. by using digitally signed messages and external, common certification authorities).

CERN is constantly evaluating new techniques for handling spam. For international organizations like CERN and the UN, the challenge is to remain open to institutes that, for various reasons, are unable to deploy the latest methods promptly. It may take years for new technologies to become globally available, so people in such organizations can expect to continue to receive spam messages for some time to come, because they can't yet afford to "drop" untraceable mail messages, an important fraction of which are legitimate.

We all know the general advice that everyone should follow to avoid having their inbox flooded with spam: don't publish your e-mail address on public readable websites (forums, newsgroups or any generally indexable electronic publishing mechanism).

Unfortunately, once spammers have obtained a valid e-mail address, there is no way to get it removed. You will receive increasing quantities of unsolicited messages until new e-mail distribution technologies are invented or you change your e-mail address.

The CERN mail gateways receive, on average, 800 000 messages every day with peaks of 1 200 000 messages (see <http://cern.ch/mmms/Services/MailStats.aspx> for the daily SMTP traffic at CERN). More than half of these are immediately deleted with simple rules that detect evident spam, viruses and worms.

Filter works on probability

For the remaining half, the probability of being spam is calculated for each message and it is always delivered to the user's mailbox, either to the inbox folder or to the CERN spam folder, according to the filtering level set by the user. After this additional filtering, the amount of mail that is finally distributed to the inboxes of users normally represents about 20% of the mail initially received via the external gateways.

Spam Fight

The MMM Spam Filter analyses incoming mail and moves those identified as Spam to the folder Cern Spam. Please check this folder occasionally for incorrectly classified mail. Note that the Cern Spam folder will appear only upon reception of the first filtered Spam.

Filtering level:

Set manually

Score: 5

Score above which mails will be moved to Cern Spam folder.

Predefined levels:

Low

15

Medium

10

High

5 Recommended

UltraHigh

1 Extreme filtering

Off

0

Quarantine level:

When a mail is quarantined, it is moved to the Quarantine folder. This folder will contain mails from untrusted sources. Simply fill in your whitelist to allow direct delivery to your Inbox. Recommended value is 0, all mails from outside Cern will be quarantined.

Score from 2 to Filtering Level.

Delete evident Spam:

Delete automatically Evident Spam without moving them to Cern Spam folder.

Mark as read when spam is moved to Cern Spam folder.

Expiration

Keep spam filtered mails for : 1 month

Move mails to Cern Spam based on character sets: [Details]

If you receive mail in foreign character sets (i.e. Chinese), you may want them to be treated as Spam. Note that for example Italian or German languages are part of the "western" character set and can therefore not be filtered.

Chinese mails

Korean mails

Japanese mails

Russian mails

Save

Switch to: [Simple mode][Advanced Mode]

The advanced CERN spam filter configuration.

The "spam fight" tool at CERN (<http://mmm.cern.ch>) allows users to tune their spam filter configuration. They can choose between three levels of filtering, which tune the threshold at which a message with a calculated probability of being spam will be delivered to the CERN spam folder instead of their inbox.

End users should understand the model and tune the anti-spam filter to a level that they estimate to be acceptable: a level set too low will deliver a lot of spam to the inbox; a level too high may deliver legitimate messages to the CERN spam folder (false positives), requiring constant monitoring by the user of the spam folder, which is counterproductive and thereby makes its *raison d'être* void.

The "spam fight" configuration tool is available for every CERN mailbox at

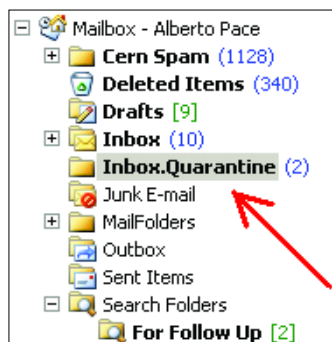
<http://cern.ch/mmms/Tools/Spam/> (authentication required).

As you will see, the general recommendation from the CERN mail team is to set the filtering level to "high". This configuration should suit well the vast majority of CERN users who receive 20–80 spam messages per day.

Users who receive little spam and who would like to minimize the probability of a legitimate e-mail (false positive) being delivered to the spam folder can simply decrease their filtering level to "medium" or "low". However, things get more complicated for users who estimate that the "high" level is not high enough.

What if "high" isn't high enough?

In several individual discussions and also requests via the helpdesk, users have been asking for an additional "very



Inbox.Quarantine folder appears after setting a quarantine level.

high” level to reject spam. Unfortunately, despite several months of tests, a small increase in the filtering threshold produces many false positives. This nonlinearity prevents the filtering threshold from being increased without forcing the user to check the CERN spam folder every day.

The majority of users requesting the “very high” level were owners of highly spammed mailboxes (more than 100 messages per day) and the increased probability of false positives only makes matters worse: the user is forced to check the messages manually in both the CERN spam folder and the inbox. Thus a better solution needed to be found.

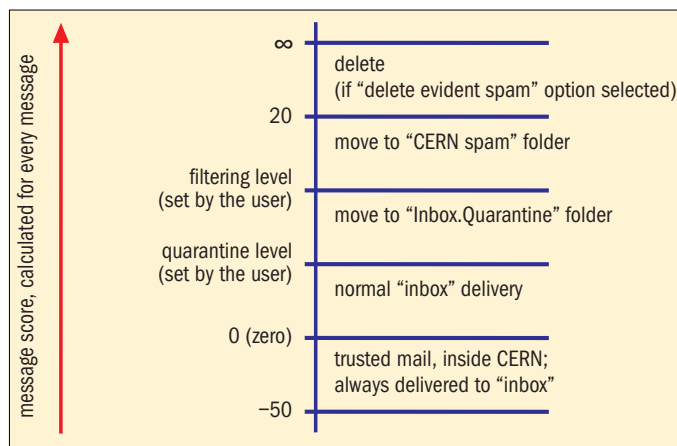
No magic solution

The recent advanced mode set-up of the CERN anti-spam filter gives additional tuning options that should help users who receive more than 150 spam messages per day. These additional parameters allow better management of incoming mail, but there is no magic solution. To benefit from these additional features, it is essential to understand the underlying model, otherwise the risk of losing legitimate mail increases.

The advanced CERN spam filter configuration is available at <http://cern.ch/mmms/Tools/Spam/> (under Advanced Mode) (authentication required).

The advanced set-up of the spam filter keeps all functionalities of the standard filter, namely:

- It allows the user to set the “filtering level”. In addition to the normal interface with “low”, “medium” and “high” levels, any positive numeric integer



Score of messages and action of the spam filter.

```
Received: from cernmx04.cern.ch ([137.138.166.167]) by cern
X-Filter: CERNMX04 SMTPGW CERN Spam Sink v1.0
Received: from mail16.cern.ch ([137.138.138.152]) by cernmx04
Thu, 4 Mar 2004 13:42:31 +0100
X-External: Man_on_the_moon
Keywords: CERN SpamKiller Note: 18
Received: from davinci.ethz.ch ([205.147.247.131]) by mail6
WITH SMTP ID 124CGH05000288; Thu, 4 Mar 2004 13:42:
X-Authentication-Warning: mail6.cern.ch: Host [205.147.247.:
Message-ID: <0a5f01c402af$efd72d8e$1ddcc018@davinci.ethz.ch
From: "Craig Le" <craigle.aw@euireland.ie>
To: alberto.pace@cern.ch, alberto.fusco@cern.ch
Subject: lowest mortgage rates bbswewdazi
Date: Fri, 05 Mar 2004 12:42:07 +0000
```

Mail headers can be displayed by right-clicking the message and then selecting Options.

Check mail in SpamKiller

Checking Item
/Cern Spam/20040305-062414-50754-URGENT REPLY.EML

Checking on cernspam02.cern.ch
Score: **24.718**
Time: 0s203ms

Content analysis details: (24.718 points)
0.418 points: Sent with 'X-Priority' set to high
1.088 points: From: ends in numbers
5 points: Forged hotmail.com 'Received:' header found
1.873 points: Subject is all capitals
1 points: HTML-only mail, with no text version
2 points: Spam phrases score is 03 to 05 (medium)
10 points: Bayesian filter: Spam probability > 0.9
3.339 points: Nigerian scam key phrase

These results may be different from original as some headers have been rewritten during delivery (the X-External check may be false).

MMM Services - Cern IT/IS - 2003

Spam Check button gives details about how the score was calculated.

value is accepted, which allows intermediate filtering.

Messages tagged with a score higher than the “filtering level” threshold are moved to the CERN spam folder.

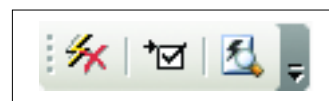
- Setting the filtering level to 0 means that no messages will be moved and that the inbox-based filtering is switched off. However, this option does not disable the message analysis and message tagging with scores, which is therefore useful if alternative, client-side

mechanisms are used for organizing messages.

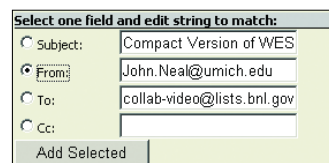
- The “delete evident spam” option remains with identical functionality as for the simple mode. The filtering level for the automatic deletion is set to 20. This value is not configurable by the user.

- Similarly, the language-based detection provides the same functionality as with the simple mode interface.

To address the needs of users receiving large volumes of spam,



CERN Spam Tools toolbar.



Automatic white-listing a sender.

the advanced interface provides a “quarantine level”, which is associated with a third, intermediate folder between the CERN spam folder and the inbox, called the Inbox.Quarantine. This folder appears after setting a quarantine level.

Only messages with a score below the “quarantine level” are delivered to the inbox. Messages with a score between the “filtering level” and the “quarantine level” are moved to the Inbox.Quarantine folder, thereby reducing the burden of sifting through a very large amount of spam in search of a few false positives.

Score of messages

If the quarantine level is activated, the user can even slightly increase the spam filtering level to reduce even further the risks of false positives in the spam folder. Something between 5 (high) and 7 is the recommended setting. For a filtering level of 7 the risk of false positives in the CERN spam folder is so small that you can simply forget about the existence of the CERN spam folder and focus only on the inbox and the Inbox.Quarantine folder. Given that the vast majority of spam will be delivered to the CERN spam folder, this will reduce significantly the number of messages to check manually.

The quarantine level should be set to a very low value, between 0 and 5, where a value of 0 means that everything coming from outside CERN and not explicitly trusted by your white list will be delivered to the Inbox.Quarantine folder. This will simply separate mail from inside CERN and the trusted white list (in the inbox) from external mail, and possibly few spams (in the Inbox.Quarantine).

Values for the quarantine level between 1 and 5 will deliver external messages with very low spam probability to the inbox and the others in the Inbox.Quarantine folder.

If you are using Outlook on a Windows-based desktop as your e-mail client, an additional toolbar called CERN spam tools is preinstalled.

False positives

The first button on the toolbar will delete the selected message and report it as spam so that the filter rules can be improved. This button should only be used for messages that have been delivered to your inbox despite a high filter level. There is strictly no need to report spam messages that have already been identified and tagged as such: just delete them.

The two other buttons are useful to handle false positive messages (i.e. valid messages that have been moved to the CERN spam or the Inbox.Quarantine folders). The middle button allows you to add similar messages to the white list, preventing it from being considered as spam. After clicking the middle button, make sure to select the right criteria (e.g. "from:") and to click "Add Selected".

Clicking on the last button, "Check Spam", displays the spam filter score and explains how it was calculated. This is important if you receive a false positive and want to understand why it was considered spam. This should help you to tune your anti-spam configuration for working more efficiently in these hard times.

The "Spam Check" button gives details about how the score was calculated.

The spam filter score is also stored in the "Keywords:" field of the mail header as "CERN SpamKiller Note". In Outlook, its value can be seen by right-clicking the message and selecting "Options". This is the value that can be used for client-side filtering.

• This is the extended version of an article in the September issue of the *CERN Courier*, which can be accessed at www.cerncourier.com.

Emmanuel Ormancey, Alberto Pace, IT/IS

Alternative SMTP server on port 2525 will use CERN mail servers remotely

For the past few months the number of viruses propagating by mail and running their own SMTP engine has been dramatically increasing.

These viruses work in a simple way: when a computer is infected, the virus scans files on the hard drive, searching for e-mail addresses and sending itself to each collected e-mail address, using another collected address as the sender.

This kind of attack is creating huge performance problems on the network, and for this reason many Internet service providers have closed the SMTP port (25) for outgoing connections from their customers, so that an infected computer cannot propagate viruses to any external e-mail address by itself.

The unfortunate side-effect of taking this measure is that legitimate customers can no

longer connect to external SMTP servers, and particularly to CERN SMTP servers, in order to send out their e-mails.

CERN's mail service has now opened an alternative SMTP server, which is running on port 2525, so as to bypass this problem, where necessary.

Configuration is simple: locate in the mail client configuration the Outgoing Server (SMTP) Settings, set the server name to `smtp.cern.ch` if this is not already done, and change the port from 25 to 2525.

Emmanuel Ormancey, IT/IS

Reverse-DNS configuration of the IP server is crucial

The increasing number of spam and virus attacks inevitably leads to new policies and rules on the CERN mail servers. These are put in place in an effort to maximize the number of unsolicited e-mails that are rejected at the gateway level.

One of the most important rules is the reverse-DNS check on the remote server IP, which was set up on 16 June 2004.

When a remote server connects to CERN SMTP gateways, a reverse-DNS check will be carried out to find its

name from the IP address. If no reverse-DNS is configured, the connection will be refused because the IP is "anonymous".

This rule is one of the most useful for evident spam and virus rejection. A test phase revealed that up to 166 333 unsolicited mails per day could be rejected owing to their lack of a reverse-DNS configuration.

Unfortunately, a few legitimate mails were also rejected, because a number of legitimate mail servers have no reverse DNS, as a result of a

lack of administration.

Facing the growing spam and virus problem, this lack of administration must be solved, because mail services will more and more rely on a trust scenario – otherwise it will become completely unusable.

If you are a mail service administrator sending mail to CERN from outside, make sure that your mail servers are properly configured with a reverse-DNS name for their IP address to avoid their rejection.

Emmanuel Ormancey, IT/IS

The deadline for submissions to the next issue of CNL is

18 October 2004

If you have a burning issue that you'd like to write about, e-mail your contributions to

cnl.editor@cern.ch

Questions and answers from the Helpdesk

Edited by Nicole Crémel

The User Assistance Team in IT/UDS maintains a database for Questions and Answers that have been dealt with by the Computing Helpdesk. This provides many tips on daily computing issues. You can search the database at <http://cern.ch/qa/>.

Below is one example of a Question and Answer (Q&A), which is related to access rights to “public” folders.

Subject

Public folder inaccessible

Question

I want to access my colleague’s public folder where I know there is some data that is important for my work. However, the folder does not seem to have the necessary “read for everyone” permission anymore, and my colleague is absent now. Who can change the access rights?

Answer

The fact that a folder is called “public” does not mean that it has to be available on read-only

for everyone, although this is the default CERN set-up for file systems like AFS or DFS (NICE).

In any case, the user’s decision whether or not to make/leave his/her public folder readable for everyone takes priority.

The CERN official statement concerning access to data belonging to someone who is absent is specifically addressed in Operational Circular No. 5 (OC5) in section IV, relating to

“third party access to users’ accounts and data”. Only the CERN Computer Security Officer (CSO), the service managers for CERN computing facilities and all people expressly authorized by the director-general should have access to information contained in CERN computing facilities, following some conditions expressed in OC5 (like the absence of a user).

The above procedure should therefore be applied in case of

the owner’s absence. Requests should be sent to the CSO from a departmental head or head of experiment with a justification of the serious impact on operations, after which the system responsible will set the necessary access rights.

Related links

- Changing access rights to NICE files (<http://cern.ch/qa/1688>)
- AFS access rights (<http://cern.ch/qa/2490>)

Other general-interest Q&As and their corresponding websites

Windows (NICE - Office) related:

- <http://cern.ch/consult/qa/3263>
- <http://cern.ch/consult/qa/3498>
- <http://cern.ch/consult/qa/3505>
- <http://cern.ch/consult/qa/3509>
- <http://cern.ch/consult/qa/3525>
- <http://cern.ch/consult/qa/3526>

Unix (AFS-Lxplus/Lxbatch) related

- <http://cern.ch/consult/qa/181>
- <http://cern.ch/consult/qa/3520>
- <http://cern.ch/consult/qa/3522>
- <http://cern.ch/consult/qa/3514>

Mail (Outlook-pine-mail services) related

- <http://cern.ch/consult/qa/3518>
- <http://cern.ch/consult/qa/3519>

Windows Terminal Services at CERN
Excel transmits wrong amount of commas to csv file
NICE departmental or workspace share
Office XP at Home: license condition
Weekly virus administrator scan on PC
Windows XP: inconsistent search for file and folders

Login scripts: restore files .tcshrc .login, etc
Batch jobs: access to external network
Passwordless login to Lxplus for ssh connection
Request for AFS password change from AFS.Support

Mailing list rejected with exceeding header counts
Mail never delivered nor in the CERN Spam folder

Recent changes to CERN’s IT services

Changes to services in IT department are announced and published in the Service Status Board at <http://cern.ch/it-servicestatus>. Below are the most recent changes and their dates of posting.

29 July 2004	As of 1 August: external access to the CERN Linux 7.3.X repositories restricted
27	TCP Port 1034 blocked in firewall
20	Move and test stoppage of the old tape management system
12	Until end 2004: delay of file reload
6	Restrictions on software for personal and professional use
2	SMS 2003 client deployment
29 June 2004	Password for local administrator account changed
25	As of end 2004; phase 1, 1 July: ACB to be phased out
15	As of 21 June: Web security scan update
1	As of 15 June: registration of BOOTP and DHCP servers mandatory at CERN
27 May 2004	As of 15 June: CERN SMTP gateway change
27	As of 8 June: planned firewall protections
19	Computing Bookshop move to 513 R-047
6	Adobe Acrobat 6.0 Professional update
20 Apr 2004	Autorouter removal (“fuzzy-matching” for e-mail addresses)
20	No more FTP service on central websites
20	NICE login required to create/manage websites
7	Spam filter activated for all mail users
5 Mar 2004	Removal of Oracle software for Linux and Solaris platforms in AFS
1	Hummingbird Exceed version 9.0
1	E-mail attachments filtered
27 Jan 2004	TCP ports 3127-3198-10080 blocked in firewall
21 Oct 2003	Registration of computers mandatory at CERN
2	The validity of AFS passwords will be limited to a maximum of 1 year
2	Offsite ftp access will be closed and replaced by ssh (scp/sftp)
19 Dec 2003	New names for CERN mailing lists

Calendar

September

20–23 **Global Grid Forum 12: Grids Deployed in the Enterprise**
Brussels, Belgium, www.ggf.org/Meetings/GGF11/GGF12.htm

20–23 **Cluster 2004, IEEE International Conference on Cluster Computing** San Diego, CA, <http://grail.sdsc.edu/cluster2004>

27–1 October **CHEP’04, Computing in High Energy Physics**
Interlaken, Switzerland, www.chep04.org

October

18–22 **HEPIX meeting**
Brookhaven National Laboratory, <http://cern.ch/wwwhepixonmeetings.html>

26 **GridNets 2004 Workshop: Networks for Grid Applications**
San Jose, CA, www.gridnets.org