THE IWR SERVICE CATALOG FOR 2007

That part of IWR that renders a variety of IT services to the organizational units of the Forschungszentrum Karlsruhe is subject to budgeting. This means that the organizational units pay the IWR for the IT infrastructure required with funds from their budget. IWR has listed all IT services offered in a catalog, together with the pertinent costs.

In principle, the costs charged by the IWR for the services are based on the costs IWR has to pay for offering and rendering these services. In most cases, the resulting costs are lower than comparable costs charged on the market outside of the Research Center. In 2007, some costs decreased considerably. Cost increase for the IP addresses, however, could not be avoided.

CPU capacity: A CPU hour of the new vector computer NEC-SX8-8R procured in late 2006 costs EUR 14.00. From the 41st CPU hour, it only costs EUR 6.00 per user and month. The old vector computers VPP5000 and NEC-SX5 will be closed down probably in late February.

IP addresses: Per IP address and month, EUR 20.00 are charged. Here, costs were increased moderately in order to guarantee the extremely good and highly available connection to the internet at FZK in the future. In addition, the FZK network was designed in a redundant manner to increase failsafety, which is associated with additional costs. Large consumers of IP addresses will be given a discount of 10%.

Data archiving: Compared to 2006, all prices were reduced by 50%. Depending on the amount of data, they now range between EUR 0.75 / GB / month and EUR 0.05 / GB / month.

WWW portals: In 2007, the supply of a portal in the Share Point Portal Service only costs EUR 50.00 / month. Compared to the past year, this price was reduced by two thirds.

The detailed IWR service catalog (1) that lists all services of the IWR and all prices can be obtained from the secretary's office of IWR and is also available on the intranet (www.fzk.de/iwr).

Klaus - Peter Mickel, ☎ 5600

CHANGE OF THE SSH ACCESS TO THE FZK INTRANET

SSH (Secure Shell) is a program and protocol, by means of which it is possible to register and execute programs on a remote computer. With the SCP (Secure Copy) program that is part of the SSH protocol family, files can be copied to or from a remote computer. The word "secure" is due to the fact that complete data transmission (in particular the user name and password in registration) is encrypted.

A computer offers the SSH service as a standard on port 22 of the network protocol. Within the framework of the virtual computing center, Forschungszentrum Karlsruhe and the Universität Karlsruhe additionally agreed on port 24 as another SSH port. When installing the central firewall between the internet and FZK intranet, these two ports, i.e. from each computer worldwide to each computer connected to FZK-LAN, were left open. As a response to increasing attacks from the internet aimed at getting unauthorized access to computers via SSH, however, port 22 was blocked in 2002. Port 24 was left open, as the attacks concentrated on the standard port 22.

In view of the constantly increasing number of automated attacks from the internet, general opening of port 24 meanwhile also seems to be highly dangerous. **With the approval of the IT expert group, it was therefore decided to eliminate the general opening of the firewall for access to port 24 on March 26, 2007 and to replace it by a need-tailored connection of individual computers**.

To apply for such a connection, an e-mail noted by the responsible LAN coordinator will be sufficient. In this mail, the IP address of your computer and the desired SSH port (22 or 24) has to be indicated. We recommend to further use port 24, if possible, as it is attacked much less frequently. If access to a few known computers in the internet only is desired (e.g. at a partner institution), connection may be restricted accordingly. For a connection, the computer must have a fixed IP address and the SSH service must be configured safely. For this purpose, we conduct safety tests, where we simulate current attacks from the internet. Information on the safe operation of the SSH service can be found under http://iwr-sicherheit.fzk.de/html/Dienste/SSH.

An alternative to connecting your computer in the firewall is the use of our service "Citrix Web Access". It offers SSH access via a browser. Hence, SSH can be accessed from practically any internet connection. Your computer remains completely protected behind the firewall.

In case of applications and questions related to the firewall, please contact

Firewall@iwr.fzk.de.

Norbert Lehmann, ☎ 6586

SX-8R Vector Computer replaces the Systems Fujitsu/Siemens VPP5000 and NEC SX-5

In early February, we are ready! The SX-8R vector computer will start production operation. As there are certain differences to the VPP5000, a training event with practical exercises will be held for users from February 05 to 07, 2007. In case you wish to register for the training, please contact Frank.Schmitz@iwr.fzk.de. It would be reasonable to first have a user number. If no account for SX-5 or VPP5000 exists, apply for it using the respective form (2).

Agenda

Monday (5.2.)

14:00 -16:00 Theory I (SX architecture overview and basics on vectorization)
coffee break
16:30 – 18:00 Theory II (Vectorization and optimization examples, libraries)

Tuesday (6.2.)

9:00 – 10.30 Theory III (Indirect addressing, performance analysis/tools, tuning your code)
coffee break
10:45 – 12:15 Practice I (Optimization example, work on user codes)
lunch break (local arrangements)
13:00 -14:30 Theory IV (Most important compiler switches)
coffee break
15:00 – 18:00 Practice II (Optimization example, continue work on user codes)

Wednesday (7.2.)

09:00 – 10:30 Theory V (Parallelization – OMP and MPI)
coffee break
11:00 – 12:30 Practice III (Final work on user codes)

Frank Schmitz, ☎ 5632

New Spam Filter at FZK?

In December, we informed you that the new version of our SPAM filter would be installed by the turn of the year. Prior to changing the version, this software was checked in detail and found to be good.

So far for the theory... The software that was then delivered to us did not correspond entirely to the tested software. After installation of the software, massive performance losses occurred.

Of course, we did not want to leave the situation as it was. For this reason, we changed back to the previous software version again and are now in close contact with the supplier for the new version being remedied in order to meet our requirements.

We regret this circumstance and hope that the functionalities promised will be made available soon.

Kerstin Schmidt, ☎ 4501

Spybot Worm Problem at the Forschungszentrum

Since December 11 of last year, a variant of the Spybot worm has infected the intranet of Forschungszentrum Karlsruhe. After it became clear that the worm problem was not limited to individual systems, but rapidly spreaded in the network, we reacted immediately. On the same day, we informed the systems administration staff at the Research Center (NT coordinators, LAN coordinators...). Following an announcement, we disconnected the conspicuous devices from the network and/or backbone on the same evening. Conspicuous means that network traffic initiated by these devices indicated the spreading of the worm. On the following day, it turned out that deworming had not been sustainable for Windows NT systems. The patches and service packs available did not protect against **this** variant of the worm. Development of a corresponding update by Microsoft would have cost EUR 80,000. This solution was presented to the expert group on December 13, discussed, and then rejected. The solution would not have been sustainable, it would have offered protection only against this type of attack.

We therefore offered our help in the upgrade of the systems to the NT coordinators, LAN coordinators, etc. as well as to the heads of the organizational units. Rapid projecting and support of the active directory integration of the organizational units to replace the NT domains also was part of this offer, which has been accepted by many sections. In addition, we conceived an interim solution and offered it a few days later. The NT4 servers from the organizational units communicated with a domain controller of the central active directory services each and with the BK domain, which were then able to serve further clients in their subnetwork. The network name services DNS and WINS were also available in this (quarantine) network. Emergency operation was possible without endangering the operation of the safe systems.

It is clear that not all NT4 systems can be raised to a safe operation system. For this purpose, we offer a technology to connect potentially unsafe devices or devices needing special protection to the FZK intranet (see Information sheet 9/2006 (3)). Please contact us, also when you need information on integration in the central antivirus protection system or on the security update management.

Moreover, it was decided by the IT expert group on January 24, 2007 to focus on the early recognition of and protection against attacks again and to apply for the respective funds. It is intended to classify end devices at FZK (e.g. according to safety criteria) and to release them specifically for applications in our network. A concept is being developed by the IT expert group.

Andreas Lorenz, ☎ 4500

(1) http://www.fzk.de/fzk/idcplg?IdcService=FZK&node=2523
(2) http://hikwww2.fzk.de/hik/orga/hlr/Allgemein/benutzeranmeldung.html
(3) http://hikwww2.fzk.de/hik/info/infoblatt/infoblatt092006.pdf

The IWR staff can be reached by e-mail under givenname.familyname @iwr.fzk.de
For more information on the IWR, click http://www.fzk.de/iwr.
Issued by: Hans Jürgen Rimbach, ☎ 5657