SECURITY ON enCORE

Introduction

When using a cloud or remote compute service, security is probably the most important issue to you. As with any service based around a multi-tenanted environment, there is always the possibility of security breaches, whether intentional or otherwise.
We fully recognise this and appreciate that you may well be running simulations and codes that are business critical and may well contain your intellectual property, or that of your clients. So the enCORE environment has been designed with security as the key feature, and is managed in accordance with best practice to give you peace of mind.

Acceptable Use

All users are required to sign and adhere to a strict AUP. The user agrees NOT to:
a) Upload, store, execute, transmit, or calculate any Content that is unlawful, inappropriate, or any other material OCF or its sub-contractors deems inappropriate or illegal or is illegal by laws of England. If necessary, the user's account and information will be reported or handed over to an enforcement agency.
b) Forge headers or otherwise manipulate identifiers in order to disguise the origin of any Content transmitted through the Service
c) Upload, store, calculate, execute, or transmit any Content that you do not have a right to transmit under any law
d) Upload, store, calculate, execute, or transmit any Content that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party
e) Upload, post, email or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or network equipment
f) Interfere with or disrupt the Service or servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service
g) Intentionally or unintentionally violate any applicable national or international law
h) Engage in any deliberate or unsolicited attacks to the system; such as, but not limited to, any activity outside the user account or user processes without the permission of OCF
i) Engage in accessing, or attempted access or use of or attempted use of the system, computers, software, information, or property of OCF plc or its subcontractor/s without the permission of OCF
We reserve the right to investigate suspected violations of this Acceptable Use Policy.
Should OCF become aware of a possible violation, we may instigate an investigation and gather information from the user and any complaining parties, and in serious cases suspend a user account/s while conducting any such investigation.

User Identity and Login Security

Extremely robust measures are in place to ensure that:

- User identities are kept totally secure
- Only valid, registered users can access the enCORE service

Upon registration via the user management portal, subscribers are required to generate public and private SSH keys to permit user authentication. The public key is registered via the user portal. When the user logs on to enCORE, their computer's SSH implementation encrypts some data using the private key and sends it to enCORE, were it is decrypted and validated using the public key the user provided. This serves as a replacement for user ID/password authentication. Having verified the user identity, the next thing that happens is that SSH negotiates a further encryption protocol for the actual transport of data between enCORE and the user, and this will use a more standard shared, symmetric key in which both ends of the connection use the same key. The reason for this is that symmetric encryption protocols are much less CPU-intensive, so the CPU-intensive bit is reserved for the authentication and initial negotiation only. Nobody else gets to see this symmetric key exchange, so the encrypted communication remains secure. Users may further protect their SSH private key on their machine by creating a "passphrase". This means that every time you use SSH you will be prompted to enter this passphrase, and so that anyone else who manages to copy your private key will be unable to use it unless they also know the passphrase. enCORE is accessed via an encrypted SSH session or, if activated, secure VPN connection. The user interface appears as a standard Linux shell.

Account Permissions

enCORE utilises standard secure Linux file system permissions, which are used to protect shared resources as follows:

- Users can only see their own data within their home directory and the ability to navigate outside their directory is restricted
- Users can only have access to the applications they requested upon registration for the service
- Only OCF has root access to the enCORE compute environment. Under no circumstances are enCORE users granted root access.
- Users do not have direct access to the compute nodes, all computational jobs must be submitted to the relevant queue
- Users do not have visibility of or access to any other user's jobs submitted to the queue system

- The Linux kernel protects users from being able to see each other's processing and memory space.

It is not possible for login nodes to transmit spoofed network traffic. Our firewall infrastructure will not permit a customer to send traffic with a source IP or MAC address other than its own. Port scanning is a violation of the enCORE Acceptable Use Policy and not effective because the enCORE firewall will only allow connections from known, static IPs to the customer's specific login node. Packet sniffing is not possible on enCORE. Users cannot receive or sniff packets that are intended for another customer on the enCORE network. For maximum security, however, users should encrypt any sensitive data.

Data Storage and Management

Data is uploaded to enCORE via encrypted SCP session over SSH. For very large data sets, users may despatch portable disk drives with encrypted data via courier. OCF will ensure secure copying of data into the user's selected directory and will if required return result data in a similar manner.

Scheduling of Compute Jobs

enCORE uses Platform Computing's LSF job scheduler. Users launch jobs from their login node. The job is forwarded to a queue on the physical master node and executed on physical compute nodes. It is not possible for users to directly access either the master node or any compute node. Where users select the dedicated compute nodes option, they will be allocated their own queue, to which only they can submit jobs. Jobs submitted in this manner will run on those compute nodes allocated to the specific user. Jobs are scheduled by LSF such that compute nodes are allocated exclusively to individual jobs. Therefore, you are running jobs exclusively on physical compute nodes, which are not shared with any other job. Linux file permissions ensure that users' jobs are prevented from accessing data outside of their assigned, local node, scratch space directory.

Data Centre Security

The enCORE compute cluster and associated storage is housed in a single, highly secure data centre in North West England. Access to the data centre is strictly via access card. Cards are only allocated to fully security vetted staff. There are two access doors to navigate in order to gain access. All access is recorded via a closely monitored access system, and CCTV monitoring is also in place. The data centre has modern fire detection and suppression systems.

Network Security

All networks and firewalls are monitored on a 24x7 basis, and network management staff check all logs on a regular basis. State-of-the-art technology is in place to ensure maximum protection against unauthorized network intrusions and denial of service attacks. Users may only make network connections to and from enCORE with the formal authorisation of the destination hosts and networks. Users may not make any external network connections for the purpose of:

- Unauthorized penetration tests or traffic that circumvents authentication systems or other unauthorised attempts to gain entry into any systems
- Unauthorised probes and port scans for vulnerabilities
- Web crawling
- Unauthorised network monitoring or packet capture
- Creating forged or non-standard protocol headers, such as altering source addresses, etc.
- Flooding
- Denial of Service (DoS) of any kind

In addition, users may not operate network services related to enCORE that include any of the following:

- Open proxies
- Open mail relays
- Open and recursive domain name servers

Security Management

All aspects of the enCORE environment are continually monitored. We will contact any user where we detect or suspect any unacceptable activity. We reserve the right, where appropriate, to suspend a user account pending a full investigation of any suspicious activity. Any user found to be in breach of the Acceptable Use Policy or system and network security policies will have their account terminated immediately.

enCORE
COMPUTE ON DEMAND

OCF plc,
5 Rotunda Business Centre,
Thorncliffe Park, Chapeltown,
Sheffield, S35 2PG
T: 0114 257 2200 E: info@ocf.co.uk
W: www.ocf.co.uk