EECS Web Page Access

Migrating to a Virtual Private data Center (VPC) in AWS

The contents of the public_html folder in your EECS home directory have been cloned to the secure SEAS Computing Managed Virtual Private data Center (VPC) on Amazon Web Services EC2 platform within the Harvard University’s consolidated service. Once the migration is complete, all of your content which was previously available at http://www.eecs.harvard.edu/~myusername (or http://www.eecs.harvard.edu/myusername) should be available again as before.

To make sure everything is OK, we will need your help. Please see the Testing section.

Table of Contents

- Migrating to a Virtual Private data Center (VPC) in AWS
  - What Has Changed?
  - What Was Cloned?
- Testing
  - Testing Web Content and Functionality
  - Testing (and Setup) Editing Content
- Who Can Use login-aws Interactively?
- Environment Layout and Access Information
  - Environment Layout and Access Before August 2015
  - Environment Layout and Access After August 2015
  - Environment Layout and Access After November 2015 (Proposed)

What Has Changed?

On the server, very little has changed. However, we did identify a significant security hole which had permitted access to data in public_html directories if it had been protected solely by restricting access through a .htaccess file. We have patched this hole in the new system. Although very unlikely, if you were using .htaccess to secure your content, you may have been affected.

Before, you edited your pages in a number of ways by changing the contents of your public_html folder in your home directory. When all is complete, you should be able to once again do things in a similar manner.

What Was Cloned?

The contents, with identical ownership and permissions, of your (or the shared account's)

- public_html directory
- .ssh directory

as they were in your (or the shared account's) home directory, and nothing else. No .bashrc file or other config files. No other content in your home directory.

IMPORTANT: All of the contents of the public_html directory were potentially accessible on the old system and will therefore be accessible on the new system. The Apache process on the old server (and therefore on the new server) is running with suEXEC set. We will NOT be allowing this in the very near future.

Links were cloned as links. If they pointed to anything outside of public_html, they will be no longer working.

Testing
We are doing as much testing for you as we can, and we hope there are very few things we’ve missed; however, we are not able to test all scenarios.

Testing Web Content and Functionality

Before the final cut-over date, we would like to ask you to look at and poke around your site. You can do so by going to http://www-aws.eecs.harvard.edu/~myusername and/or http://www-aws.eecs.harvard.edu/myusername and comparing to the original at http://www.eecs.harvard.edu/~myusername or http://www.eecs.harvard.edu/myusername respectively.

If you are responsible for one of the other sites hosted from the EECS server (e.g., http://accelerator.eecs.harvard.edu, see below) please check the corresponding site in AWS (e.g., http://accelerator-aws.eecs.harvard.edu)

<table>
<thead>
<tr>
<th>Current URL</th>
<th>Test URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.eecs.harvard.edu/~myusername">http://www.eecs.harvard.edu/~myusername</a></td>
<td><a href="http://www-aws.eecs.harvard.edu/~myusername">http://www-aws.eecs.harvard.edu/~myusername</a></td>
</tr>
<tr>
<td><a href="http://www.eecs.harvard.edu/myusername">http://www.eecs.harvard.edu/myusername</a></td>
<td><a href="http://www-aws.eecs.harvard.edu/myusername">http://www-aws.eecs.harvard.edu/myusername</a></td>
</tr>
<tr>
<td><a href="http://accelerator.eecs.harvard.edu">http://accelerator.eecs.harvard.edu</a></td>
<td><a href="http://accelerator-aws.eecs.harvard.edu">http://accelerator-aws.eecs.harvard.edu</a></td>
</tr>
<tr>
<td><a href="http://helix.eecs.harvard.edu">http://helix.eecs.harvard.edu</a></td>
<td><a href="http://helix-aws.eecs.harvard.edu">http://helix-aws.eecs.harvard.edu</a></td>
</tr>
<tr>
<td><a href="http://vlsiarch.eecs.harvard.edu">http://vlsiarch.eecs.harvard.edu</a></td>
<td><a href="http://vlsiarch-aws.eecs.harvard.edu">http://vlsiarch-aws.eecs.harvard.edu</a></td>
</tr>
<tr>
<td><a href="http://vlsi.eecs.harvard.edu">http://vlsi.eecs.harvard.edu</a></td>
<td><a href="http://vlsi-aws.eecs.harvard.edu">http://vlsi-aws.eecs.harvard.edu</a></td>
</tr>
</tbody>
</table>

Testing (and Setup) Editing Content

Depending on which methods you used or would like to use, please test and see if they are still working for you.

For all of the setup, the server (e.g, ”hostname”, ”server name”, ”server address”) is login-aws.seas.harvard.edu.

If you edited your web pages by:

- Using SFTP or some Integrated Development Environment (IDE) such as Aptana, Microsoft Visual Studio, Adobe DreamWeaver. See Editing Pages via SFTP.
- Using SSH to go directly to the server and edit using a shell-based text editor (or with X11 forwarding, a GUI editor) . See SSH Access to login-aws.
- Editing files locally in a folder which are reflected on the website. See Mounting login-aws as a Folder.

Using SSH on Windows

Who Can Use login-aws Interactively?

Each of the accounts that hosted content in their public_html folder will be able to SSH to login-aws.seas.harvard.edu. This may leave people who did not previously have content without an SSH login. Those who, through shared permissions, edited the contents of public_html directories from other shared or personal accounts, can request an account by sending an email to help@seas.harvard.edu.

Only people who did this using SSH should be affected, while all others should be OK.

The system is not exclusive to members of the EECS community, though EECS members are the vast majority of them. Those who need to edit their dynamically served content (formerly by logging into pub.seas.harvard.edu) will also be users on login-aws.seas.harvard.edu.

Environment Layout and Access Information

Environment Layout and Access Before August 2015
For a few years prior to August of 2015, the EECS website files could be accessed, and therefore edited, in any one of the following manners:

1. Direct SSH access using SSH public/private key pairs (referred to as SSH+Keys)
   a. This did NOT include access using passwords; however, because some of the SSH private keys had passphrases, a number of users believed they were accessing the server with SSH+Password only. This was not the case.
2. Via a network mounted home directory folder by going into the public_html folder and directly editing content
3. Using SFTP, SCP, or rsync with password authentication from Harvard only networks

The setup can be roughly visualized as follows:

Environment Layout and Access After August 2015

Key Changes For Users

- Your data outside of your public_html directory will be safe from accidental or intentional exposure.
- You may continue to use single-factor authentication from most networks in and around Harvard.
  - **NOTE:** You will NOT be able to use unsecured wireless networks (Harvard University), you must use either wired networks or Harvard Secure wireless.
  - SSH Keys will not be required during the transition from secured Harvard networks.
- You may continue to use SSH+Keys to connect.
- Web users can temporarily continue to use HTTP instead of HTTPS until later this year.

Key Security Changes

- Home directories and all files and folders therein may no longer be world-readable or writable with few exceptions.
- Key folders and files may no longer be readable, writable, or executable by others or at times groups as per CISO recommendations.
- Some .htaccess features will be enabled, but many, such as `FollowSymLinks` or `AllowOverride ALL` will no longer be enabled.
- `suEXE` will be disabled.
- The contents of public_html folders may be scanned from time to time for confidential or high-risk information in accordance to Harvard University security practices.

Environment Layout and Access After November 2015 (Proposed)

Key Changes For Users

- Your data will be considerably more secure from other EECS users, other SEAS users, and all Web users.
You may continue to use single-factor authentication from select networks within SEAS.
You will need to use multi-factor authentication for connecting from all other networks, including from the rest of the world.
Web users will be required to use the HTTPS protocol rather than the HTTP protocol when accessing all content.

Key Security Changes

- Home directories and all files and folders therein may no longer be world-readable or writable with few exceptions.
- Key folders and files may no longer be readable, writable, or executable by others or at times groups as per CISO recommendations.
- Some .htaccess features will be enabled, but many, such as FollowSymLinks or AllowOverride ALL will no longer be enabled.
- suEXE will be disabled.
- The contents of public_html folders may be scanned from time to time for confidential or high-risk information in accordance to Harvard University security practices.