Central Web Service – Linux

WordPress SaaS Architecture Design

Table of Contents

Support Staff

Title	Name	email	Telephone	Initials
Service Owner	Peter J. Rzeminski II	ptr@fnal.gov	630.840.5524	
System Managers – Apache HTTPD	Andrew Duranceau John Inkmann	adurance@fnal.gov inkmann@fnal.gov	630.840.6457 630.840.6508	
System Managers – Linux OS	James O'Leary	joleary@fnal.gov	630.840.2230	
System Managers – Virtual Environment	Briant Lawson	blawson@fnal.gov	630.840.2944	
Management Contact	Jon Bakken (Division) Michael Rosier (Dept) Peter J. Rzeminski II (Group)	bakken@fnal.gov mrosier@fnal.gov ptr@fnal.gov	630.840.4790 630.840.8385 630.840.5524	

System Design

WordPress SaaS Architecture Design Document

This document is presented as a high-level overview of how the WordPress SaaS, a new Standard Service of the Central Web Hosting service, will be configured. This document is not intended to be used for supporting the Service itself; the minutiae and low-level configurations of each piece of the architecture design will be handled in the internal documentation for the service.

Server Layout

Each website that we host is configured to run on two or more virtual servers. For Central Web Hosting, we call these servers a Cluster. Each Cluster is load-balanced behind the F5 Big Iron or simply "F5" here at Fermilab. The Cluster is paired up with two physical servers from the Site Down service in what the F5 terms a "Resource Pool". In each Cluster, the same two physical servers from the Site Down service will always be used; this saves us resources and ensures a consistent message from that service when something breaks.

For the WordPress SaaS Service, we are tying two Resource Pools together at the F5, with each Resource Pool handling a single port; either Port 80 or Port 443. To differentiate the Resource Pools, we are calling them Zones. The Public Zone is configured to handle only Port 80 traffic with the Admin Zone handling only Port 443 traffic.

Access Zones

The zones are defined as follows:

Hardware Layer

Public Cluster Zone

- A standard configuration Central Web Hosting Cluster used to deliver all public-facing content of the WordPress SaaS to the Internet.
- The NAS, using NFSv4, will be configured so that the Kerberos principals for the host machine will be granted read-only access to all portions of the file system except the logs directory, where Apache requires read-write access.
- The credentials used to access the MySQL database where the content is stored will have Read-Only access at the database level.
- Load Balance Profile Example

  MEMBER (PRIORITY)
  - web5001.fnal.gov (150) (active)
  - web5002.fnal.gov (150) (active)
  - web-sorry01.fnal.gov (50)
  - web-sorry02.fnal.gov (1)

Administrative Cluster Zone

- A standard configuration Central Web Hosting Cluster used to manage all administrative functions of the WordPress SaaS.

- The VIP (virtual IP) address for the Cluster, hosted on the F5, will be denied access to the Open Internet. This is done by ensuring that ports 80 and 443 are not granted a border router exception outside of the Fermilab Subnet.
- The NAS, using NFSv4, will be configured so that the Kerberos principals for the host machine will be granted read-only access to all portions of the file system except the logs directory, where Apache requires read-write access.
- The credentials used to access the MySQL database where the content is stored will be allowed read/write access at the database level, from only these servers.
- Load Balance Profile Example

  MEMBER (PRIORITY):
  - web5101.fnal.gov (150) (active)
  - web5202.fnal.gov (100) (stand-by)
  - web-sorry01.fnal.gov (50)
  - web-sorry02.fnal.gov (1)

Software Layer

Public Software Zone

- A special configuration Central Web Hosting Cluster used to deliver all public-facing content of the WordPress SaaS to the Internet.
- Access to the file system (NAS) for the Apache HTTPD process is managed by a special Kerberos principal tied specifically to the HTTPD process running on that server. The ACLs for that principal will be granted read-only rights to the content areas of the web server for each website. It will not be granted read/write access to any portion of the NAS file system.
- The credentials used to access the MySQL database where content is stored will be granted read-only access at the database level, from only these servers.

Administrative Software Zone

- A special configuration Central Web Hosting Cluster used to manage all administrative functions for the WordPress SaaS to the Internet.
- Access to the file system (NAS) for the Apache HTTPD process is managed by a special Kerberos principal tied specifically to the HTTPD process running on that server. The ACLs for that principal will be granted read/write rights to the content areas of the web server for each website.
- The credentials used to access the MySQL database where content is stored will be granted read/write access at the database level, from only these servers.
- Within the WordPress software itself, multiple types of accounts, or “Roles” as WordPress terms them, will be used. The specifics of those Roles are detailed later in this document.

Access Charts by Zone

The following shows what access will be allowed, based on the category and location of the user and the target of the access attempt.

Anonymous User outside of the Fermilab Network

Zones	Public Software Zone	Administrative Software Zone
Public Cluster Zone	**Full access to all non-administrative content**	**Administrative software, /wp-admin, is blocked via Apache configuration**
Administrative Cluster Zone	**Unavailable outside of the Fermilab Network; blocked by the Border Router**	**Unavailable; blocked by both Border Router and Apache configurations**

Anonymous User inside the Fermilab Network

Zones	Public Software Zone	Administrative Software Zone
Public Cluster Zone	**Full access to all content**	**Administrative software, /wp-admin, is blocked via Apache configuration**
Administrative Cluster Zone	**The URL is available, and content will be served over port 443, but without proper credentials, they cannot access the Admin functions.**	**The URL is available, but they cannot access the content without being mapped to a Role within the website.**

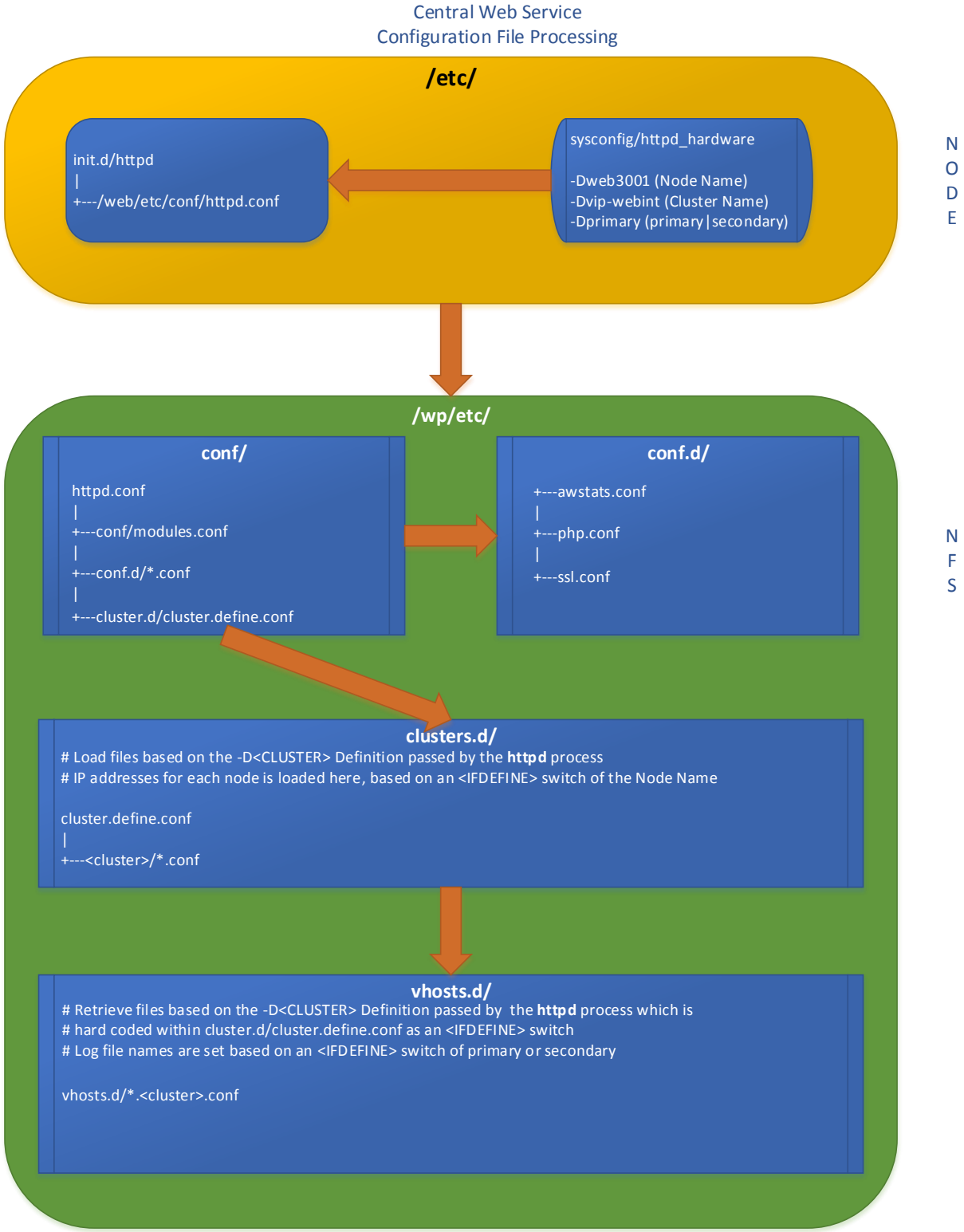
Admin User outside of the Fermilab Network

Zones	Public Software Zone	Administrative Software Zone
Public Cluster Zone	**Full access to all content**	**Administrative software, /wp-admin, is blocked via Apache configuration**
Administrative Cluster Zone	**Unavailable outside of the Fermilab Network; blocked by the Border Router**	**Unavailable; blocked by both Border Router and Apache configurations**

Admin User inside the Fermilab Network

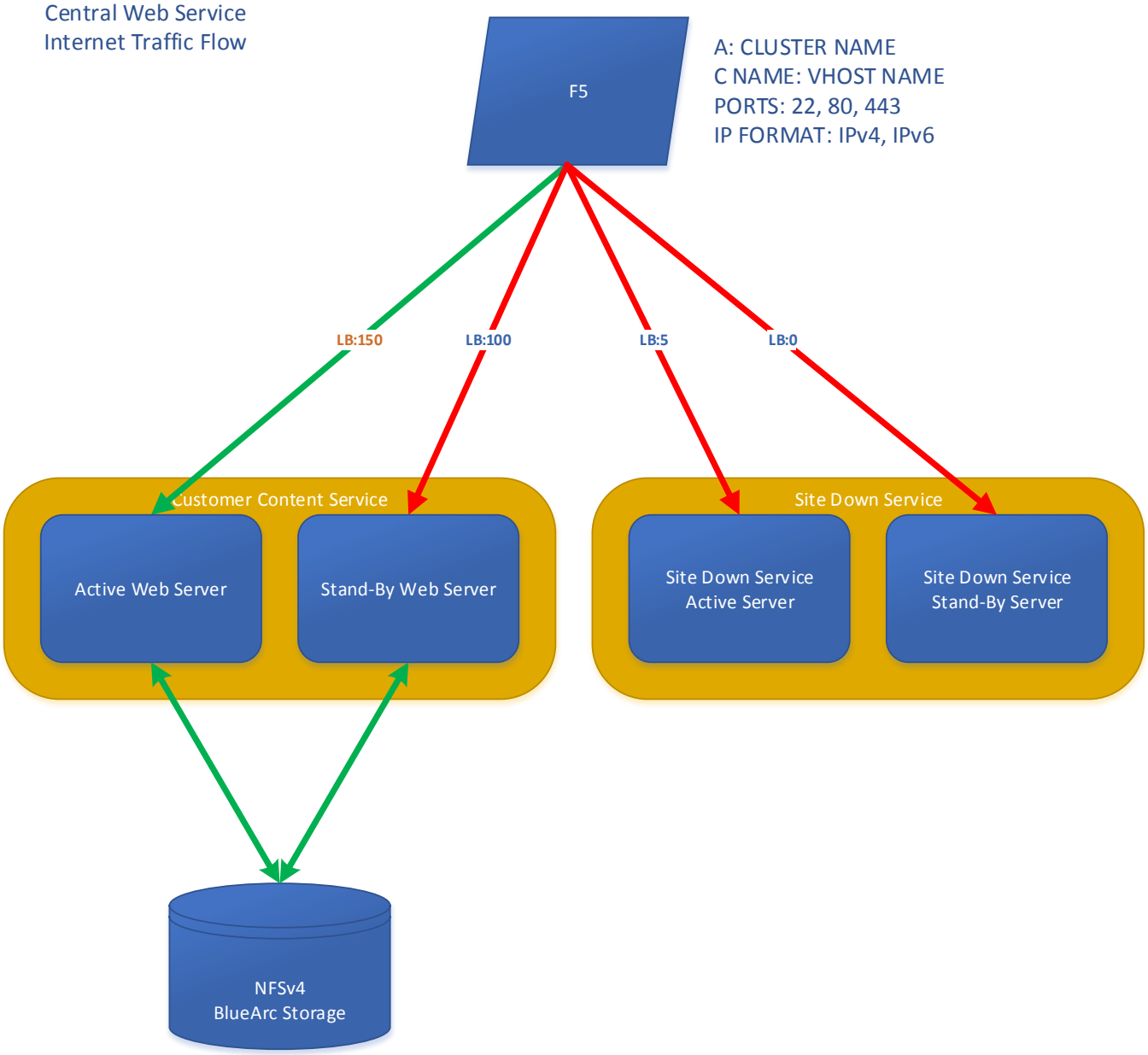
Zones	Public Software Zone	Administrative Software Zone
Public Cluster Zone	**Full access to all content**	**Administrative software, /wp-admin, is blocked via Apache configuration**
Administrative Cluster Zone	**With the proper credentials, full access to site content**	**With proper credentials, full access to site administrative controls**

Configuration Load



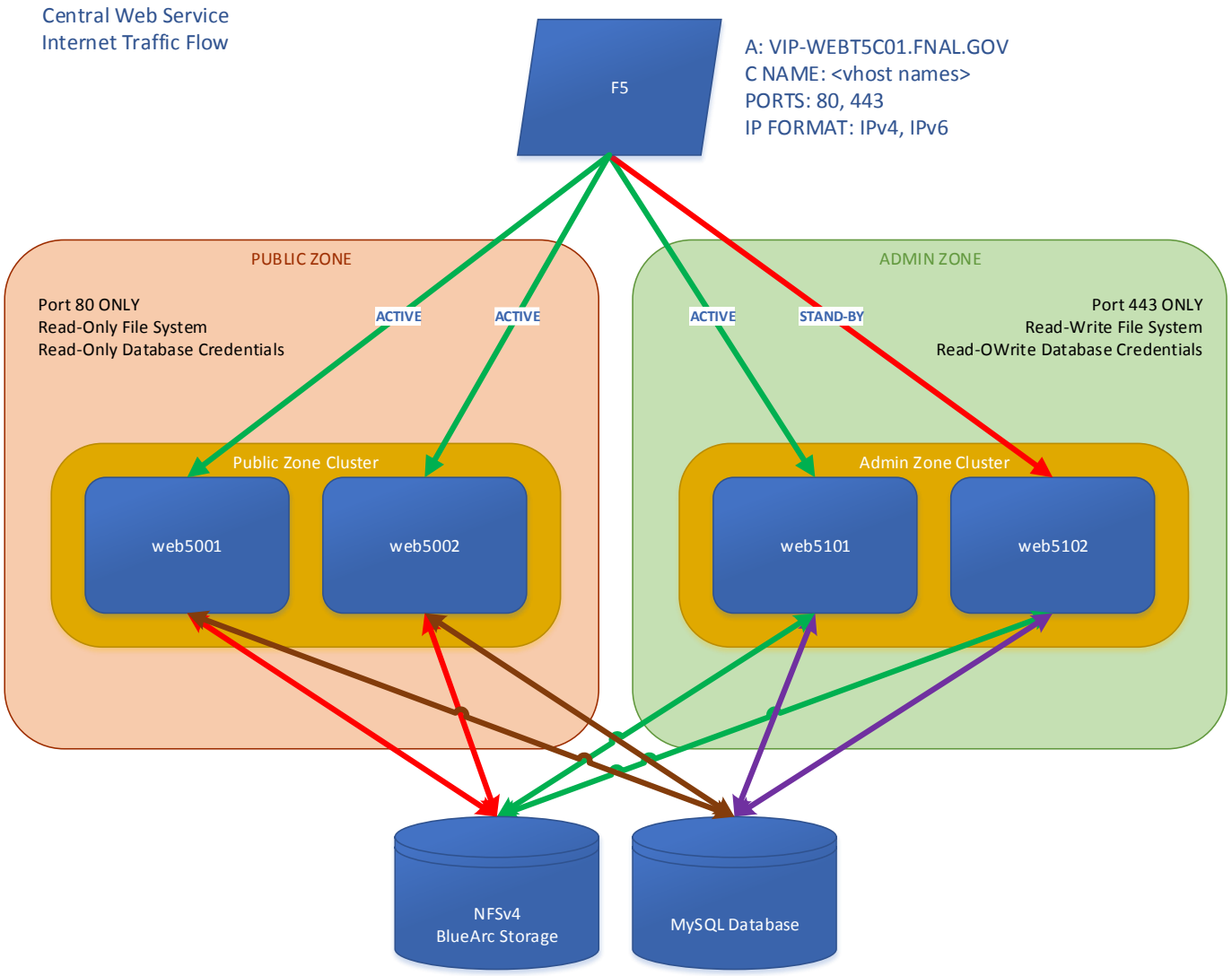
Standard Cluster Design

Central Web Service
Internet Traffic Flow



Cluster / Zone Configuration

Note: The Site Down servers are still present and operate independently in each Zone, but they are not shown here to save space in the drawing.



Naming Schemes

Each part of the Central Web Hosting service has a specific naming scheme to ensure it can be easily identified.

Server Naming Scheme

Individual servers are named based on the tier they are in. They follow this format:

web*tsss*

- *t* = The numeric tier of the server in question.
- *sss* = The server number within this tier.

Additionally, within any cluster[1], the **odd numbered** server will always be the primary server with the **even numbered** server being the secondary server.

Examples would be:

- web1001
  - Tier 1, Server 1—Primary Server
- web1002
  - Tier 1, Server 2—Secondary Server
- web3001
  - Tier 3, Server 1—Primary Server

Servers will always have the domain name of fnal.gov.

Cluster Name Format

Each Cluster uses the following naming scheme:

- VIP-WEBT*t*C*cc*

T*t* = The letter T and the numeric tier of the cluster in question

C*cc* = The letter C and the cluster number

Examples would be:

- VIP-WEBT1C01
  - Tier 1, Cluster 01
- VIP-WEBT1C02
  - Tier 1, Cluster 02
- VIP-WEBT2C01
  - Tier 2, Cluster 01

The domain for each cluster is fnal.gov with the DNS entry being an A record. No other domain is used, although CNAME records in other domains may point to these cluster names in fnal.gov.

[1] Tier 5 Public Zone servers will be configured for active/active use.

Defined Cluster Names

The following cluster names have been defined to describe each tier we service

Tier 1 – The general tier for Central Web Hosting.

Tier 2 – The tier set aside for organizations that wish to have an entire cluster to themselves and are able to pay for it

Tier 3 – The development & integration clusters owned by the Central Web Hosting group, used to test patching and other technology improvements before rolling them out to production

Tier 4 – The "one-off" tier. Similar to Tier 2, but each cluster is customized to the Site Owner's needs.

Tier 5 – The WordPress SaaS tier. This is a specialized tier used for hosting WordPress SaaS sites.

- Tier 5.0 – A sub-tier for the Public Zone Clusters.
    - Machine names will be in the range web5000–web5099.
- Tier 5.1 – A sub-tier for the Admin Zone Cluster(s)
    - Machine names will be in the range web5100–web5199.
- Tier 5.2 – A sub-tier where an independent cluster will be stood up for the Site Owners to host only their website. This is considered to be the "Tier 2" offering within WordPress.
    - Machine names will be in the range web5200–web5299.
    - NOTE: This is documented for future purposes only; it will not be available at the launch of the service.

System Configuration

General Configuration

The WordPress SaaS Service is a Standard Service of the Central Web Hosting service. The service is centrally managed and has a number of security procedures put in place to protect the software, the content, the infrastructure, and ultimately, the Site Owners.

To offer a stable, centrally managed service to its customers, a trade-off between security and flexibility will be made. Specifically, the flexibility and freedom a WordPress Administrator is used to having will be curtailed in favor or increased security and centralized management. It is well understood that this approach will limit and possibly preclude certain functions and/or plugins from working with the WordPress SaaS Service, causing some individuals to refuse to use this service. This is accepted because the security of each website and the Service as a whole is necessary to protect the Laboratory from attack and possible loss of reputation.

Production, Integration, & Development Systems

There will only be a Production instance of each WordPress SaaS site.

There will not be any dedicated Integration or Development WordPress SaaS offerings made available to the Site Owners.

Theme & Plugin Development

Theme and Plugin development are out of scope for Central Web Hosting, the WordPress SaaS Project, and the eventual Production WordPress SaaS Service.

However, one-off WordPress sites will be stood up on the Central Web Service, separate from the WP SaaS hardware, allowing dedicated developers to create and test themes and plugins without conflicting with the WP SaaS restrictions that would otherwise prevent such work. This development site concept will be rolled after the main WordPress SaaS Service has gone to production and is not a part of the initial Project.

WordPress Software Configuration

WordPress SaaS Configuration & Access Rights

What capabilities were removed from Site Admins

The Administrator Role has full access to all the functions of the WordPress software. Access to this Role will not be granted to anybody outside the Web Systems Administration (WSA) Group. There are no exceptions to this rule.

This has the effect of removing the following capabilities from a Site Admin:

- The ability to install or delete a Plugin
- The ability to install or delete a Theme, including a Child Theme.
- The ability to add, create, delete, or edit WordPress user accounts.
    - The ability to add users to a Role is handled through a separate feature and is described later in this document.
- The ability to update the core WordPress software.

All of the above items are retained by the WSA Administrators, with the exception of the WordPress user accounts; those are not allowed under any circumstances.

Themes

For sites in the fnal.gov domain, the default theme that is installed will be the Xeno Media-authored "FNAL Basic" Theme. This is a Theme that is based on the design of www.fnal.gov circa May, 2015.

For a site not in the fnal.gov domain, the default themes that come with WordPress at the time of the most current release will be installed and active by default.

In both cases, the Site Owner can request to have a different Theme installed to their site. If the Theme is already on the approved list, then a simple request for installation is all that is required. If the theme is not on the approved list, then it will have to go through a Governance Process to gain approval and subsequent installation.

Site Owners wishing to develop their own custom theme and/or purchase a theme from a third party will require advance approval.

Plugins

Plugin functionality is something that will be tightly controlled on the WP SaaS Service. There are a number of restrictions that all Plugins will have to operate under.

- Site Owners wishing to develop their own custom plugins or purchase a plugin from a third party will require advance approval.
- A plugin that caches the database credentials in use at the time it was installed, instead of using the credentials under which it is accessed, will not be able to function. Our security model precludes that. Specifically, if it attempts to cache the Read/Write credentials when installed, and then attempts to use them from the Read-Only interface, the database will refuse the connection, breaking the plugin.
- Any plugin that requires Read/Write access to the WordPress database for the website it was installed to will not function as a matter of the security design. However, plugins that require Read/Write access to some other, non-WordPress, database will be allowed.
- Any plugin written in-house will be required to use code that "calls home" to check for updates. This is a requirement to ensure that it can be centrally managed.

WordPress Roles

What Roles are Available

Unlike the Central Web Service – Linux & IIS, where there are only two categories of user: Site Owner and Content Editor, WordPress has multiple categories, or Roles as they are known within WordPress. Each Role has a defined set of capabilities.

In the Central Web Service – Linux service, we give Site Owners full access to everything and let them manage their site and content as they see fit, adding whatever code they wish, so long as it meets the policies and provisions laid out for web hosting.

However, as a part of the trade-off of flexibility for security with the WordPress SaaS Service, we are unable to grant that level of access to a Site Owner. Where we would normally grant a Site Owner the Administrator Role, it has been determined that the rights allowed to that Role create security and

management issues. As such, the Administrator Role is being withheld from all Site Owners and will be retained for the exclusive use by the WSA Web Team. To compensate, we have created a custom Role called “Site Admin” that grants most of the rights of the built-in Administrator Role while removing those functions that cause us to withhold the Administrator Role in the first place.

The Roles are as follows:

- Administrator – Built-in Role. Access to this account will only be granted to the WSA Web Team; no exceptions.
- Local-Admin – A WSA-created Role. This Role grants some administrative functions but removes the Roles ability to manipulate User accounts and the ability to update the base WordPress software; it retains the ability install and delete Themes and Plugins. This Role will only be used on a few specific non-public sites where Plugin or Theme testing is being conducted and a higher level of access it necessary. The Role will never be granted to anyone on a Production site.
- Site Admin – A WSA-created Role. This Role will be granted, initially, to the two Site Owners for each WP SaaS site. The Site Owners will have the ability to add additional persons to the Site Admin role, at their discretion. (Such persons do not thereby become Site Owners.)
- Editor – A Built-in Role to WordPress. Users will be granted this role by the Site Admin.
- Author – A Built-in Role to WordPress. Users will be granted this role by the Site Admin.
- Contributor – A Built-in Role to WordPress. Users will be granted this role by the Site Admin.
- Subscriber – A Built-in Role to WordPress. Users will be granted this role by the Site Admin.

Content Editors & Role Mapping

As described above, there is no direct equivalent of a Content Editor as they exist within the Central Web Service Linux & IIS offerings. Instead, each person must be assigned to a WordPress Role, where they will have a specific set of permissions when interacting with the Administrative interface of the WordPress website.

Each WordPress website has a set of Active Directory (AD) groups assigned to it. The groups are named in such a manner as to be unique for each website and each group within the website. The naming convention is as follows:

web-wp + _ + URL + _ + ROLE

...where URL is the fully-qualified domain name of the website with periods replaced by hyphens, and ROLE is the specific WordPress Role with spaces, if any, changed to hyphens.

Using the website wsa.fnal.gov as the example, the AD groups controlling some of the roles are:

web-wp_wsa-fnal-gov_site-admin
web-wp_wsa-fnal-gov_editor
web-wp_wsa-fnal-gov_contributor

Note the underscores between sections.

Site Owners have the ability to map a user to each of those groups through the “WordPress User Role Management” tool. This web application allows those persons with the Site Admin Role grant or remove any WordPress role to or from users in the “OU=FermiUsers,DC=services,DC=fnal,DC=gov” OU of the SERVICES Active Directory, by causing them to be added to or removed from the corresponding

group. Upon request, and with justification, on a case-by-case basis, we will allow Site owners to have all authenticated users that are not mapped to another Role within that website, be granted the "Subscriber" Role so that they can gain access to protected content within that website.

WordPress Development

The WordPress SaaS Service will provide a development site for those Site Owners that have a valid and documented need for creating custom Plugins and Themes for their production site.

The WordPress SaaS Development site will operate in the following manner:

- It will be hosted on servers managed by the Central Web Hosting Service that are not connected to the WordPress SaaS Production servers.
- Site Owners will be granted access to the file system to allow them to edit their custom code directly.
    - Edits to the core WordPress code will not be allowed. Any changes made to the core will be overwritten at each update and possibly cause Site Owner's other customizations to fail when exported to the Sandbox or Production website.
- The Central Web Hosting service will install and manage the WordPress software as if it were a normal production site, with the following exceptions:
    - Unless required because of open security issues, Themes and Plugins installed to the Development site will not be automatically updated. It will be at the discretion of the Site Owners to update the Plugins and Themes to ensure they do not interfere with theyir development work.
    - Site Owners will be granted the capability to add and remove Themes and Plugins without the assistance of the Central Web Hosting group. Any Themes and Plugins added to the development site must be submitted through the normal approval process (see page 13) before they will be accepted on the Production site.
- Once a Site Owner has finished authoring a Theme or Plugin, they can do a test upload on the Sandbox site, and if it functions there, they can submit it for approval and installation on their production site.