Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Evaluación y mejora del proceso para configurar HTTPS con Bitnami

Autor: Marcos Bjorkelund

Tutor: Francisco Javier Muñoz Calle

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2022

Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Evaluación y mejora del proceso para configurar HTTPS con Bitnami

Autor:
Marcos Bjorkelund

Tutor:
Francisco Javier Muñoz Calle
Profesor Colaborador

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2022

Trabajo Fin de Grado: Evaluación y mejora del proceso para configurar HTTPS con Bitnami

Autor: Marcos Bjorkelund
Tutor: Francisco Javier Muñoz Calle

El tribunal nombrado para juzgar el trabajo arriba indicado, compuesto por los siguientes profesores:

Presidente:

Vocal/es:

Secretario:

acuerdan otorgarle la calificación de:

El Secretario del Tribunal

Fecha:

Agradecimientos

Quiero agradecer a toda mi familia por el intenso apoyo durante estos años. No tengo ninguna duda de que no lo podría haber hecho sin vosotros.

Quiero también agradecer a mis compañeros de Bitnami; Beltrán, Javier, José Luis, Daniel y muchos otros que me dejo por nombrar, por el gran apoyo y todo lo que he aprendido de todos ellos todos estos años.

Finalmente, agradecer a mi gran amigo Daniel Mantel, por la inspiración para estudiar telecomunicaciones.

Marcos Bjorkelund
Sevilla, 2022

Resumen

Este proyecto estudia la configuración de HTTPS en soluciones de Bitnami. Esta temática fue revelada como la más frecuente en el foro de Bitnami, tras un análisis de todos los casos de soporte.

Para ello, se han evaluado las herramientas existentes para la configuración de HTTPS, con el propósito de encontrar sus puntos débiles y, basándonos en estadísticas de uso y los problemas encontrados por los usuarios, se ha desarrollado una versión mejorada de estas desde cero.

Con esta nueva herramienta de configuración de HTTPS de Bitnami, se ha mejorado la experiencia de usuario y reducido la cantidad de nuevos casos de soporte, permitiendo al equipo de ingeniería de Bitnami dedicar menos tiempo a trabajo de soporte.

Abstract

This project analyzes the state of the HTTPS configuration process in Bitnami stacks, which has been found to cause issues for users and is currently the most visible theme in the Bitnami support forums.

In this process, all existing solutions for configuring HTTPS in Bitnami stacks have been reviewed to identify their weak points. Basing on the usage statistics and problems highlighted by users, an improved solution has been created from scratch.

With the new HTTPS configuration tool from Bitnami, the overall user experience has been improved, and the amount of new support cases has been reduced, allowing the engineering team to spend less time doing support work.

Índice

1 Introducción

Bitnami nació para simplificar el despliegue de aplicaciones Web de todo tipo; desde comercio en línea hasta comunicación instantánea entre personas. Estas aplicaciones habitualmente requieren una configuración previa para poder funcionar correctamente, y que para usuarios no avanzados suele resultar complicado, y es aquí donde entra en juego Bitnami.

Con un catálogo de más de 150 aplicaciones disponibles de manera totalmente gratuita, Bitnami ofrece soluciones en multitud de plataformas y formatos; como instaladores, máquinas virtuales, imágenes de contenedores Docker, etc.

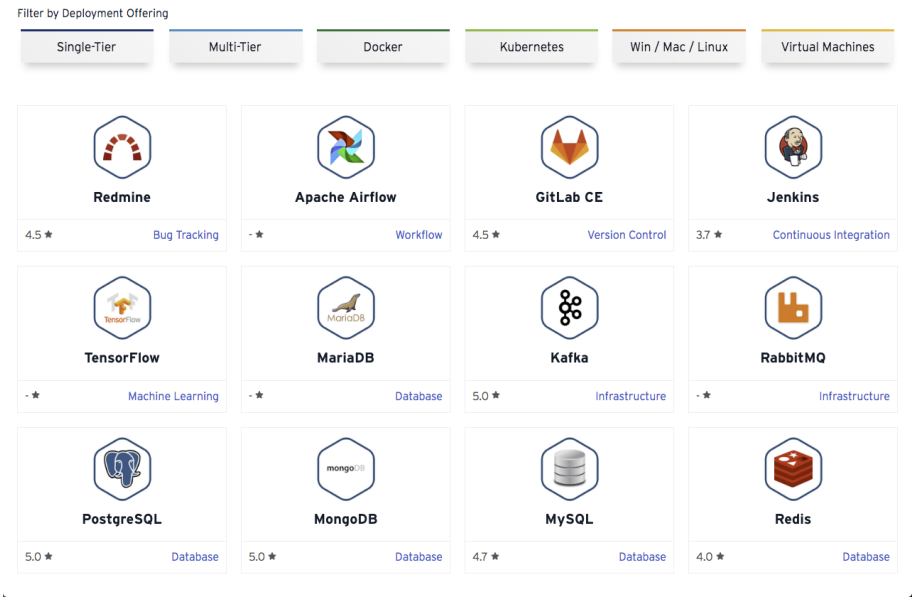


Figura 1.1 Captura parcial del catálogo de Bitnami junto al selector de formatos y plataformas.

Las soluciones de Bitnami cuentan con documentación y tutoriales de alta calidad, además de distintos medios de soporte totalmente gratuitos. Todas las soluciones están en un proceso continuo de mejora, y las sugerencias o ideas para ello originan tanto internamente, como externamente mediante los medios de soporte.

Bitnami realiza además análisis periódicos para determinar los cambios en las tendencias de uso de sus productos, y tomar acciones según las observaciones encontradas, y que ello permita optimizar los recursos empleados en soporte. En particular, este proyecto va a centrarse en una de estas temáticas y que ha sido identificada como la más frecuente en el análisis del año 2018; la configuración de comunicaciones Web seguras mediante HTTPS en soluciones de Bitnami.

1.1 Descripción del problema

La configuración de HTTPS hace pocos años era un problema poco frecuente por el bajo nivel de uso del protocolo HTTPS. No obstante, se ha ido popularizando en parte por buscadores como Google favoreciendo sitios Web que soporten el protocolo HTTPS [1], y por la aparición y popularización de la autoridad de certificación gratuita Let's Encrypt [2], que simplifica radicalmente el proceso de generación de certificados.

Gracias a Let's Encrypt se hizo posible desarrollar una herramienta con la que configurar HTTPS en soluciones de Bitnami en pocos minutos. No obstante, un análisis de todos los casos de soporte comprendidos entre julio y septiembre del 2018 ha encontrado una baja efectividad de estas propuestas, puesto que la configuración de HTTPS en productos de Bitnami es la temática más frecuente de todos ellos. Este análisis se puede encontrar en el Apéndice A.

Con este proyecto se analizarán los motivos de la ineficacia de las soluciones anteriormente mencionadas, además de identificar mejoras e implementar una nueva herramienta de configuración de HTTPS en soluciones de Bitnami, con la máxima comodidad para los usuarios.

1.2 Objetivos

El principal objetivo de este proyecto es reducir la frecuencia de nuevos casos de soporte relacionados con la configuración de HTTPS en soluciones de Bitnami.

Los objetivos secundarios, relacionados, son mejorar la experiencia de usuario de los productos de Bitnami en cuanto a la configuración de HTTPS, y reducir el tiempo empleado en soporte por el equipo de ingeniería.

1.3 Motivación

La misión principal de Bitnami es la de ayudar a sus usuarios construir y desplegar aplicaciones más rápido y fácilmente. De hecho, Bitnami cuenta con una comunidad de millones de usuarios, que la usan para todo tipo de proyectos; desde páginas Web personales hasta proyectos de grandes empresas. De esta forma, es una prioridad corporativa la de continuar mejorando la experiencia de los usuarios utilizando sus productos, y de crear nuevo contenido que permita seguir esta misión.

La seguridad es parte fundamental en este aspecto, y dentro de este área, la configuración de HTTPS es una parte imprescindible para cualquiera que busque construir una página Web. Se puede observar la relevancia de estos temas en el análisis de los casos de soporte documentado en el Apéndice A, siendo la temática más frecuente, pese a existir extensas guías y herramientas con el fin de simplificar estos procesos.

Debido al crecimiento lineal de la cantidad de casos de soporte que están apareciendo con estas temáticas, el equipo de ingeniería está viendo como se ve obligado a dedicar cada vez más tiempo en trabajo de soporte, que es tiempo que no se va a poder dedicar a otros proyectos y tareas. Esto es algo que se desea acotar, sin que sea necesario relajar los tiempos de respuesta de los casos de soporte.

1.4 Alcance

Este proyecto se divide en cinco grandes bloques:

- Análisis de soluciones existentes: Se analizan los resultados de un estudio realizado sobre todos los casos de soporte en el periodo de septiembre y octubre del 2018, con base en las herramientas y guías existentes, se buscarán los puntos flojos y que sean causa de problemas. Tras ello, se realizará una propuesta de solución basándonos en las conclusiones obtenidas.
- Desarrollo e implementación: Se realiza la propuesta técnica, el análisis de requisitos, el desarrollo y la implementación de la nueva herramienta de configuración de HTTPS. En el momento de finalización de este bloque, el proyecto será completamente funcional.
- Pruebas y publicación: Se desarrollarán las pruebas que se van a realizar sobre la solución implementada, y los procesos de publicación de la herramienta tras la revisión manual. Posteriormente, se procederá a automatizar las pruebas individuales sobre un entorno estandarizado. Este bloque culminará con la publicación de la nueva herramienta de configuración de HTTPS de Bitnami.

- Validación de resultados: Tras la publicación de la solución publicada, se realiza un breve análisis de casos de soporte para identificar el impacto de esta. En este punto se identificará mejoras futuras que permitan mejorarlas con base en la respuesta de la comunidad.
- Memoria: Describir el proceso de desarrollo del proyecto, así como aquellos aspectos necesarios para su comprensión como la Web, DNS, HTTPS, criptografía de clave pública, certificados y Let's Encrypt.

1.5 Plan de trabajo

En la Figura 1.2 se representa un diagrama de Gantt con la planificación temporal del trabajo, que comienza el 18 de marzo de 2019.

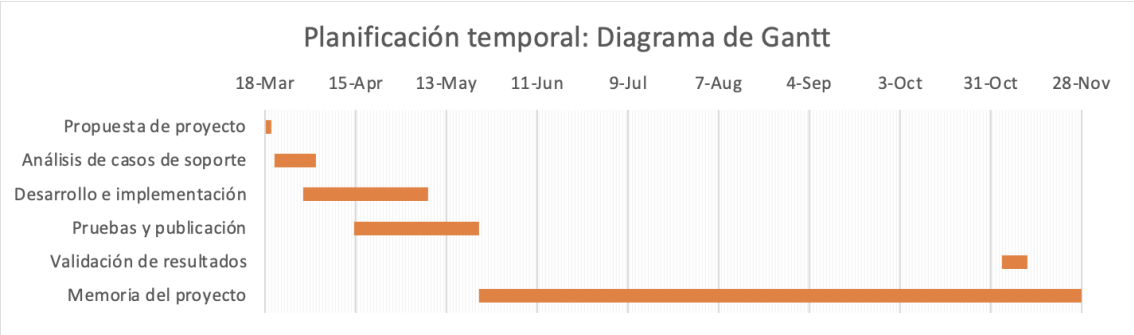


Figura 1.2 Diagrama de Gantt con la planificación temporal del proyecto.

La fecha de inicio, fecha de fin y la duración de cada uno de los bloques se representa en la Tabla 1.1. Nótese que se ha decidido atrasar el comienzo del bloque de validación de resultados, ya que se va a realizar un nuevo análisis de casos de soporte un año posterior al análisis que dio lugar a este proyecto (Apéndice A), que fue realizado entre septiembre y octubre del 2018.

Bloque	Fecha de inicio	Fecha de fin	Duración (días)
Propuesta de proyecto	18/03/2019	20/03/2019	2
Análisis de casos de soporte	21/03/2019	03/04/2019	13
Desarrollo e implementación	30/03/2019	08/05/2019	39
Pruebas y publicación	15/04/2019	24/05/2019	39
Validación de resultados	04/11/2019	12/11/2019	8
Memoria del proyecto	24/05/2019	28/11/2019	188

Tabla 1.1 Estimación de fecha de inicio, fin y duración de los bloques del proyecto.

En la Tabla 1.2 se representa una estimación de las cantidades de horas que se emplearán en este proyecto, tanto como trabajo dentro de Bitnami como por libre. Nótese que parte del trabajo se realiza dentro de la empresa Bitnami a jornada parcial (5 horas diarias), pero la mayor parte se realiza por libre.

Bloque	Tiempo empleado (en Bitnami)	Tiempo empleado (por libre)
Propuesta de proyecto	4	4
Análisis de casos de soporte	20	20
Desarrollo e implementación	100	0
Pruebas y publicación	40	40
Validación de resultados	0	40
Memoria del proyecto	0	160
TOTAL	120 horas	220 horas

Tabla 1.2 Estimación de tiempo que se empleará en el proyecto (en horas).

1.6 Medios materiales

Para la realización de este proyecto se han usado los medios materiales descritos a continuación.

1.6.1 Hardware

Este proyecto hace uso de un dispositivo MacBook Pro del 2018 (modelo A1989) con conexión a Internet, para el desarrollo de la memoria, desarrollar la herramienta de configuración de HTTPS para las soluciones de Bitnami y realizar los análisis de casos de soporte.

1.6.2 Software

El software empleado se describe en la Tabla 1.3.

Nombre	Uso	Notas
Mozilla Firefox [3]	Navegador Web empleado.	
Vim [4]	Editor de texto empleado para desarrollar la herramienta, las pruebas automatizadas y la memoria.	Preinstalado en el ordenador usado.
Git [5]	Herramienta para gestionar el control de versiones del proyecto.	Uso de GitHub para hospedar los ficheros.
VMware InstallBuilder [6]	Desarrollo y construcción de la herramienta de configuración de HTTPS.	
Tclkit [7] y Expect [8]	Desarrollo de pruebas automatizadas usando el lenguaje de programación Tcl.	
Microsoft Excel [9]	Análisis de casos de soporte.	
LaTeX [10]	Desarrollo y generación de la memoria.	
MockFlow [11]	Prototipado del diseño de la interfaz de usuario de la herramienta.	
diagrams.net [12]	Diseño de algunos de los diagramas usados en la memoria.	

Tabla 1.3 Software usado en el desarrollo de este proyecto.

1.6.3 Servicios

Se ha hecho uso de Amazon Web Services [13] para desplegar instancias de Amazon EC2 [14], usadas para desarrollar y probar la herramienta de configuración de HTTPS implementada. Además, se ha hecho uso de Amazon Route 53 [15] para configurar dominios a utilizar en las pruebas.

Para el hospedaje del código fuente del proyecto, se ha hecho uso del servicio de GitHub [16].

2 Antecedentes

Para comprender mejor los problemas a los que se quiere atacar con el proyecto, es necesario realizar una breve introducción a Internet y la World Wide Web en su estado actual, a la seguridad en estos entornos, y cómo es usado por los usuarios hoy día.

2.1 Internet y la World Wide Web

Internet es un conjunto descentralizado de redes de comunicación interconectadas, basado en tecnologías de conmutación de paquetes.

Su origen se remonta a los años 1960, cuando el Departamento de Defensa de EE. UU. desarrolló ARPANET, con el fin de poder realizar comunicaciones entre las distintas instituciones académicas como estatales. En 1981 se introducen los protocolos TCP/IP y el término «Internet», y su estandarización se produce en 1982. En 1992, Tim Berners-Lee publica la World Wide Web (o WWW) mientras trabaja en el CERN, e introdujo el concepto de páginas Web.

En los últimos 20 años, la UIT estima la penetración del 5 % de toda la población mundial en 1999, a más del 50 % en 2019 [17]. Durante estos años, y gracias a Internet, se ha producido una revolución en la manera con la que nos comunicamos y trabajamos, la enseñanza, ha provocado la aparición de nuevas industrias, etc., dicho en pocas palabras, ha cambiado el mundo [18].

2.1.1 Definiciones previas

Antes de proceder a describir las tecnologías de Internet relacionadas con este proyecto, se realizará una serie de definiciones que permitan una mejor comprensión del proyecto para el lector.

Comunicación cliente-servidor

La World Wide Web sigue una arquitectura cliente-servidor, en la que hay dos entidades:

- Los servidores, que son los productores o proveedores de recursos o servicios (como por ejemplo una página Web).
- Los clientes, que son demandantes de recursos o servicios.

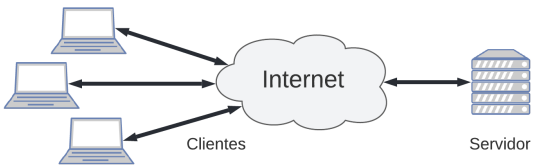


Figura 2.1 Diagrama cliente-servidor vía Internet.

Es importante mencionar que servidor no necesariamente tiene que estar compuesto por una sola máquina, ello dependerá de la arquitectura del servicio implementado en este.

Canal de comunicación

Un canal de comunicación es el elemento de un sistema de comunicación, entre emisor y receptor, en el que se transmite información.

Para el envío de la información, debe ser codificada en el emisor de forma que pueda ser enviada por el canal, y a la llegada al receptor es de nuevo decodificada.

Haciendo un símil con una comunicación entre dos personas, el canal sería el aire por el que vibra la voz entre el emisor (persona que habla) y receptor (persona que escucha). En este caso es de doble sentido, ya que en una conversación un emisor es también receptor, y viceversa.

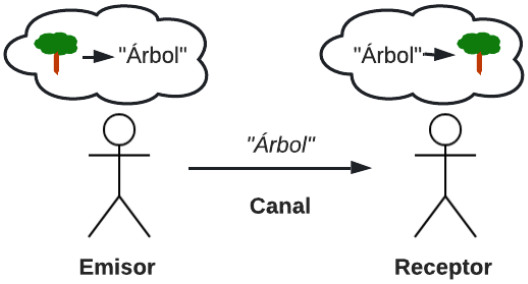


Figura 2.2 Emisor, canal de comunicación y receptor.

Nótese que en la mayoría de ocasiones el canal no se puede controlar, por lo que no se puede considerar seguro. Si queremos establecer una comunicación segura que no pueda ser interceptada por otro participante, debemos codificar las comunicaciones de forma que solo pueda ser conocida por quien se desee. A esta área se le denomina criptografía.

Protocolo de comunicaciones

Un protocolo de comunicaciones (o protocolo de aquí en adelante) es un conjunto de normas que permiten la comunicación de dos entidades, para transmitir información a través de un canal de comunicaciones.

2.1.2 El protocolo IP

El protocolo de Internet o IP es el protocolo más importante de Internet, y supone de facto su constitución. Esto se debe a que su función consiste en realizar la entrega de datos desde un nodo origen a un destino en una red, permitiendo la interconexión de redes.

Una unidad de datos del protocolo de Internet es denominada paquete, e incluye los datos que se desean enrutar junto con la cabecera de IP, que incluyen metadatos para definir la comunicación (como nodo origen, destino, tamaño de los datos, etc.).

Hay dos versiones del protocolo de Internet, la versión 4 y la versión 6. Aunque las cabeceras de ambos protocolos son sustancialmente distinto, ambos protocolos incluyen los siguientes campos:

- Versión del protocolo utilizada en el paquete.
- Dirección destino: Dirección IP que identifica el nodo con el que se quiere comunicar.
- Dirección origen: Dirección IP que identifica el nodo origen, que permite la respuesta al mensaje por parte del nodo destinatario.

Una dirección IP permite identificar a un nodo concreto en una red. De esta forma, cualquier otro nodo en la red podría realizar una comunicación con este conociendo la dirección IP. El tamaño de la dirección IP varía según la versión del protocolo.

Protocolo de Internet versión 4 o IPv4

El protocolo de Internet versión 4 o IPv4 fue la primera implementación del protocolo IP, y aún es usado ampliamente.

En IPv4, las direcciones IP tienen un tamaño de 4 bytes (o 32 bits), que supone un total de 2^{32} o 4,294,967,296 direcciones IPv4 en total. Esto es un problema, puesto que hay más humanos en la Tierra que direcciones IP existentes, y de hecho es uno de los motivos por los que se quiere abandonar este protocolo por una implementación más moderna [19].

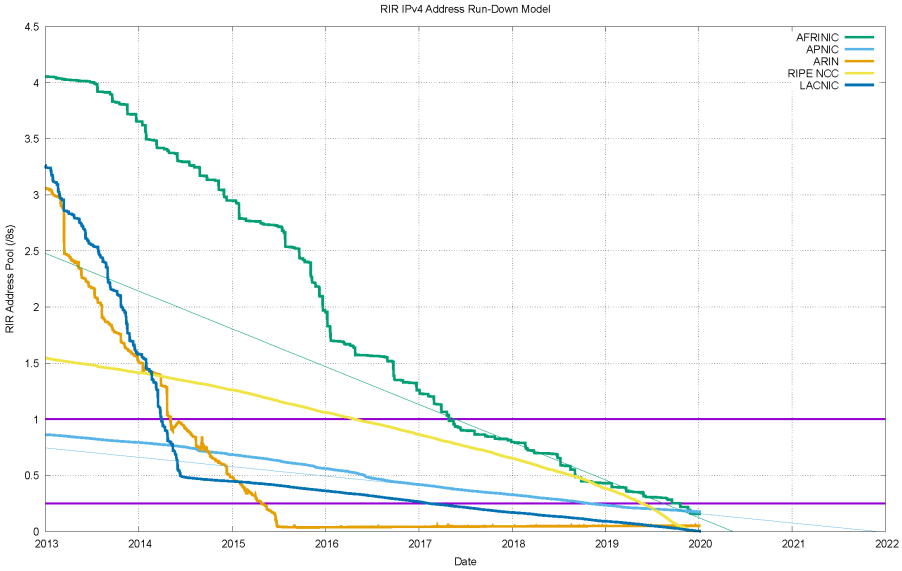


Figura 2.3 Disponibilidad de direcciones IPv4 hasta 2020 para los distintos Registros Regionales de Internet mundiales, y modelos predicción para el futuro (fuente: APNIC) [20].

Para solucionar el problema de falta de disponibilidad de direcciones IPv4, junto a otras mejoras, se ha definido e implementado el protocolo de Internet versión 6 o IPv6.

Protocolo de Internet versión 6 o IPv6

El protocolo de Internet versión 6 o IPv6 supone una mejora del protocolo IPv4 en varios aspectos, el cual quiere reemplazar completamente.

El cambio más notorio consiste en el aumento del tamaño de cada dirección IP a 16 bytes (o 128 bits). Esto quiere decir que hay un total de 2^{128} direcciones IPv6 disponibles.

Los protocolos IPv4 e IPv6 son incompatibles entre sí, por lo que se está realizando una migración que ya está resultando costosa. Se han propuesto formas para simplificar la migración, aunque a día de hoy no hay una solución clara a este problema.

El despliegue de IPv6 aún es bastante escaso. A principios de 2020, RIPE estimó que alrededor del 25 % de las redes soportan IPv6 [21], y Google observó que alrededor del 25 % de sus usuarios accedieron sus servicios con IPv6 [22].

2.1.3 TCP y UDP

Tanto TCP como UDP son protocolos de transporte. Funcionan sobre el protocolo IP (tanto sobre IPv4 como IPv6) y permiten el intercambio de datagramas a través de la red. Habitualmente son usados por una aplicación o un protocolo de aplicación que hace uso de estos para el envío de datos a través de la red.

Hay diferencias notables entre ambos:

- UDP no garantiza que la entrega del datagrama se vaya a producir. No requiere el establecimiento de conexión, no implementa control de flujo ni control de congestión. Es usado por protocolos como DNS o DHCP.
- TCP es orientado a conexión, garantiza la entrega del datagrama, e implementa control de flujo y control de congestión. Es usado por protocolos como HTTP y SSH.

Ambos protocolos comparten rango de puertos válidos (de 1 a 65535), no obstante no hay relación entre estos. Es decir, puede haber un servidor TCP funcionando en el mismo número de puerto que UDP.

2.1.4 El sistema de nombres de dominio o DNS

El sistema de nombres de dominio o DNS es un sistema de resolución de nombres de dominio en direcciones IP, para equipos conectados a Internet o a una red privada [23].

De esta forma, permite relacionar una o más direcciones IP asociadas a un equipo en la red, con un nombre de dominio. Esto simplifica el acceso a recursos en Internet o redes privadas a humanos, puesto que es mucho más fácil de memorizar `google.com` que alguna de sus direcciones IPv4 (p. ej. `91.126.225.225`) o IPv6 (p. ej. `2a00:1450:4003:80a::200e`).

Las comunicaciones DNS se producen habitualmente por UDP, aunque en ciertos casos se puede hacer uso de TCP [24]. Para ambos casos, la IANA tiene asignado el puerto 53.

Jerarquía del sistema de nombres de dominio

El sistema de nombres de dominio tiene una topología en árbol, donde un nombre de dominio consiste en la concatenación de todos los nodos en un camino, separando cada una con puntos. Los dominios terminan en punto, aunque normalmente se omite, ya que es puramente formal.

Un ejemplo de un nombre de dominio correctamente formado o FQDN es `es.wikipedia.org.` (incluyendo el punto final), y su árbol DNS se representa a continuación. Nótese que se representa de derecha a izquierda, comenzando el árbol arriba.

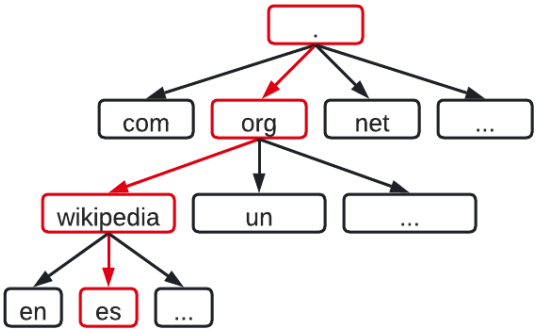


Figura 2.4 Ejemplo de jerarquía DNS del dominio o FQDN es.wikipedia.org.

Tipos de servidores DNS

Hay cuatro tipos de servidores DNS; solucionadores recursivos, servidores raíz, servidores de nombres de dominio de nivel superior y servidores autoritativos [25].

Un solucionador de nombres de dominio o solucionador recursivo es un servidor responsable de gestionar todas las peticiones DNS que les lleguen y responder con el registro buscado. Dicho de otra forma, un cliente delega en el solucionador la responsabilidad de resolver una consulta DNS. Si se hubiese realizado una petición para el mismo nombre de dominio recientemente, se puede agilizar la respuesta mediante almacenamiento caché. Ejemplos conocidos de solucionadores son `8.8.8.8` y `8.8.4.4` de Google, o `1.1.1.1` de CloudFlare.

En el árbol DNS, el nodo `.` representa el servidor raíz. Existen un total de 13 organizaciones que gestionan servidores raíz [26] y son conocidos por todos los sistemas de resolución de nombres, ya que son la primera parada en una búsqueda de un solucionador para resolver una consulta DNS. Una vez recibida una petición válida para la resolución de un nombre de dominio por parte de un solucionador, responde indicando un servidor de nombres de dominio de nivel superior con el que consultar.

Un servidor de nombres de dominios de nivel superior o servidor de nombres TLD mantiene la información sobre todos los nombres de dominio de una extensión específica, como `.com` o `.org`. Recibida la petición por parte del solucionador, responde indicando el servidor de nombres autoritativo para ese dominio, en caso de ser válido.

La consulta a un servidor autoritativo es el último paso en la cadena de peticiones requeridas para resolver un nombre de dominio. Este almacena los registros DNS de un listado de dominios específico [27]. Un registro DNS en el servidor autoritativo puede ser referido a otro servidor, con lo que sería necesario realizar otro salto más.

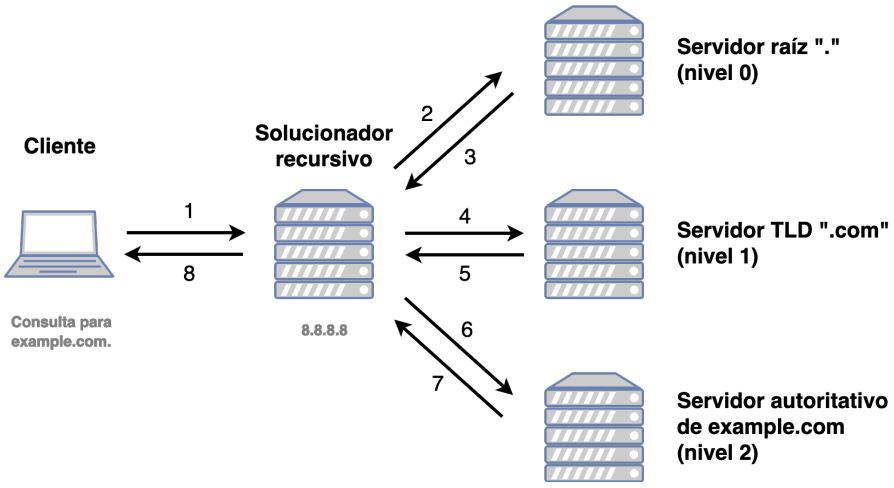


Figura 2.5 Listado de peticiones necesarias para resolver el nombre de dominio example.com.

Registros DNS

Hay muchos tipos de registro DNS, pero los más interesantes y los más relevantes para este proyecto son los siguientes:

- `A`: Registro de dirección. Asocia un nombre de dominio a una serie de direcciones IPv4. Por ejemplo, permite asociar `google.com` a la dirección IPv4 `91.126.225.225`.
- `AAAA`: Registro de dirección. Asocia un nombre de dominio a una serie de direcciones IPv6. Por ejemplo, permite asociar `google.com` a la dirección IPv6 `2a00:1450:4003:80a::200e`.
- `CNAME`: Registro de nombre canónico. Asocia un alias a un nombre de dominio. Por ejemplo, es muy usado para que un nombre de dominio como `www.example.com` se asocie con `example.com`.
- `NS`: Registro de servidores DNS. Permite asociar un nombre de dominio con un servidor DNS autoritativo para ese dominio.
- `MX`: Registro de intercambio de correo. Asocia un dominio a una serie de intercambio de correo. De esta forma, se permitiría el uso de direcciones de correo con el sufijo `@example.com` para los servidores especificados en el registro.
- `TXT`: Registro de texto. Permite almacenar un campo de texto asociado al dominio que no afecte a la resolución.

2.1.5 HTTP y la World Wide Web

HTTP, o protocolo de transferencia de hipertexto, es un protocolo de aplicación que permite la transferencia de datos entre dos participantes. Está basado en TCP y el puerto asignado por IANA para servidores HTTP es el 80.

Aplicación	HTTP
Transporte	TCP
Red	IP

Figura 2.6 Torre de protocolos de HTTP.

Fue creado por Tim Berners-Lee en 1989 mientras trabajaba en el CERN, junto a la definición inicial de HTML y URI, los cuales permitieron el desarrollo de la red informática mundial (más conocida como World Wide Web o WWW).

Estas especificaciones se siguen desarrollando activamente hoy día, y debemos a todas estas tecnologías una parte importante de la revolución digital que se ha producido en estos últimos años.

La versión más utilizada es HTTP/1.1 que está descrito por RFC2616[1], aunque ya está disponible HTTP/2.0[2]. HTTP/2 es más eficiente que la versión previa, sin embargo, el soporte empezó a aparecer en 2015 para la mayoría de navegadores populares[3].

Como HTTP/1.1 es la versión dominante hoy día, el proyecto se centrará en ella.

Funcionamiento de HTTP/1.1

El protocolo de nivel de aplicación HTTP sigue una arquitectura cliente-servidor, donde el servidor ofrece un recurso basado en la URI pedida por el cliente.

Es un protocolo de texto, lo que significa que tanto las peticiones como respuestas son fácilmente legibles [28].

Formato de petición HTTP

Hay varios tipos de peticiones en HTTP, las que más interesan suelen ser las siguientes:

- `GET`: Petición típica, que permite obtener un recurso desde un servidor web.
- `HEAD`: A diferencia del anterior, solo muestra las cabeceras de HTTP.
- `POST`: Permite realizar una petición con datos a un recurso específico, en el cuerpo de la petición. Útil para páginas con formularios.
- `PUT`: Pensado para crear un nuevo recurso, o reemplazar uno ya existente. Es similar a `POST`, ya que los datos se encuentran en el cuerpo de la petición.
- `DELETE`: Utilizado para eliminar un recurso existente.

A continuación se describe un ejemplo de una petición muy sencilla de HTTP:

Código 2.1 Ejemplo de una petición HTTP para obtener http://example.com.

```
GET / HTTP/1.1
Host: google.com
Accept: */*
```

De forma bastante fácil se puede realizar una petición HTTP con el programa `telnet`, al servidor de `example.com` para la página principal (o recurso `/`). Nótese el doble salto de línea después de la última línea de cabecera.

Código 2.2 Ejemplo de cliente HTTP vía Telnet para obtener http://example.com.

```
$ telnet example.com 80
Trying 93.184.216.34...
Connected to example.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: example.com
Accept: */*
```

El programa `telnet` permite ejecutar fácilmente una petición HTTP, introduciéndola carácter a carácter tras la línea `Escape character is '^]'`. Nótese que en HTTP, las peticiones finalizan con un doble salto de línea, que permite determinar que se ha introducido. Por ello, es necesario pulsar botón `Enter`

[1] HTTP/1.1: https://tools.ietf.org/html/rfc2616
[2] HTTP/2.0: https://tools.ietf.org/html/rfc7540
[3] Soporte de HTTP/2 basado en versiones de navegadores y fechas de actualización: https://caniuse.com/#feat=http2

dos veces para introducir tras introducir la última línea de la petición. Consecuentemente, el servidor ofrece la respuesta.

Formato de respuesta HTTP

La primera línea de HTTP nos muestra el estado de petición. HTTP tiene cinco tipos de respuesta o estado, que se representan con números de tres cifras [29]:

- `1xx` (por ejemplo, `100 Continue`): Informativa.
- `2xx` (por ejemplo, `200 OK`): Respuesta satisfactoria.
- `3xx` (por ejemplo, `302 Found`): Redirecciones.
- `4xx` (por ejemplo, `404 Not Found`): Errores, en el lado del cliente.
- `5xx` (por ejemplo, `500 Internal Server Error`): Errores, en el lado del servidor.

Con el ejemplo usado en el apartado anterior, se obtiene una respuesta como la siguiente:

Código 2.3 Respuesta a petición para obtener http://example.com.

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Tue, 19 Nov 2019 13:38:11 GMT
Etag: "3147526947+gzip"
Expires: Tue, 26 Nov 2019 13:38:11 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (nyb/1D04)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256

<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "
            Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
```

```
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may
        use this
    domain in literature without prior coordination or asking for permission.</
        p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></
        p>
</div>
</body>
</html>
```

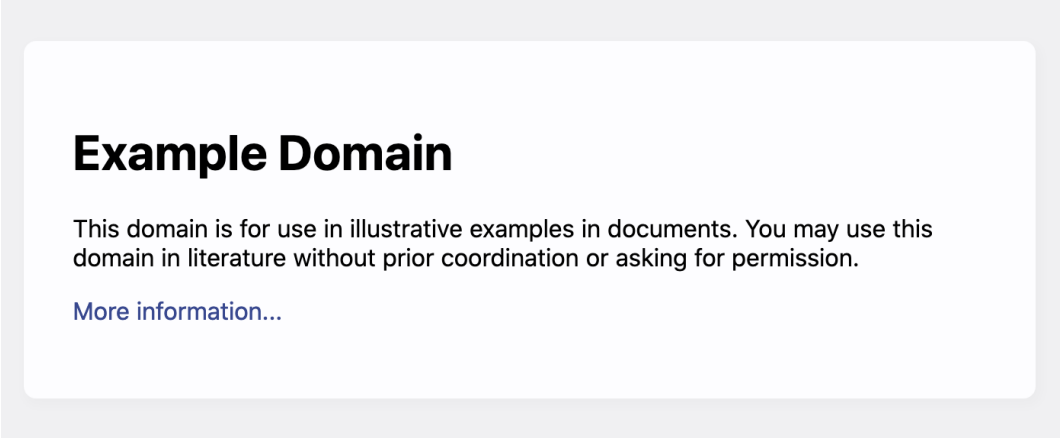


Figura 2.7 Captura de pantalla de http://example.com usando el navegador Web Firefox 70.0.1.

Dominios como example.com, example.net, example.org entre otros, están reservados por la IANA para ser utilizados como ejemplos para documentación [30].

2.1.6 HTTPS

HTTPS es el protocolo seguro de transferencia de hipertexto. Está basado en HTTP, ya que semánticamente es idéntico a este, pero funciona sobre una capa de cifrado basado en TLS o SSL, que a su vez funciona sobre TCP. El puerto asignado por IANA para HTTPS es el 443.

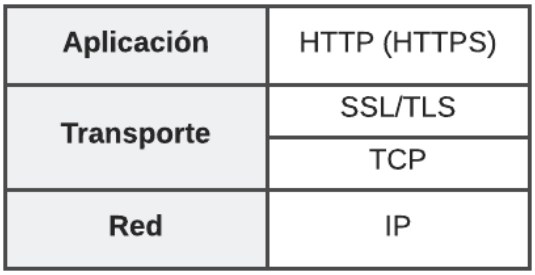


Figura 2.8 Torre de protocolos de HTTPS.

Con ello, y siempre que se tomen las precauciones de seguridad apropiadas tanto en el cliente como servidor, se puede conseguir una comunicación segura a pesar de que se produzca a través de un canal de comunicaciones inseguro. Así se evita que un atacante pueda obtener datos sensibles de usuarios, credenciales y contraseñas, números de tarjetas de crédito, etc.

Es importante destacar que aunque el contenido de la comunicación no se pueda conocer, debido al diseño de los protocolos sobre los que funciona HTTPS, sí que es posible identificar tanto al cliente y servidor de la comunicación.

En la siguiente sección se introducirán conceptos que permitirán conocer mejor el funcionamiento de este protocolo, así como describiendo los métodos de seguridad utilizados y problemas como el descrito en el párrafo anterior.

2.1.7 Navegadores Web

Un navegador Web es un tipo de cliente Web capaz de acceder y representar recursos de un servidor Web, tal como ficheros y páginas Web, apoyándose tecnologías Web (como HTTP o HTML).

Tras la publicación de las tecnologías World Wide Web, se lanzó un navegador Web primitivo desarrollado por Tim Berners-Lee. Posteriormente, fueron apareciendo distintos navegadores que ganaron popularidad, entre los que se puede destacar Mosaic (1993) y Netscape (1994) que se hicieron ampliamente populares.

En la actualidad, los navegadores Web más populares son los siguientes [31]:

- Google Chrome: Desarrollado por Google y lanzado en 2008, se ha convertido en el navegador Web más popular por su simplicidad y rapidez. Está basado en Chromium, un proyecto de Google de código abierto.
- Safari: Desarrollado por Apple para sus sistemas operativos (macOS e iOS), es el navegador mayoritario en estas plataformas. A pesar de ser de código cerrado, su motor WebKit es de código abierto y ha servido de base para el desarrollo de varios navegadores Web, como Google Chrome [32].
- Mozilla Firefox: El navegador de código abierto más utilizado, depende en última instancia de la fundación sin ánimo de lucro Mozilla. Origina del navegador Netscape, líder antes de la irrupción de Internet Explorer, tras la publicación de su código fuente en 2003.
- Microsoft Edge: Desarrollado por Microsoft, es el navegador por defecto de Microsoft Windows. Es un remplazo a Microsoft Internet Explorer, el navegador Web de Microsoft Windows desde 1995, que tuvo un pico de 95% en cuota de mercado en 2003 [33].
- Opera: Es un navegador desarrollado por la empresa noruega Opera Software. Lanzado inicialmente en 1996, es el navegador Web más antiguo actualmente siendo mantenido activamente, y es conocido por implementar variedad de características que luego han aparecido en otros navegadores (como navegación privada, bloqueo de pop-ups, navegación por pestañas, etc.).

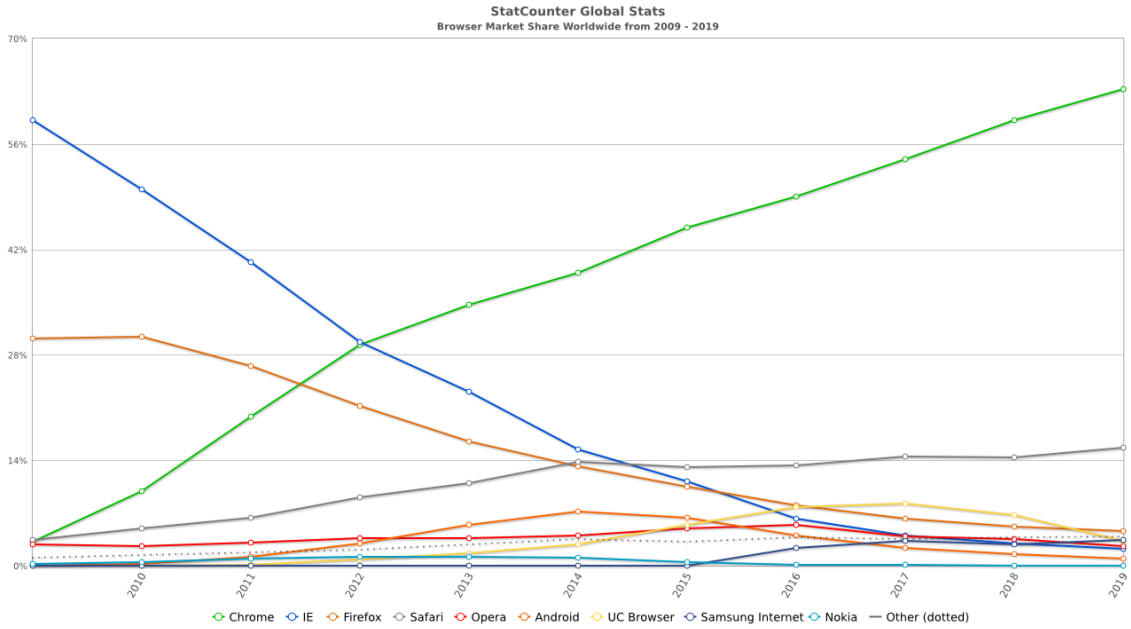


Figura 2.9 Evolución de cuota de mercado de los navegadores Web más populares (fuente: StatCounter) [34].

Los navegadores Web más populares están disponibles tanto en plataformas de escritorio (ordenadores) como móviles (teléfonos móviles y tabletas). Con la irrupción y el crecimiento en uso de los sistemas operativos móviles iOS y Android, ha permitido que la cuota de mercado de los navegadores Web en estas plataformas haya pasado de ser prácticamente irrelevante en 2009 a superar el 50% en 2019.

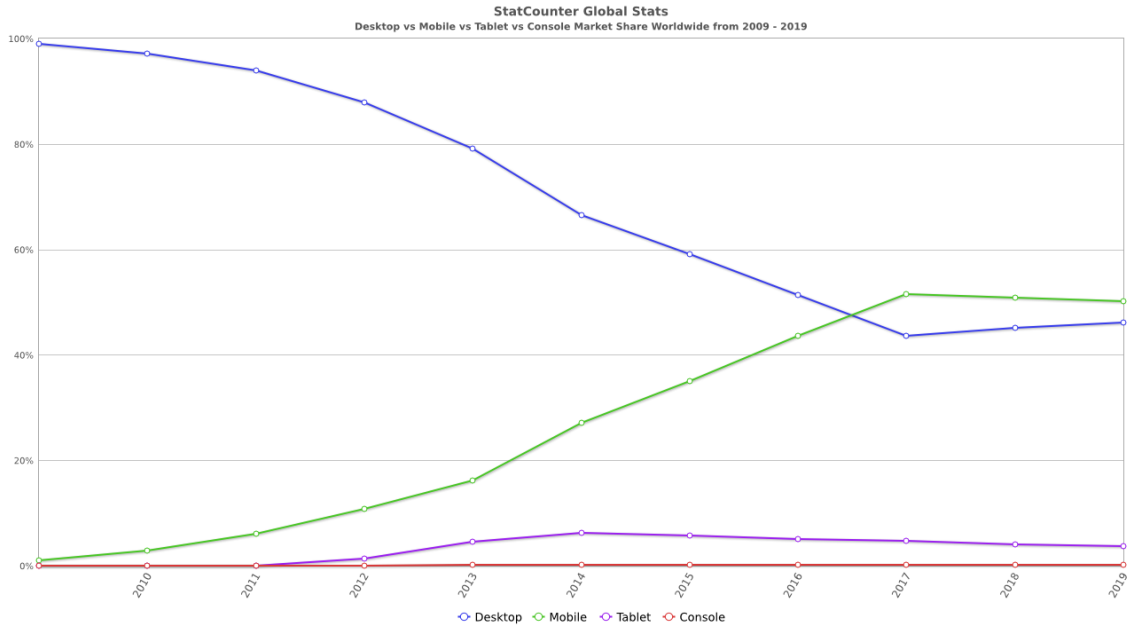


Figura 2.10 Evolución de la cuota de mercado de las distintas plataformas en la Web (fuente: StatCounter) [35].

2.1.8 Servidores Web

Un servidor Web es un software capaz de escuchar y servir peticiones HTTP de clientes Web. Puede tener variedad de funcionalidades; por ejemplo, servir páginas web, actuar de proxy o balanceador de carga,

permitir consultar o gestionar bases de datos (por ejemplo, Apache CouchDB), etc.

El primer servidor Web fue publicado por Tim Berners-Lee el 1991, denominado CERN httpd aunque fue rápidamente discontinuado [36]. Los servidores Web más populares hoy día son [37]:

- Apache: Basado en el servidor `httpd` de NSCA tras la paralización de su desarrollo y publicado en 1995, es uno de los primeros servidores Web, y uno de los navegadores Web más populares. Tiene una gran variedad de funcionalidades y es fácilmente extensible mediante el uso de módulos.
- NGINX: Publicado en 2004, se desarrolló para resolver el problema de las 10.000 conexiones simultáneas al mismo tiempo, es decir, para soportar una alta carga de clientes al mismo tiempo. Ha ganado popularidad por su eficiencia y extensibilidad, y actualmente es el navegador Web más usado en todo Internet.
- Microsoft IIS: Servidor Web diseñado para funcionar en los sistemas operativos Microsoft Windows basados en Windows NT. Está plenamente integrado con las funcionalidades del sistema operativo y cuyo software por defecto funciona con interfaz gráfica.

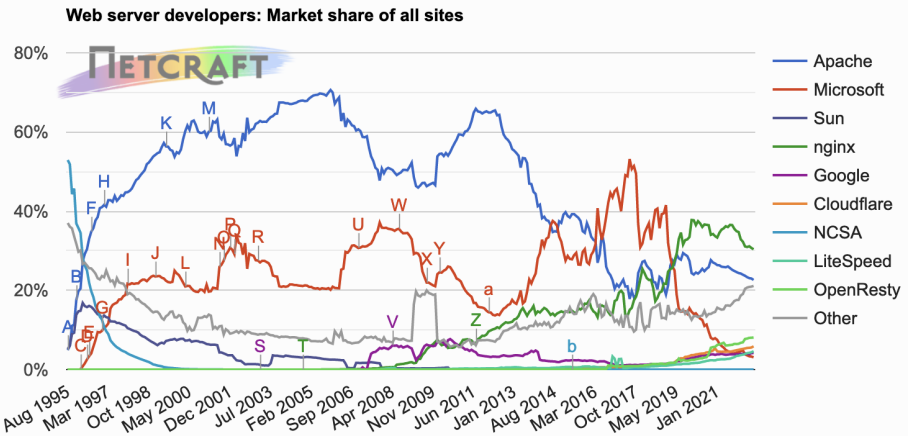


Figura 2.11 Evolución de la cuota de mercado de los distintos servidores Web, hasta junio del 2022 (fuente: Netcraft) [38].

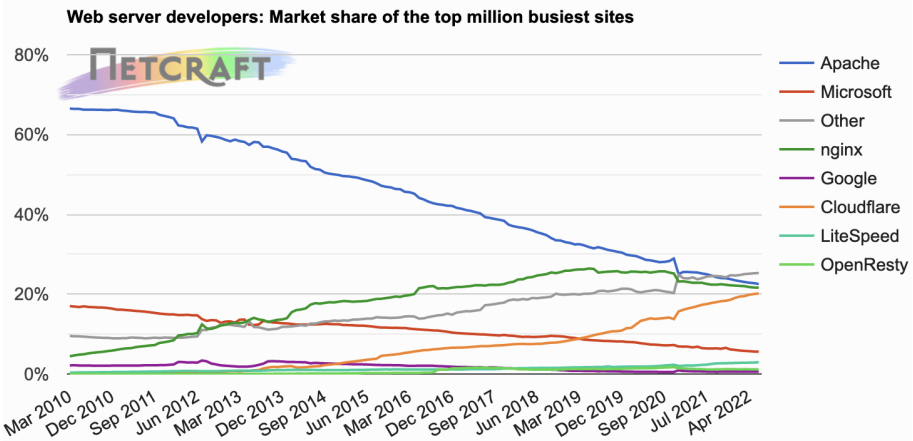


Figura 2.12 Evolución de la cuota de mercado de los distintos servidores Web del millón de sitios Web más activos, hasta junio del 2022 (fuente: Netcraft) [38].

2.2 Seguridad de las comunicaciones en Internet

Para lograr comunicaciones seguras en Internet es necesario estudiar criptografía y técnicas de cifrado, que permitan ocultar intencionadamente un contenido por un canal, que pueda ser revelado por el receptor deseado, y de una forma óptima.

A continuación se describirá la teoría necesaria para comprender los fundamentos criptográficos en los que se basa HTTPS, y que permita una total comprensión de lo que se puede lograr con el proyecto.

2.2.1 Criptografía

La criptografía, en la rama de la informática, es la técnica que busca ocultar el contenido de un mensaje de forma que solo pueda ser conocido por un grupo de destinatarios específicos, mediante técnicas de codificado y/o cifrado [39].

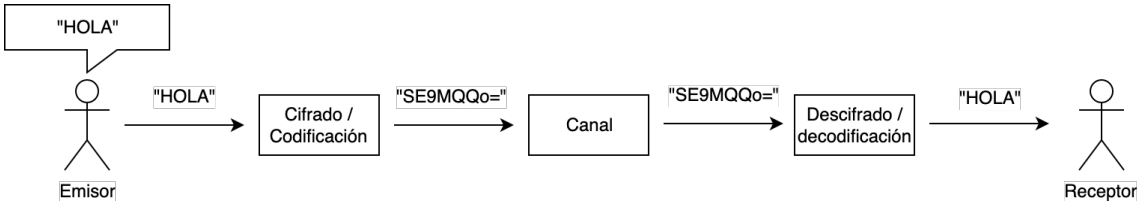


Figura 2.13 Ejemplo de criptografía con un emisor y receptor (algoritmo Base64).

En la figura anterior, el emisor envía un mensaje por el canal al receptor que está codificado (en este caso en Base 64), y no es legible hasta que se decodifique. Este ejemplo específico no es seguro, puesto que otros participantes podrían comprender fácilmente que se está transmitiendo en Base 64, y decodificar el mensaje.

Debido a que el canal de comunicaciones entre cliente y servidor no se puede controlar, como se ha establecido anteriormente, para establecer una comunicación segura es necesario proteger los mensajes mediante técnicas de codificado y/o cifrado, es decir, mediante la aplicación de criptografía.

2.2.2 Cifrado

El cifrado es una técnica que, basándose en un algoritmo de cifrado, es capaz de transformar un mensaje en otro diametralmente distinto, con una clave de cifrado.

Los algoritmos de cifrado se aseguran que romper la protección de un mensaje no sea computacionalmente sencillo, siempre que se sigan las recomendaciones en el uso de claves de cifrado.

Así, una clave de cifrado permite proteger el mensaje, que puede ser comunicado por un canal inseguro sin riesgo de filtrar información confidencial. Una vez en el destino, se puede revelar fácilmente con una clave de descifrado.

Las claves para el cifrado y descifrado pueden ser iguales (cifrado simétrico), diferentes (cifrado asimétrico) o hacer uso de claves de ambos tipos (cifrado híbrido), y a continuación se procederá a describir cada uno de ellos.

Cifrado simétrico

Un sistema de cifrado simétrico es aquel que permite cifrar un mensaje con una clave de cifrado. Para descifrar el mensaje, es necesario hacer uso de la misma clave.

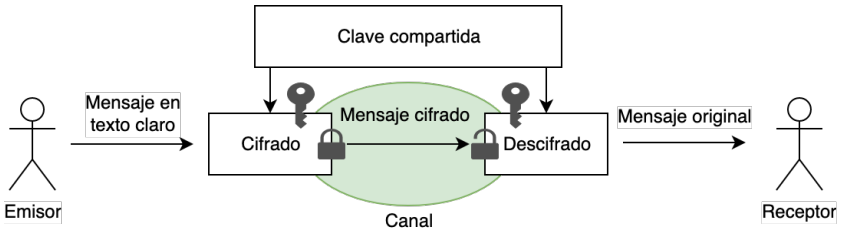


Figura 2.14 Cifrado simétrico, donde los mensajes se cifran con una única clave compartida.

Se pueden diferenciar los siguientes tipos de sistemas de cifrado simétrico:

- Con clave compartida fija: La clave compartida es conocida de antemano por los participantes.
- Con clave compartida dinámica: No hay una clave preestablecida, por lo que es única por conexión o sesión.

Para utilizar un sistema de cifrado simétrico con clave dinámica, es necesario acordar una clave común. Esto se puede lograr con criptografía híbrida, que se verá posteriormente, o con un protocolo de establecimiento de claves.

Un protocolo de establecimiento de claves, también denominado protocolo de intercambio de claves, permite a dos o más interlocutores decidir una clave de cifrado entre ellos, a través de comunicaciones públicas, sin que estas permitan determinar la clave resultante. El protocolo más popular de este estilo es el algoritmo Diffie-Hellman, y se basa en propiedades matemáticas de los números primos.

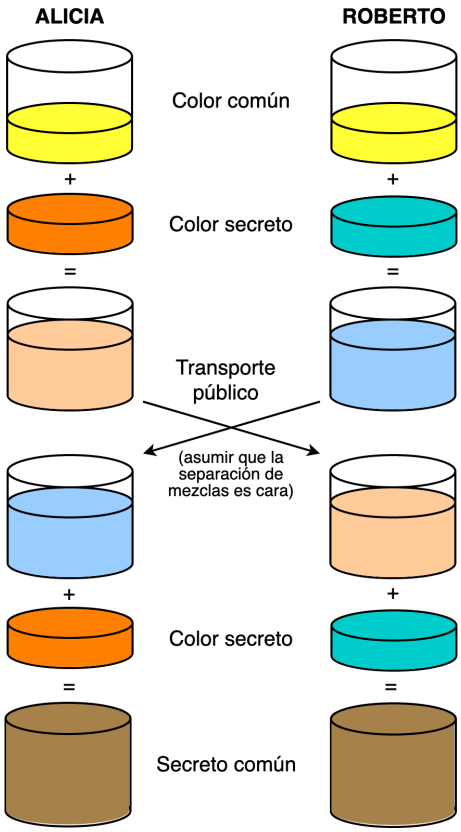


Figura 2.15 Explicación visual de un algoritmo de establecimiento de claves basado en colores de pintura.

Una vez conocida la clave, se debe establecer un algoritmo de cifrado. Algunos ejemplos son AES, DES, 3DES (o Triple DES) y Blowfish.

Cifrado de clave pública o cifrado asimétrico

Un sistema de cifrado de clave pública, también denominado cifrado asimétrico, es aquel donde se cifra un mensaje con una clave, pero el descifrado se realiza con una clave distinta.

La clave utilizada para cifrar el mensaje es denominada clave pública, ya que puede ser compartido públicamente sin que suponga un problema. A la clave que permite descifrar el mensaje se le denomina clave privada, debido a que no debe ser compartida (permitiría a otros usuarios descifrar el mensaje).

Se pueden destacar los algoritmos de cifrado de clave pública RSA, cuyo algoritmo de generado de claves se basa en propiedades matemáticas de los números primos. En particular, este permite cifrar mensajes con la clave privada y descifrar con la clave pública. Esto se aprovecha en multitud de sistemas para realizar una comunicación bidireccional, con un único par de claves de cifrado asimétrico.

Es importante notar que hay una relación matemática entre las claves pública y privada, y hay una relación uno-a-uno entre estas. Por diseño, es posible obtener la clave pública de la clave privada, pero no al revés.

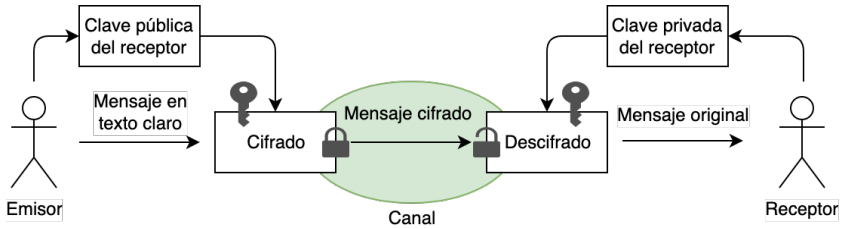


Figura 2.16 Cifrado asimétrico, donde una clave cifra el mensaje y otra clave lo descifra.

En la figura anterior, se observa que el emisor cifra el mensaje con la clave pública del receptor. Para que esto se pueda producir, es necesario que el receptor comunique al emisor su clave pública. No obstante, esto se puede hacer en texto plano gracias a que la clave privada no puede obtenerse de la pública.

En un sistema de cifrado de clave pública es habitual la existencia de una autoridad de certificación, que sea capaz de ofrecer un certificado de clave pública con la que sea posible verificar la autenticidad de la entidad que dispone de la clave pública.

Una autoridad de certificación es una entidad de confianza, responsable de emitir y revocar certificados utilizando firma electrónica, mediante el uso de criptografía de clave pública. Son usadas principalmente para garantizar la seguridad de comunicaciones cifradas, así como para resguardar documentos digitales.

Un certificado de clave pública o certificado X.509 es un tipo de documento digital firmado por una autoridad de certificación, y asocia una clave pública a una entidad que posee la clave privada asociada. Se describe en el estándar X.509 de la UIT-T.

Cifrado híbrido

Un sistema de cifrado híbrido es aquel que hace uso simultáneo de criptografía simétrica y criptografía asimétrica para el cifrado de un mensaje.

Así, en una comunicación, el receptor del mensaje original antes debe compartir su clave pública con el emisor. El emisor luego genera una clave simétrica aleatoria (única por conexión o sesión) que comparte con el receptor cifrado con la clave pública. A partir de este momento, cualquier comunicación estará cifrada con la clave simétrica generada.

Ejemplos conocidos de sistemas de cifrado híbrido son PGP, GnuPG, además de HTTPS, que es en el que nos centraremos en este proyecto.

Lo que se logra con este tipo de cifrados es que un emisor no necesite conocer de antemano ninguna clave, al obtenerse durante el proceso de establecimiento de comunicación.

A diferencia de un protocolo de establecimiento de claves, usar cifrado híbrido permite comprobar la autenticidad de un participante a través de la verificación de su clave pública. Posteriormente, se verá el caso detallado de HTTPS.

2.2.3 Cifrado en TLS y SSL

El protocolo Transport Layer Security o TLS, y su antecesor Secure Sockets Layer o SSL, son protocolos de criptográficos que tienen el fin de ofrecer comunicaciones seguras en una red, habitualmente Internet.

Se basan en criptografía híbrida, ya que utilizan cifrado asimétrico para fines de autenticación y envío de información inicial sensible, y cifrado simétrico para proteger el resto de comunicaciones.

El protocolo SSL, que es predecesor de TLS, se considera deprecado debido a que todas sus implementaciones públicas se han demostrado inseguras. Por ello, de aquí en adelante, el proyecto solo hará mención de TLS.

Las conexiones de TLS pasa por un proceso denominado handshake [40], que consta de los siguientes pasos:

- Negociación de conjuntos de cifrado.
- Autenticación.
- Creación o intercambio de claves de cifrado simétrico para la sesión.

Con TLS 1.2 y anteriores, las comunicaciones anteriores se realizan en dos rondas. Sin embargo, en TLS 1.3 se ha simplificado el proceso y se alcanza con una única ronda.

Negociación de conjuntos de cifrado

Un conjunto de cifrado es un conjunto de algoritmos de cifrado usados para proteger una serie de comunicaciones realizadas con TLS. Se compone de un algoritmo de intercambio de claves (como Diffie-Hellman [41]), un algoritmo de autenticación del servidor (como RSA), un algoritmo de cifrado (como AES) para proteger la comunicación y un algoritmo de autenticación de mensajes (como SHA1) para permitir verificar la autenticidad de los mensajes intercambiados.

Hoy día existe una multitud de conjuntos de cifrado, principalmente debido a todas las configuraciones habituales, la variedad de clientes o navegadores Web existente y la cantidad de servidores Web utilizados.

De forma no cifrada, el cliente y servidor Web acuerdan un conjunto de cifrado a utilizar, de entre todos los que soportan en común. En caso de no haber ninguno, el proceso de negociación falla y se termina la conexión.

Autenticación

En este proceso, el servidor comunica al cliente su clave pública mediante un certificado de una clave pública.

A continuación, para confirmar la autenticidad del certificado, el cliente realiza varias comprobaciones como verificar la firma digital, la fecha de expiración o que desciende del certificado raíz del que dispone.

Finalmente, el cliente comprueba que el servidor realmente dispone del certificado que dice tener. Para ello, envía una clave aleatoria que se usará para cifrar de forma simétrica las siguientes comunicaciones. Si es capaz de obtener este dato, significa que es el dueño de la clave privada, que es la única que permitiría obtenerlo.

Si el conjunto de cifrado elegido utiliza el algoritmo Diffie-Hellman (DH) o su variante Diffie-Hellman efímero (DHE) para generar la clave de cifrado, el servidor comunica al cliente otra semilla con la que ambos podrán construir la clave de cifrado simétrica final. La comunicación se realiza cifrándolo con la clave privada del servidor, y deberá ser descifrada con su clave pública en el lado del cliente. Esto es posible con algoritmos como RSA, como se ha mencionado anteriormente.

Intercambio de claves

La última parte del proceso de handshake [40] TLS consiste en la creación de una clave de sesión, que será única por sesión y que se usará para proteger las comunicaciones.

Es una clave de cifrado simétrica, y permite cifrar de manera mucho más eficiente que si se hubiese hecho uso de una clave asimétrica, por lo que es ideal para la transmisión de datos entre cliente y servidor.

El método utilizado para el intercambio de claves depende del conjunto de cifrado utilizado, y normalmente suele ser RSA o Diffie-Hellman.

2.2.4 Seguridad de comunicaciones con HTTPS

Anteriormente, se ha mencionado que el protocolo HTTPS consiste en el protocolo HTTP funcionando sobre una capa de cifrado TLS. Estos protocolos requieren que el servidor disponga de un certificado de clave pública y una clave privada asociada, de forma que pueda verificarse la autenticidad del dueño de estas claves.

Debido a que las comunicaciones están cifradas y no se transmiten en texto plano, es necesario hacer uso de programas específicos para establecer una comunicación, como `openssl`.

En el caso de un servidor HTTPS, basta con establecer una conexión con el comando siguiente. Una vez hecho, se introducirá la petición terminando en salto de línea doble, ya que semánticamente es idéntico a HTTP.

Código 2.4 Ejemplo de cliente TCP vía OpenSSL para conexión con https://example.com.

```
$ openssl s_client -connect example.com:443
```

Este comando realiza el procedimiento de handshake de TLS, y la salida se analiza detalladamente en el Apéndice C.

Por ejemplo, se podría introducir el Código 2.2 y se obtendría el mismo resultado.

2.3 Autoridades de certificación

Actualmente, existe una cantidad limitada de autoridades de certificación soportada por todos los navegadores Web más populares, todas integradas en el Foro de Autoridades de Certificación y Navegadores o CA/Browser Forum [42].

El Foro Autoridades de Certificación y Navegadores o CA/Browser Forum es un consorcio formado voluntariamente por autoridades de certificación, responsables de desarrollo de los navegadores Web más populares, de sistemas operativos y otras organizaciones implicadas en desarrollo de aplicaciones basadas en infraestructuras de clave pública.

Su misión consiste en promulgar las pautas para la emisión y gestión de certificados digitales X.509 v3 que puedan ser considerados de confianza.

2.3.1 Proceso de certificación

Para obtener un certificado de clave pública asociado a una clave privada, es necesario crear una solicitud de firma de certificado o CSR. Este fichero contiene la clave pública e información que permiten identificar a la entidad que quiere obtener el certificado.

La certificación habitualmente tiene un coste monetario, y requiere un proceso de verificación para confirmar la validez de los datos provistos en la solicitud de firma del certificado. Este proceso culmina con la obtención de un certificado de la clave pública y asociado a una entidad.

Si la autoridad de certificación es reconocida por el Foro Autoridades de Certificación y Navegadores, y se accede por el dominio asociado al certificado, sería reconocido como válido en los navegadores Web más populares, siempre que el certificado no haya sido revocado y no haya expirado.

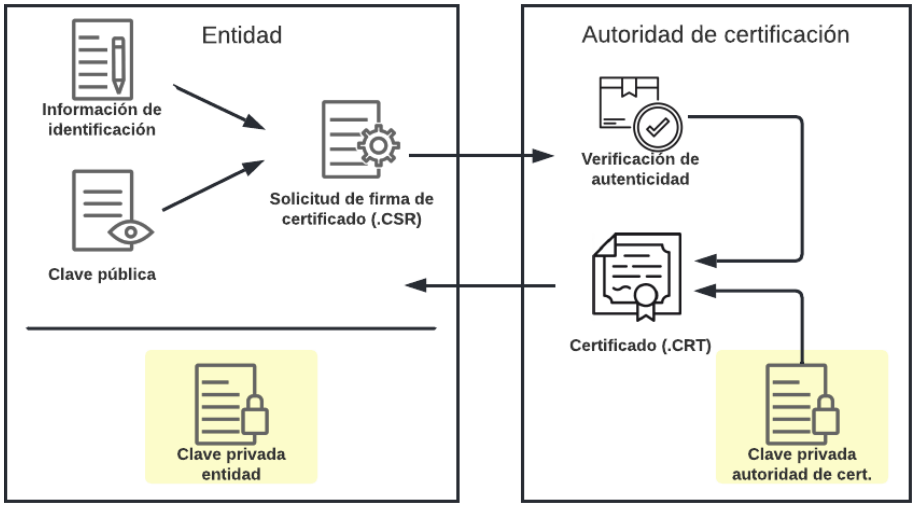


Figura 2.17 Procedimiento de obtención de un certificado de una clave pública.

2.3.2 Let's Encrypt

Let’s Encrypt es una autoridad de certificación constituida en 2016, y que ofrece certificados X.509 de forma gratuita para el cifrado con TLS.

Constituye junto a CACert.org las dos únicas autoridades de certificación existentes sin ánimo de lucro [43].

A diferencia de CACert.org, los certificados de Let’s Encrypt sí son reconocidos por todos los navegadores modernos, y ello se debe a que utilizan un certificado intermedio firmado por la autoridad de certificación IdenTrust. Es además respaldado por importantes organizaciones como la Fundación Mozilla, EFF, Google o Internet Society.

Gracias a ello, Let’s Encrypt ha alcanzado cuotas de uso muy elevadas, y se estima que en 2022, más del 50 % de todos los certificados de la Web son firmados por Let’s Encrypt [44].[4]

[4] En 2015, los certificados de IdenTrust representaban menos del 0.1 % de todos, con lo que actualmente se puede justificar todo el crecimiento a Let’s Encrypt, para quien firma las claves intermedias [45].

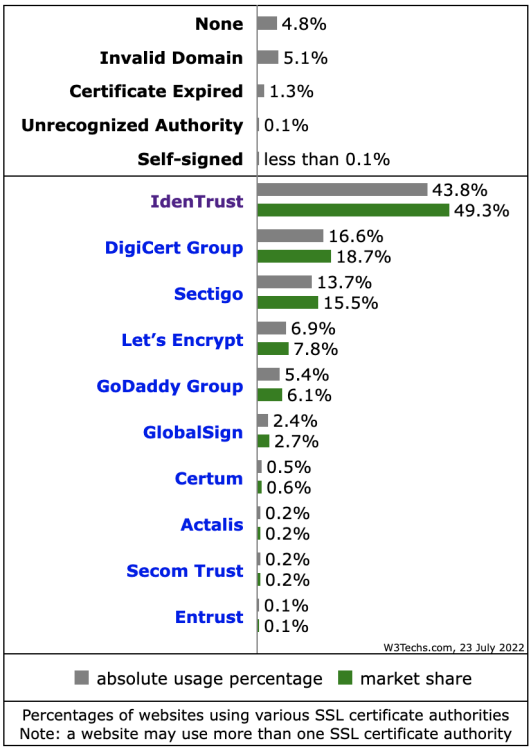


Figura 2.18 Estimación del uso de autoridades de certificación (fuente: W3Techs.com) [44].

Funcionamiento de Let's Encrypt

Para crear un certificado con Let's Encrypt basta tener los siguientes datos:

- Una lista de dominios para las cuales se desea crear el certificado.
- Una dirección de correo electrónico, donde se enviarán notificaciones sobre la caducidad del certificado.

Let's Encrypt utiliza el protocolo ACME versión 2 para automatizar las comunicaciones entre servidor y autoridad de certificación a efectos de crear y gestionar el certificado. Gracias a este protocolo, es posible crear, renovar y revocar certificados de forma automatizada.

Por diseño, los certificados con Let's Encrypt están pensados para tener una validez máxima de 90 días (o 3 meses). La intención detrás de esta decisión consiste en forzar a los administradores de sistema a automatizar la renovación de los certificados.

Retos para verificación de dominios

Los procesos de validación de Let's Encrypt se realizan con el protocolo ACME.

Primero se comprueba que no se haya superado ningún límite [46]. Por ejemplo:

- Límite de 5 validaciones falladas por cuenta, dominio y hora.
- Límite de 10 cuentas por dirección IP, en 3 horas.
- Límite de 50 certificados por dominio, en una semana.

Para fines de desarrollo donde los límites pueden suponer un problema, Let's Encrypt dispone de un servidor staging, donde los límites son considerablemente superiores. No obstante, los certificados generados no son reconocidos por navegadores Web.

A continuación, comprueba que todos los dominios para los que se va a crear el certificado pertenecen al usuario. Esto se realiza con lo que denominan un reto [47], y actualmente soporta tres tipos:

- `TLS-ALPN-01` (por defecto): Se lanza un servicio en el puerto TCP 443 del servidor que ejecuta el cliente de Let's Encrypt, cuyos servidores verifican si el servicio es accesible en la lista de los dominios para los que se quiere crear el certificado. La principal desventaja es su incompatibilidad con los servidores web más populares, y que requiere acceso exclusivo al puerto 443 que puede estar ocupado por uno de estos.

- `HTTP-01`: El funcionamiento consiste en que se crea un fichero temporal con contenido aleatorio en un directorio, y se aprovecha el servidor Web en ejecución para mostrar estos contenidos (lo cual puede requerir una configuración previa). A continuación, los servidores de Let's Encrypt verifican que la ruta al fichero muestra el contenido aleatorio en cada uno de los dominios. A diferencia del anterior, este sí es compatible con los servidores Web más populares.
- `DNS-01`: El cliente Let's Encrypt se comunica con el servidor DNS autoritativo para los dominios, y mediante unas credenciales (habitualmente temporales) es capaz de crear un registro DNS del tipo `TXT` que contiene una clave aleatoria, para cada uno de los dominios. Los servidores de Let's Encrypt posteriormente, verifican que se ha creado esta entrada con el valor específico. La principal ventaja en comparación con los anteriores es que no necesita configurar el servidor web, pero es más difícil de configurar.

Una vez se supera el reto, se genera una clave privada y un certificado válido para todos los dominios especificados.

Clientes de Let's Encrypt

Hay una amplia variedad de clientes de Let's Encrypt. Esto se debe principalmente a que el protocolo de ACME es público, y el código del cliente oficial es de código abierto. Algunos clientes destacados se listan a continuación [48]:

- CertBot: El cliente oficial de Let's Encrypt, de código abierto y escrito en Python. Es el cliente recomendado, debido a que es fácil de usar, está soportado en variedad de sistemas operativos y tiene buena documentación.
- Lego: Cliente escrito en Go, con binario único y fácil de compilar en variedad de plataformas como arquitecturas. Es fácil de usar y tiene buena documentación.

Buenas prácticas para gestión de certificados

Gracias a la facilidad de generar certificados con Let's Encrypt, se pueden listar una serie de buenas prácticas que cualquier página Web debería seguir en cuanto a gestión de sus certificados:

- Forzar el uso de HTTPS: Con el fin de garantizar la seguridad de las comunicaciones realizadas por los usuarios a una página, se recomienda forzar el uso de HTTPS para accesos a la página mediante HTTP [49]. Esto se puede lograr fácilmente forzando una redirección de HTTP a HTTPS y configurando el servidor Web para usar la cabecera HTTP `Strict-Transport-Security`.
- Establecer fecha de caducidad de certificados no muy elevada (como 3 meses): Con el protocolo ACME es bastante sencillo renovar certificados, con lo que es buena práctica aprovechar esto para establecer una rotación frecuente de certificados [50]. Esto permite limitar el impacto causado por un mal uso previo de certificados.
- Renovar certificados forma automatizada: Gracias a que el protocolo ACME permite la renovación automática de certificados utilizando una variedad de cliente, se recomienda automatizar el proceso para evitar que caduque un certificado. Esto se puede lograr fácilmente utilizando clientes como CertBot o Lego, y herramientas de sistema como `cron` para programar la ejecución del comando de renovación.

2.4 Configuración automatizada de HTTPS en servidores Web

Hoy día es posible configurar HTTPS de manera automatizada en servidores Web. Estas son algunas de las herramientas y soluciones que proporcionan tal funcionalidad:

- Caddy [51]: Es un servidor Web que permite configurar, renovar y revocar certificados HTTPS de manera automatizada, y es una alternativa a otros servidores como Apache y NGINX.
- Traefik [52]: Proxy reverso y balanceador de carga para aplicaciones TCP y HTTP, con soporte nativo y automático para certificados Let's Encrypt.

- Kubernetes cert-manager [53]: Permite generar, renovar y revocar certificados HTTPS de manera automatizada usando recursos de Kubernetes, permitiendo una fácil integración con otros componentes como controladores de Ingress.
- Herramienta CertBot de Let's Encrypt [54]: Contiene integraciones opcionales con los servidores Web Apache y NGINX para instalar de forma automatizada nuevos certificados SSL. No obstante, requiere de configuración avanzada para configurar la renovación automatizada del certificado, y solo es compatible con los paquetes de Apache y NGINX instalados vía el gestor de paquetes oficial de distribuciones GNU/Linux basadas en Debian o CentOS.
- Balanceadores de carga de servicios en la nube: Los servicios de hospedaje en la nube suelen ofrecer servicios de balanceo de carga, que permiten instalar por encima un certificado HTTPS gestionado a través del propio servicio, sin necesitar ningún tipo de gestión en el servidor. Por ejemplo, esto es el caso de AWS Certificate Manager con AWS Load Balancer.
- Servicios de protección de ataques de denegación de servicio distribuidos (DDoS), como por ejemplo CloudFlare, permiten instalar un certificado HTTPS gestionado a través del propio servicio.

3 Análisis del estado actual

A continuación se realizará un análisis de la situación actual en Bitnami en cuanto a configuración de HTTPS. Para ello, se analizarán los métodos de configuración recomendados para sus soluciones, buscar sus puntos débiles a través de un análisis de casos de soporte, y realizar una propuesta para solucionar los problemas encontrados.

3.1 Estudio sobre soluciones existentes

Bitnami actualmente provee dos formas para que los usuarios puedan configurar HTTPS usando productos de Bitnami; mediante guías y tutoriales en Bitnami Docs, tanto para Let's Encrypt como para otras autoridades de certificación; y con una herramienta automatizada de generación de certificados que solo es compatible con Let's Encrypt.

3.1.1 Herramienta automatizada para la generación de certificados

Bitnami provee a los usuarios una herramienta automatizada para la generación de certificados, denominada `generate-certificates.sh`. Viene incluida en Bitnami Stacks con servidor Web Apache o NGINX.

Funciones

Esta herramienta necesita que el usuario indique lista de dominios para las cuales desea generar el certificado con la opción `-d`, y el correo electrónico para notificaciones de caducidad de dominios con la opción `-mn`. Realiza las siguientes labores:

- Crear un certificado SSL de Let's Encrypt (mediante la herramienta `lego`).
- Configurar el servidor Web (Apache o NGINX) para usar el certificado recién creado.
- Programar renovación de dominios con Cron.
- Crear copia de seguridad al principio de la ejecución, y restaurar en caso de error grave en cualquier parte del proceso.

A continuación se muestra un ejemplo de uso de `generate-certificates.sh`:

Código 3.1 Ejemplo de uso de generate-certificates.sh para el usuario ejemplo@bitnami.com y dominios ejemplo.bntestdomain.cf y www.ejemplo.bntestdomain.cf.

```
$ sudo /opt/bitnami/lego/scripts/generate-certificates.sh -d ejemplo.
    bntestdomain.cf -d www.ejemplo.bntestdomain.cf -m ejemplo@bitnami.com
```

3.1.2 Documentación, guías y tutoriales

Bitnami provee documentación en inglés para cada uno de sus productos en cada una de las plataformas soportadas[1], así como guías y tutoriales sobre temas determinados en su plataforma Bitnami Docs. Dispone

[1] A excepción de contenedores Docker y plantillas Helm (o Helm charts) para Kubernetes, para los cuales la documentación específica por aplicación se encuentra en repositorios de GitHub

de un equipo específico para el mantenimiento de esta plataforma, y el equipo de ingeniería y soporte colabora activamente con el fin de que toda la información sea correcta y esté al día.

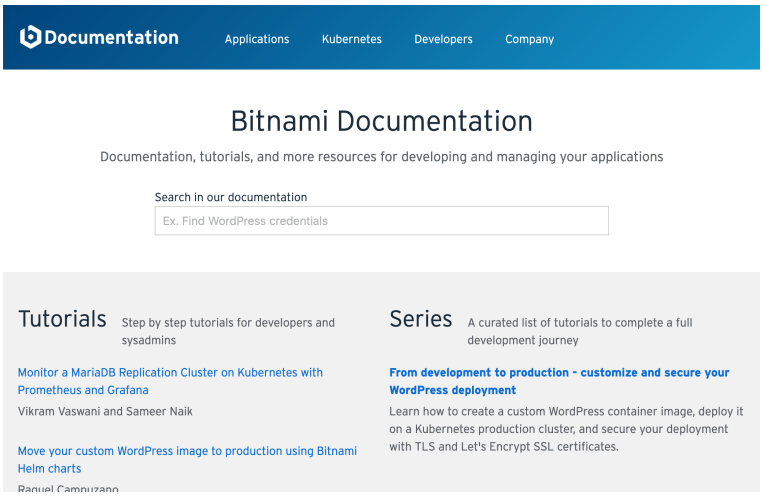


Figura 3.1 Portal de Bitnami Docs.

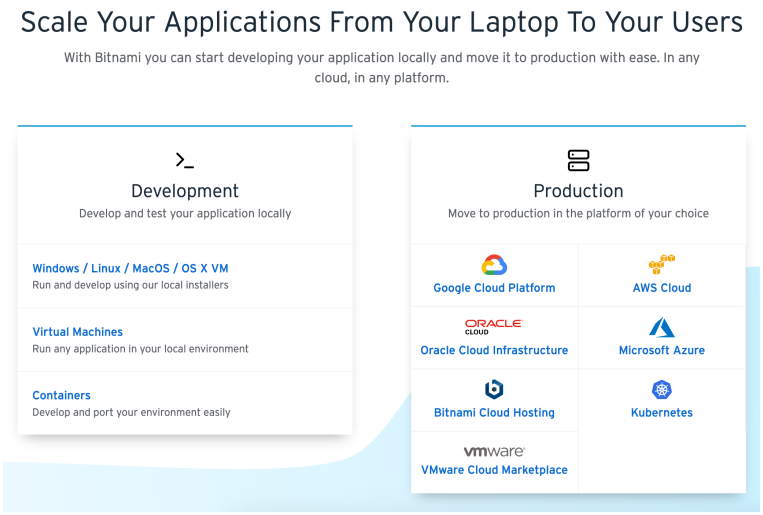


Figura 3.2 Selector de plataforma en Bitnami Docs.

Documentación existente

En lo que respecta configuración de HTTPS en soluciones de Bitnami, están documentadas las siguientes guías, disponibles para todas las aplicaciones que incluyan un servidor HTTPS como Apache o NGINX:

- Creación de certificado SSL para el servidor Web Apache[2] y NGINX[3]: Todos los pasos para crear un certificado válido firmado por una autoridad de certificación miscelánea, y para el servidor Web. Se incluyen los pasos para crear un certificado autofirmado con carácter temporal, y se enlaza a una guía para configurar certificados con Let's Encrypt.
- Creación automatizada de un certificado de Let's Encrypt[4]: Describe cómo crear un certificado de Let's Encrypt mediante la herramienta automatizada de generación de certificados, y configurar el servidor Web para usarlo.

[2] Documentación para crear un certificado de HTTPS para el servidor Web Apache: https://docs.bitnami.com/aws/apps/wordpress/administration/create-ssl-certificate-apache/

[3] Documentación para crear un certificado de HTTPS para el servidor Web NGINX: https://docs.bitnami.com/aws/apps/wordpress-pro/administration/create-ssl-certificate-nginx/

[4] Documentación para generar y configurar un certificado de Let's Encrypt usando Lego: https://docs.bitnami.com/aws/apps/wordpress/administration/generate-configure-certificate-letsencrypt/

- Forzar redirección a HTTPS con el servidor Web Apache[5] y NGINX[6]: Lista los pasos necesarios para configurar una redirección de HTTP a HTTPS en el servidor Web.
- Solucionar problemas con certificados y claves SSL[7]: En caso de error de certificados iniciando el servidor Web, esta página describe las distintas causas y como arreglarlo.
- Activar HTTPS con el servidor Web Apache[8] y NGINX[9]: Describe como es la configuración de HTTPS de soluciones de Bitnami, y como instalar certificados ya creados. Esta guía es específica para soluciones de infraestructura como Bitnami LAMP Stack.
- Configurar renovación de un certificado de Let's Encrypt[10]: Describe como configurar trabajos programados para la renovación automatizada de certificados.

Además, se han creado una serie de tutoriales genéricas que aplican a todas las soluciones de Bitnami con un servidor HTTPS como Apache o NGINX:

- Generar e instalar un certificado SSL de Let's Encrypt para una aplicación con Bitnami[11]: Muestra como crear un certificado de Let's Encrypt y asociarlo al servidor Web mediante dos formas; primero con la herramienta automatizada de generación de certificados, y luego la alternativa manual.
- Solucionar problemas con SSL[12]: Describe una gran variedad de problemas distintos que pueden causar que un certificado no se asocie correctamente con el servidor Web.

3.2 Análisis de casos de soporte

El equipo de soporte de Bitnami realiza anualmente un análisis de casos de soporte para identificar cambios de tendencias en el uso de sus productos y problemas comunes a todas las soluciones. Esta información permite estudiar cambios de tendencia, encontrar puntos débiles y mejorar las soluciones de cara a un futuro análisis.

Se realiza para un sub-periodo del año y se centra en todos los casos sobre el producto Bitnami WordPress Stack, el más popular y que además es similar a muchos otros productos de Bitnami.

Por ejemplo, el análisis de los casos de soporte del año 2017 reveló que los usuarios tenían problemas a la hora de configurar HTTPS en productos de Bitnami, y deseaban poder de desplegar aplicaciones con un servidor Web distinto a Apache. Con ello, se mejoró los tutoriales y se desarrolló el producto Bitnami WordPress Stack con el servidor Web NGINX y pre-configurado con HTTPS, e incluye una herramienta automatizada para la generación de certificados. Esta acabaría siendo incluida en todos los productos con el servidor web Apache o NGINX a los pocos meses.

El último análisis se basó en los casos creados en septiembre y octubre del año siguiente, 2018. Los resultados completos, incluyendo el desglose de todos los casos de soporte analizados, se detallan en el Apéndice A. En resumen, encontró que los siguientes temas dominaban en una parte mayoritaria de los casos analizados por encima del 5 % de casos:

- Configuración de certificados HTTPS creados con Let's Encrypt: 13.74 %: 29 casos.
- Configuración de WordPress: 9 %: 19 casos.

[5] Documentación para activar redirección forzada a HTTPS en el servidor Web Apache: https://docs.bitnami.com/aws/apps/wordpress/administration/force-https-apache/

[6] Documentación para activar redirección forzada a HTTPS en el servidor Web NGINX: https://docs.bitnami.com/aws/apps/wordpress-pro/administration/force-https-nginx/

[7] Documentación para solucionar problemas con certificados HTTPS: https://docs.bitnami.com/aws/apps/wordpress/administration/check-ssl-certificate/

[8] Documentación para activar HTTPS en el servidor Web Apache: https://docs.bitnami.com/bch/infrastructure/lamp/administration/enable-https-ssl-apache/

[9] Documentación para activar HTTPS en el servidor Web NGINX: https://docs.bitnami.com/aws/infrastructure/nginx/administration/enable-https-ssl-nginx/

[10] Ya no existe documentación para configurar la renovación de un certificado de Let's Encrypt, tras los cambios realizados a causa de este proyecto.

[11] Documentación para generar e instalar un certificado SSL de Let's Encrypt: https://docs.bitnami.com/aws/how-to/generate-install-lets-encrypt-ssl/

[12] Documentación para solucionar problemas con certificados SSL: https://docs.bitnami.com/aws/how-to/troubleshoot-ssl-issues/

- Extensiones (plug-ins) de WordPress: 8.53 %: 18 casos.
- Redirecciones: 8.06 %: 17 casos.
- Misceláneos: 8.06 %: 17 casos.
- Configuración de Apache: 7.58 %: 16 casos.
- Rendimiento: 5.21 %: 11 casos.

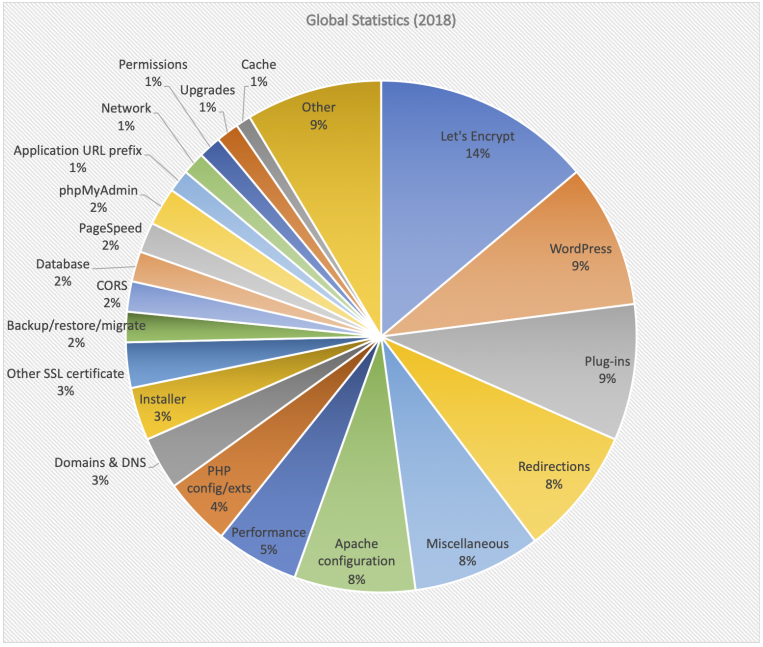


Figura 3.3 Porcentaje de casos de cada temática en el análisis de casos de soporte del año 2018.

Se observa que la configuración de HTTPS, muy relacionado a la configuración de certificados HTTPS (más del 20 %), las redirecciones a HTTPS y configuración de DNS, es aún un problema bastante común de los usuarios.

Todos estos resultados son la base de este proyecto, que busca reducir estas cifras, mejorar la experiencia de los usuarios y que así se pueda emplear menor tiempo realizando tareas de soporte.

Problemas identificados tras análisis de casos de soporte

Se ha observado una elevada cantidad de casos analizados sobre Let's Encrypt, de los cuales se encuentran los siguientes problemas relacionados con la documentación:

- Los errores de obtenidos al crear un certificado de Let's Encrypt son confusos y no fáciles de comprender para el usuario medio. Esto se puede ver en casos como 58929.
- La configuración a HTTPS causa muchos problemas a usuarios, por bucles de redirección, contenido mezclado (páginas HTTPS que cargan recursos específicos en HTTP), o que simplemente no funciona. Ejemplos de casos: 58076, 58261, 58502.
- Soluciones multi-nodo no incluyen toda la documentación necesaria para configurar HTTPS, y parte de ella es incorrecta. Casos relacionados: 58869 y 59377.
- En muchos de los casos se puede observar que los usuarios no son capaces de encontrar documentación específica de algunas partes de la configuración de HTTPS, como por ejemplo de redirecciones. Esto se puede observar en casos como 58117.
- Hay usuarios que no siguen la guía correctamente, y, por lo tanto, se encuentran problemas como ficheros inexistentes, mal creados o enlazados, etc. Ejemplos: 58261.
- Problemas al intentar configurar un certificado en una instancia incorrectamente configurada. Ejemplos: La configuración DNS del dominio no está asociada a la instancia; puertos necesarios para ejecutar Let's Encrypt están siendo ocupados por un servicio ajeno. Esto se observa en casos como 58839 o 59003.

Problemas identificados tras análisis de casos de soporte

El análisis realizado de los casos de soporte ha revelado graves deficiencias en la herramienta existente, y que afecta gravemente a la usabilidad por parte de los usuarios. Se listan a continuación:

- No se realiza ningún tipo de verificación sobre el estado de la instalación de Bitnami y permisos de ficheros, la conectividad a Internet, configuración de puertos, validación de los dominios introducidos (como por ejemplo que existan, o que su configuración DNS sea adecuada y apunten a la instancia correcta) o validación del correo electrónico introducido.
- La renovación de certificados, basado en tareas programadas, no está bien implementada, puesto que está configurada para usar el tipo de reto `TLS-ALPN-01`, que requiere parar y reiniciar el servidor Web. Estas tareas no son ideales como tareas programadas, y los tipos de retos alternativos `HTTP-01` o `DNS-01` requieren configuración avanzada.
- Debido a la ausencia de validaciones y no revocar el certificado existente si el dominio principal es el mismo, es fácil llegar a los límites de Let's Encrypt en caso de múltiples ejecuciones seguidas de la herramienta. Por ejemplo, el límite de validaciones fallidas es de 5 a la hora, y el de certificados duplicados es de 5 a la semana.
- Los posibles errores no enlazan a documentación específica de Bitnami Docs, que pueden ser útiles para la comprobación.
- Solo es válido para Bitnami Stacks de un solo nodo, es incompatible con soluciones multi-nodo como Bitnami WordPress Multi-Tier.
- Solo configura los certificados en el servidor Web, pero no otras tareas como las redirecciones a HTTPS o el cambio del nombre del servidor para ser compatible con los certificados configurados.
- No se configura la aplicación para funcionar sobre los nuevos dominios configurados.
- La ubicación de la instalación de Bitnami está codificado en el fichero. Usuarios que necesiten descargar la herramienta posteriormente necesitan modificar varias líneas de este fichero manualmente si el directorio es distinto de `/opt/bitnami`.
- No se guarda un fichero de registros sobre las acciones realizadas, los resultados obtenidos y los errores encontradas.

3.3 Propuestas

3.3.1 Creación de herramienta avanzada de configuración de HTTPS

Debido a la cantidad de cambios importantes a realizar sobre la herramienta original, se propone escribir una herramienta nueva desde cero y que permita configurar todos los aspectos de HTTPS en soluciones de Bitnami mencionados anteriormente. Por lo tanto, contará con las siguientes funcionalidades adicionales a la solución anterior:

- Detección de nuevas versiones de la herramienta y actualización automática. De esta forma, los usuarios no tendrán que preocuparse de buscar la última versión disponible.
- Configuración de redirecciones, tanto para forzar HTTPS como entre dominios no-www a www y viceversa.
- Realizar las comprobaciones necesarias de los campos de entrada proporcionados por los usuarios, como dominios y correo electrónico, incluyendo cualquier comprobación necesaria como conectividad a Internet o de validación de dominios y DNS.
- Configurar correctamente la renovación automatizada de dominios.
- Detección de certificados de Let's Encrypt para evitar llegar a límites.
- Enlazar errores específicos a documentación relacionada para solventar los problemas.
- Funcionamiento universal en todas las plataformas de Bitnami.

- Configuración de la aplicación instalada para funcionar con los nuevos dominios provistos por el usuario.
- Generar un fichero de registro que incluya las acciones realizadas y cualquier error obtenido, así como información relevante para depurarlos.

3.3.2 Documentación

Se proponen los siguientes cambios:

- Crear una guía para solucionar errores de Let's Encrypt.
- Relacionar la documentación de configuración de SSL con la documentación para configurar redirecciones, tanto para forzar HTTPS como entre dominios no-www a www y viceversa.
- Adaptar la documentación a los cambios tras el reemplazo de la herramienta para configurar HTTPS.

4 Diseño, desarrollo e implementación

En este capítulo se procederá a describir todo el proceso de desarrollo de una nueva herramienta para la configuración de HTTPS en soluciones de Bitnami, comenzando por un análisis de requisitos. A continuación, se presentará una propuesta técnica y una prueba de concepto. Posteriormente, se describirá el proceso de desarrollo e implementación de la solución, culminando con una herramienta completamente funcional que se describirá detalladamente.

4.1 Análisis de requisitos

4.1.1 Actores

AC-01	Usuario
Descripción	Representa al usuario que desea configurar HTTPS en su instalación de Bitnami.

Tabla 4.1 AC-01.

AC-02	Servidor de verificación de Let's Encrypt
Descripción	Representa el sistema de verificación de la autoridad de certificación, utilizado para verificar la autenticidad de los dominios del usuario.

Tabla 4.2 AC-02.

4.1.2 Casos de uso

CU-01	Creación de un nuevo certificado HTTPS
Descripción	Creación de un nuevo certificado Let's Encrypt para los dominios especificados.
Pre-condición	Se verifica que el dominio principal (primer dominio especificado) no tiene asociado un certificado de Let's Encrypt en la instalación de Bitnami. Los dominios tienen formato correcto y la resolución DNS devuelve los valores esperados.
Post-condición	Se configura el servidor Web para asociar el certificado HTTPS con este. Se instala la configuración necesaria para la renovación automatizada de este certificado. El acceso al servidor Web muestra el nuevo certificado.

Actores	• AC-01: Usuario • AC-02: Servidor de verificación de Let's Encrypt
Dependencias	• CU-05: Configuración de la instalación de Bitnami con un nuevo nombre de dominio

Tabla 4.3 CU-01.

CU-02	Renovación de certificado HTTPS
Descripción	Renovación del certificado HTTPS existente de Let's Encrypt si se encuentra dentro de la época de renovación (normalmente 30 días anteriores a su caducidad).
Pre-condición	El dominio principal (primer dominio especificado) tiene asociado un certificado de Let's Encrypt en la instalación de Bitnami, y la lista de dominios asociados al certificado son idénticos a los provistos por el usuario. Los dominios tienen formato correcto y la resolución DNS devuelve los valores esperados.
Post-condición	El acceso al servidor Web muestra el certificado renovado.
Actores	• AC-01: Usuario • AC-02: Servidor de verificación de Let's Encrypt
Dependencias	Sin dependencias.

Tabla 4.4 CU-02.

CU-03	Recreación de un certificado HTTPS de Let's Encrypt con distintos dominios
Descripción	Se revoca el certificado HTTPS existente de Let's Encrypt, y se crea uno nuevo, tal y como se describe en CU-01: Creación de un nuevo certificado HTTPS.
Pre-condición	El dominio principal (primer dominio especificado) tiene asociado un certificado de Let's Encrypt en la instalación de Bitnami, pero la lista de dominios asociados al certificado no coinciden con los provistos por el usuario. En este punto se genera una notificación al usuario, y pese a ello decide seguir. Los dominios tienen formato correcto y la resolución DNS devuelve los valores esperados.
Post-condición	El acceso al servidor Web muestra el nuevo certificado.
Actores	• AC-01: Usuario • AC-02: Servidor de verificación de Let's Encrypt
Dependencias	• CU-01: Creación de un nuevo certificado HTTPS de Let's Encrypt

Tabla 4.5 CU-03.

CU-04	Configuración de redirecciones
Descripción	Activación o desactivación de tres tipos de redirecciones: • De HTTP a HTTPS • De dominios no-www a www (por ejemplo, de `example.com` a `www.example.com`) • De dominios www a no-www (por ejemplo, de `www.example.com` a `example.com`)
Pre-condición	La configuración del servidor Web no ha sido alterada por el usuario. El usuario ha provisto para cada dominio su par no-www como www (p. ej. `example.com` y `www.example.com`) para configurar redirecciones. Los dominios tienen formato correcto y la resolución DNS devuelve los valores esperados.
Post-condición	El acceso a los dominios provoca una redirección de HTTP a HTTPS, y/o entre dominios tipo no-www y www.
Actores	• AC-01: Usuario
Dependencias	• CU-05: Configuración de la instalación de Bitnami con un nuevo nombre de dominio

Tabla 4.6 CU-04.

CU-05	Configuración de la instalación de Bitnami con un nuevo nombre de dominio
Descripción	Se aplicará la configuración necesaria tanto al servidor Web como a la aplicación para funcionar con un nuevo nombre de dominio principal.
Pre-condición	Los dominios tienen formato correcto y la resolución DNS devuelve los valores esperados.
Post-condición	El servidor Web y las aplicaciones de la instalación Bitnami tienen configurados el dominio principal.
Actores	• AC-01: Usuario
Dependencias	• CU-01: Creación de un nuevo certificado HTTPS de Let's Encrypt

Tabla 4.7 CU-05.

4.1.3 Requisitos generales

RG-01	Auto-actualización
Prioridad	Máxima

Descripción	Se realizará una comprobación de la última versión disponinble de la herramienta. Si hubiera disponible una nueva versión, se informará al usuario y, en el caso de estar de acuerdo con la actualización, se descargarán los ficheros necesarios y se saldrá del programa con información sobre cómo volver a ejecutarlo. En caso contrario, la ejecución continuará su curso.

Tabla 4.8 RG-01.

RG-02	Configuración de certificados en instalación de Bitnami
Prioridad	Máxima
Descripción	Una ejecución correcta instalará y configurará nuevos certificados HTTPS gratuitos con Let's Encrypt en la instalación de Bitnami correspondiente, siempre que no existiese uno para los dominios especificados.

Tabla 4.9 RG-02.

RG-03	Configuración de renovación automatizada de certificados
Prioridad	Máxima
Descripción	Una ejecución correcta programará con servicios del sistema una renovación automatizada de certificados.

Tabla 4.10 RG-03.

RG-04	Configuración de certificados SSL existentes
Prioridad	Alta
Descripción	Deberá soportar la configuración de certificados existentes.

Tabla 4.11 RG-04.

RG-05	Configuración de redirecciones
Prioridad	Alta
Descripción	Será posible activar redirecciones de HTTP a HTTPS, de dominios www a no-www y de dominios no-www a www.

Tabla 4.12 RG-05.

RG-06	Plataformas soportadas
Prioridad	Alta
Descripción	Será compatible con versiones actualmente soportadas de las distribuciones GNU/Linux Debian, Ubuntu, CentOS, Red Hat Enterprise Linux, Oracle Linux y Amazon Linux.

Tabla 4.13 RG-06.

4.1.4 Requisitos funcionales

Se deben tener en cuenta una serie de requisitos sobre el funcionamiento de la herramienta.

Requisitos de conducta

RC-01	Ejecución exitosa
Prioridad	Media
Descripción	Una ejecución exitosa del programa deberá indicar un mensaje de éxito, junto con información sobre los pasos realizados.

Tabla 4.14 RC-01.

RC-02	Ejecución errónea reversible
Prioridad	Alta
Descripción	En caso de error reversible, se deberá indicar detalles en un mensaje específico y con la posibilidad de obtener información más detallada. Además, se revertirá la instalación a la situación original.

Tabla 4.15 RC-02.

RC-03	Ejecución errónea irreversible
Prioridad	Alta
Descripción	En caso de error no reversible, se deberá indicarlo junto con un mensaje específico del error, además de la posibilidad de obtener información más detallada del error. Debido a no ser reversible, se revertirá la instalación al estado original pero indicando pasos adicionales a realizar por el usuario.

Tabla 4.16 RC-03.

RC-04	Fichero de registros
Prioridad	Alta
Descripción	La ejecución del programa deberá crear un fichero de registro que permita obtener información detallada de la ejecución del programa.

Tabla 4.17 RC-04.

RC-05	Instalación de herramientas de Let’s Encrypt
Prioridad	Alta
Descripción	En caso de que la instalación existente no incluyese las herramientas necesarias de Let’s Encrypt, se copiarán durante el proceso de configuración del servidor.

Tabla 4.18 RC-05.

Requisitos de información

RI-01	No recopilación de datos

Prioridad	Alta
Descripción	La solución no deberá compartir ningún dato con Bitnami sobre el uso, sobre los usuarios ni sobre el sistema en el que se esté ejecutando.
Comentarios	Para el cumplimiento del Reglamento General de Protección de Datos.

Tabla 4.19 RI-01.

4.1.5 Requisitos no funcionales

Requisitos de fiabilidad

RF-01	No corromper instalaciones existentes
Prioridad	Alta
Descripción	Bajo ningún concepto la ejecución de la herramienta debe provocar un fallo en el funcionamiento de la instalación existente de un usuario que no estuviese ya presente. Para ello, realizará las comprobaciones oportunas y verificará la configuración del servidor Web.

Tabla 4.20 RF-01.

RF-02	Límites externos
Prioridad	Alta
Descripción	Se realizarán todas las acciones posibles para evitar alcanzar límites externos, de forma que sea posible una ejecución sucesiva.
Comentarios	Por ejemplo, revocar certificados existentes asociados al dominio principal para evitar alcanzar el límite de certificados activos por dominio, validación de dominios y correos electrónicos para evitar alcanzar límites relacionados al dominio o usuario, etc.

Tabla 4.21 RF-02.

RF-03	Creación de copias de seguridad
Prioridad	Alta
Descripción	Previa modificación de un fichero, se realizará una copia de seguridad de este.

Tabla 4.22 RF-03.

Requisitos de usabilidad

RU-01	Modo texto
Prioridad	Alta
Descripción	La herramienta funcionará en entornos sin interfaz gráfica.

Tabla 4.23 RU-01.

RU-02	Múltiples ejecuciones
Prioridad	Alta
Descripción	Será posible ejecutar la herramienta múltiples veces sobre una misma instalación, sin que ello cause pérdida de funcionalidades.

Tabla 4.24 RU-02.

RU-03	Parámetros de usuario
Prioridad	Alta
Descripción	Los parámetros de obligada configuración por parte de los usuarios serán imprescindibles para el cumplimiento de las funcionalidades principales, en caso contrario no serán visibles.
Comentarios	Se busca que la solución sea lo más simple posible.

Tabla 4.25 RU-03.

RU-04	Errores
Prioridad	Alta
Descripción	Los errores técnicos incluirán un enlace a documentación que contenga-más información.

Tabla 4.26 RU-04.

RU-05	Dependencia de programas externos
Prioridad	Media
Descripción	No habrá ninguna dependencia con programas del sistema operativo e incluidas dentro de instalaciones de Bitnami, salvo los programas específicos para gestión de servicios.

Tabla 4.27 RU-05.

RU-06	Detección del directorio de instalación de Bitnami
Prioridad	Alta
Descripción	Se realizará una búsqueda rápida de directorios de instalación de Bitnami conocidos. Las ubicaciones identificadas se comprobarán una a una, asegurando compatibilidad con la herramienta (por ejemplo, se ignorará instalaciones sin servidor Web). En el caso de no haber identificado ninguna instalación, se le preguntará al usuario realizando la misma serie de comprobaciones.
Dependencias	Sin dependencias.

Tabla 4.28 RU-06.

RU-07	Detección de redirecciones ya configuradas
Prioridad	Alta

Descripción	Se comprobará en la configuración del servidor Web cualquier configuración de redirección existente. En caso de existir redirecciones añadidas por el usuario y no por ejecuciones anteriores de la herramienta, y para evitar problemas, se deshabilitará cualquier posibilidad de configuración de redirecciones en la ejecución actual.

Tabla 4.29 RU-07.

RU-08	Comprobación del funcionamiento de renovación automatizada de certificados
Prioridad	Alta
Descripción	Se realizará las comprobaciones del funcionamiento de renovación de certificados tras la configuración del servidor Web y la instalación del certificado. En caso de fallo se notificará al usuario con enlaces a la documentación.
Comentarios	Esto permitirá a usuarios identificar problemas con la configuración del servidor Web para su aplicación.

Tabla 4.30 RU-08.

Requisitos de eficiencia

No se especifican requisitos de eficiencia.

Requisitos de mantenibilidad

RE-01	Curva de aprendizaje
Prioridad	Baja
Descripción	El desarrollo de la herramienta debe, en la medida de lo posible, contar con una curva de aprendizaje rápida de forma que otros miembros del equipo puedan trabajar cómodamente en esta.
Comentarios	Esto aplica principalmente a la mantenibilidad del código y en la plataforma escogida.

Tabla 4.31 RE-01.

RE-02	Adición de nuevos servidores web soportados
Prioridad	Media
Descripción	Añadir un nuevo servidor web soportado debe ser una tarea sencilla y requerir de mínimas modificaciones en código existente.

Tabla 4.32 RE-02.

Requisitos de portabilidad

RP-01	Sistema de construcción y empaquetado compatible
Prioridad	Baja
Descripción	La construcción de la herramienta se podrá realizar en sistemas operativos diferentes a GNU/Linux.

Tabla 4.33 RP-01.

Requisitos de seguridad

RS-01	Ejecutables libre de vulnerabilidades
Prioridad	Alta
Descripción	La plataforma que se use para la construcción y el empaquetado de la herramienta debe ser segura y producir ejecutables libres de vulnerabilidades.

Tabla 4.34 RS-01.

4.2 Propuesta técnica

La herramienta a desarrollar se llamará Bitnami HTTPS Configuration Tool, o herramienta de configuración de HTTPS de Bitnami. Su abreviación será `bncert`, en referencia a su utilidad para configurar certificados en Stacks de Bitnami. Se encuentra así en sintonía con otras herramientas de Bitnami como Bitnami Configuration Tool (de abreviación `bnconfig`) o Bitnami Support Tool (`bnsupport`).

A continuación se procederá a describir con detalle sus componentes y la plataforma en la que se basará la implementación.

4.2.1 Herramienta de gestión de certificados de Let's Encrypt

Para los procesos de creación, renovación y revocación de certificados se ha decidido seguir utilizando la herramienta LEGO, que se invoca mediante línea de comandos con `lego` [55]. Es una herramienta desarrollada en Go y está activamente mantenida. Su uso en comparación con otras soluciones (como la oficial) resulta en distintas ventajas:

- Consta de un único binario por plataforma sin dependencias externas. Gracias a ello no es necesario preocuparse por programas y bibliotecas instaladas en el sistema operativo, simplemente funciona. La solución oficial `certbot`, por ejemplo, tiene dependencias con Git y Python.
- Soporta los métodos de creación, renovación y revocación de certificados HTTPS de Let's Encrypt, con multitud de opciones.
- Su licencia es de tipo MIT, lo cual es beneficioso para la inclusión del binario en la herramienta resultante, sin necesidad de descargarlo separadamente.
- Es la solución previamente escogida para su uso con la herramienta anterior `generate-certificates.sh` que ya se encuentra documentada. De esta forma hay un ahorro de trabajo necesario en documentación y en la familiarización con esta por parte de los usuarios existentes.

4.2.2 Plataforma de desarrollo

La plataforma escogida para el desarrollo de la herramienta es VMware InstallBuilder, desarrollada en Bitnami, por varios motivos:

- El equipo que se encargará del mantenimiento de la herramienta a desarrollar está familiarizado con VMware InstallBuilder. De esta forma, se reduce de manera drástica la fase de aprendizaje para nuevos contribuidores a la herramienta.
- Permite ahorrar tiempo de desarrollo en cuanto a funcionalidades de gestión de errores, entradas, interfaces gráficas, etc., las cuales ya están implementadas.
- Comparte el código fuente para todas las plataformas soportadas y modos de funcionamiento -con interfaz gráfica o en modo texto, y en modo interactivo o no interactivo-.

- Para la depuración de errores complejos, dispone de un potente depurador.
- Soporta de manera nativa un mecanismo de auto-actualización de instaladores/herramientas.
- Por último, y más importante, no pone obstáculos al cumplimiento con todos los requisitos identificados anteriormente.

Nótese que al usar VMware InstallBuilder para el desarrollo de esta herramienta se recurre a una serie de inconvenientes:

- Esta está pensada para desarrollar instaladores y no herramientas genéricas.
- La programación en VMware InstallBuilder se realiza mediante ficheros XML, no se dispone del poder de un lenguaje de programación completo.
- Inserta cabeceras de más de 10 MB en los binarios resultantes. Esto tiene un impacto directo sobre los usuarios que se encuentran descargan una nueva solución que incluya la herramienta.

No obstante, para el desarrollo de la herramienta en particular no se consideran lo suficientemente importantes como para tener que buscar otra solución.

4.3 Prueba de concepto

Antes de proceder al desarrollo de la herramienta se realizará una prueba de concepto sobre la solución a implementar, permitiendo incorporar fácilmente ideas y sugerencias y, en la medida de lo posible, evitar malentendidos durante la fase de diseño e implementación.

4.3.1 Metodología

A pesar de que el modo texto se considere más importante y prioritario que el diseño de la interfaz gráfica y modos no interactivos, la prueba de concepto se realizará basado en una interfaz gráfica debido a que es mucho más fácil de comprender a primera vista.

Código 4.1 Código fuente necesario para generar un parámetro de ejemplo con VMware InstallBuilder.

```
<project>
   <fullName>test</fullName>
   <shortName>test</shortName>
   <version>0.1</version>
   <parameterList>
      <parameterGroup name="p1" description="Título">
         <parameterList>
            <stringParameter name="p11" description="Parámetro de texto"/
                >
            <booleanParameter name="p12" description="Parámetro booleano"
                />
         </parameterList>
      </parameterGroup>
   </parameterList>
</project>
```

Figura 4.1 Parámetro de ejemplo p1 representado en modo texto con VMware InstallBuilder.

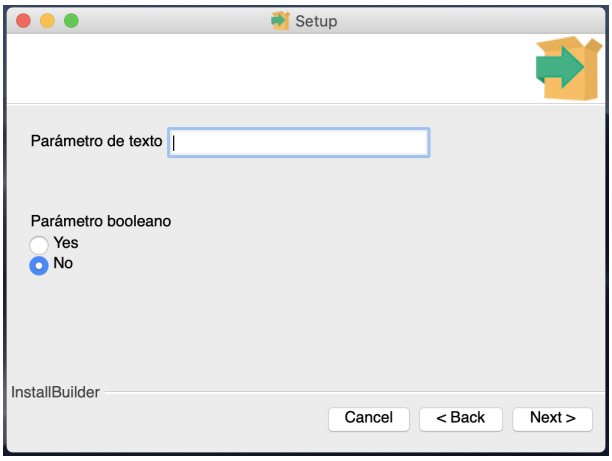


Figura 4.2 Parámetro de ejemplo p1 representado en modo interfaz gráfica con VMware InstallBuilder.

Del mismo modo, en VMware InstallBuilder, tanto el modo texto como el de interfaz gráfica son equivalentes y permiten compartir código fuente, como se muestra con el código fuente del Código 4.1 con el parámetro representado en modo texto (Figura 4.1) como en modo intefaz gráfica (Figura 4.2).

Para la realización de la prueba de concepto de la interfaz, se usará MockFlow, ya que es gratuita para un proyecto, muy sencilla de usar y ágil. Con esta se representarán las distintas páginas que contendrá, acompañadas de la correspondiente descripción para cada una de ellas.

Resultado

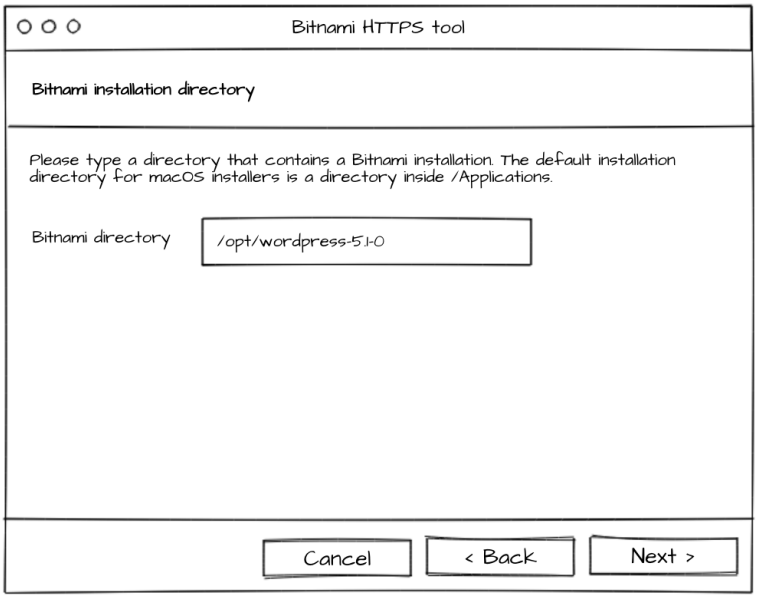


Figura 4.3 Prueba concepto 1. Directorio de instalación.

En la primera página (Figura 4.3), el usuario deberá especificar el directorio de la instalación de Bitnami para la que quiera configurar HTTPS. Tras ello, se validará, y en caso de ser correcta permitirá ir a la siguiente página.

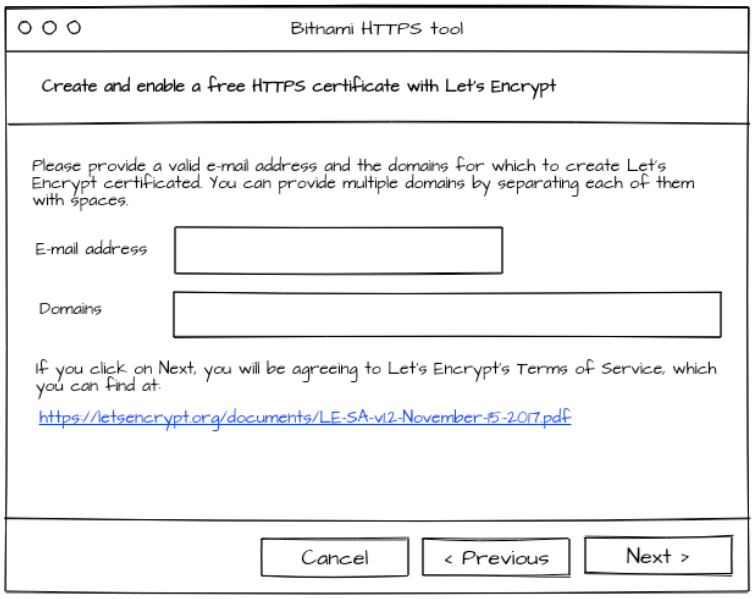


Figura 4.4 Prueba de concepto 1. Configuración de Let's Encrypt.

La segunda página (Figura 4.4) contiene la configuración de Let's Encrypt. Para crear un certificado con esta herramienta es necesario especificar una serie de dominios y un correo electrónico asociado, para notificar la renovación. Además, Let's Encrypt requiere que se acepten términos de servicio para generar certificados.

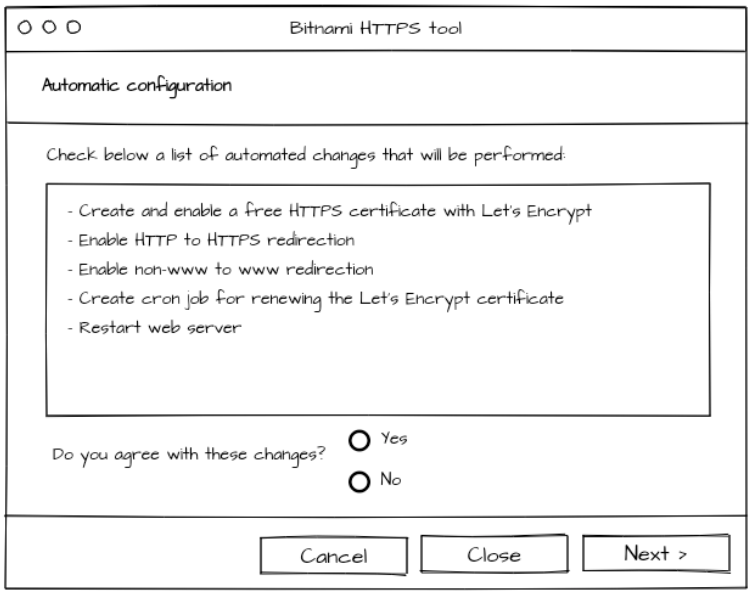


Figura 4.5 Prueba de concepto 1. Descripción de cambios a realizar.

A continuación, la siguiente página lista al usuario la serie de cambios que se realizarán (Figura 4.5).

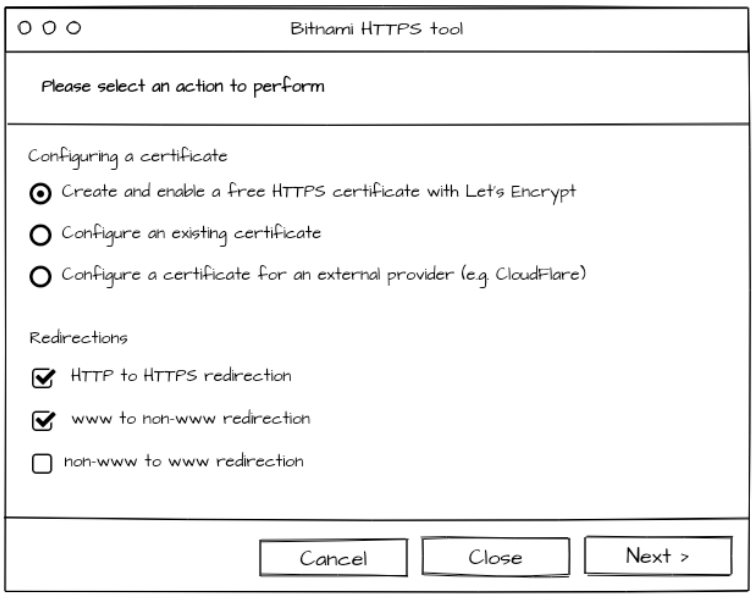


Figura 4.6 Prueba de concepto 1. Ajuste de opciones (en caso de seleccionar Ño').

En caso de no estar de acuerdo con alguno de los cambios propuestos, el usuario podrá cambiar el modo de ejecución como activar o desactivar algunas de las opciones (Figura 4.6). Esta página lleva al usuario de vuelta a la página anterior, de listado de cambios propuestos a realizar.

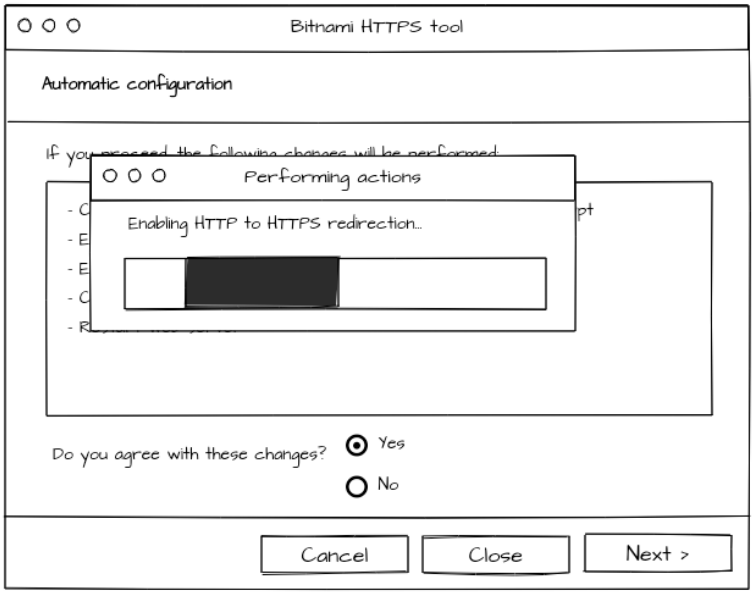


Figura 4.7 Prueba de concepto 1. Realización de cambios.

Una vez que el usuario haya aceptado la propuesta de cambios a realizar, se comenzará a aplicarlos y se abrirá un diálogo de progreso describiendo el estado de la configuración (como se observa en la Figura 4.7).

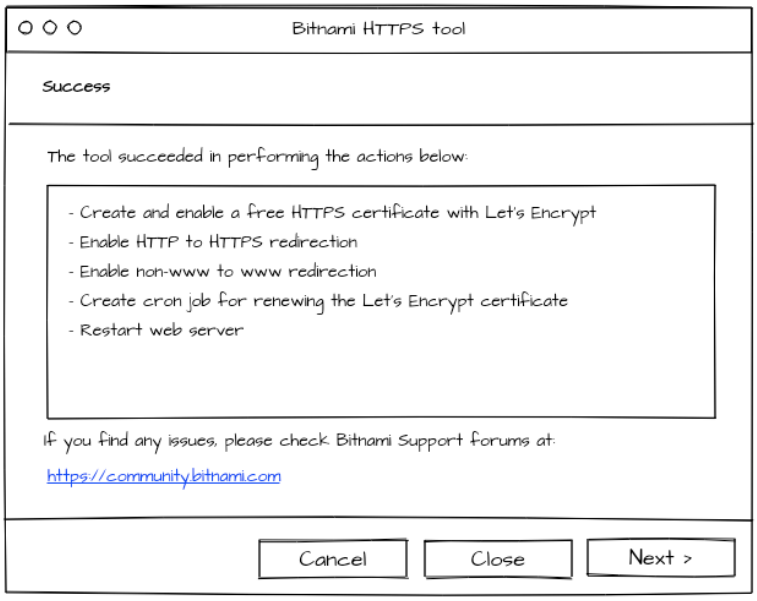


Figura 4.8 Prueba de concepto 1. Página final con cambios realizados.

Finalmente, dependiendo de si ha ido todo bien o no, se mostrará la página de éxito o error respectivamente, en el que se listarán los cambios realizados (Figura 4.8).

Mejoras propuestas

Tras la presentación interna, se proponen una serie de mejoras:

- Intentar detectar el directorio de instalación de manera automática, permitiendo así ocultar la página de la Figura 4.3 en caso de éxito.
- Separar la introducción de dominios de la configuración de Let's Encrypt (correo electrónico y EULA) en la Figura 4.4, ya que en caso de la existencia de un certificado y en modos de ejecución futuros puede no ser necesaria la configuración de Let's Encrypt, permitiendo así una separación de contexto.
- Siempre que sea posible, utilizar dominios y direcciones web especificadas por el usuario antes que `example.com`. Por ejemplo, en la página de la Figura 4.5, si el usuario hubiese especificado el dominio `midominio.es`, los ejemplos usarían este dominio para mayor facilidad de comprensión.
- Numerar la serie de cambios a realizar en la página de la Figura 4.5, en el orden por el que se realizan las acciones.
- Dividir la actual página de selección de acciones a realizar (Figura 4.6). El camino a realizar se mostraría al principio, aunque podría no ser una característica de las primeras versiones. Las redirecciones tendrían su propia página.
- En la página final (Figura 4.8), evitar especificar los cambios realizados, y en su lugar información que pueda ayudar a los usuarios a identificar el origen de problemas. Por ejemplo, mostrar el fichero de registros de mensajes usado por la herramienta.

A partir de este punto contamos con suficiente información para comenzar el proceso de diseño de la herramienta, a partir del análisis de requisitos identificados anteriormente, la propuesta técnica, la prueba de concepto y las mejoras propuestas.

4.4 Diseño

La nueva herramienta de Bitnami para configurar HTTPS, a diferencia de anteriores soluciones, será interactiva por defecto. De este modo, contendrá una serie de páginas navegables hacia adelante, cada uno con un propósito distinto, y que contendrán objetos (parámetros) con los que el usuario podrá interactuar u obtener información acerca del estado del proceso de la configuración.

El diseño de esta se realizará comenzando desde la visión global (percibido por el usuario) hacia los bloques más fundamentales, inspirado en la prueba de concepto realizada anteriormente.

Para los diagramas de flujo utilizados en este capítulo, incluyendo los dos anteriores, se empleará el formato descrito en la Tabla 4.35.

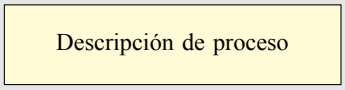
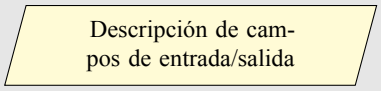
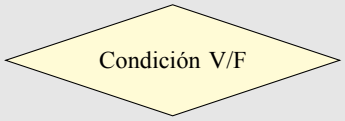
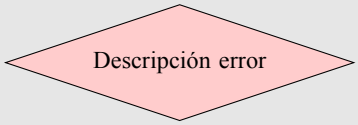
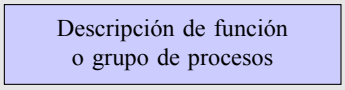
Figura	Descripción
	Inicio de proceso.
	Descripción de un proceso
	Campos de entrada o salida de texto.
	Bifurcación tras la evaluación de una condición lógica verdadero/falso.
	Diálogo de error. En un proceso de validación, hace cambiar el foco de nuevo a los campos de la página para su corrección. Con otros tipos de procesos, la ejecución de la herramienta termina con código de error.
	Descripción de una función o grupo de procesos.
	Línea de flujo, la flecha indica la siguiente instrucción.
	Fin del proceso actual.

Tabla 4.35 Leyenda de diagramas de flujo.

4.4.1 Visión global

En la Figura 4.9 se representa la visión más global de esta herramienta, donde se pueden observar las distintas páginas que la compondrán.

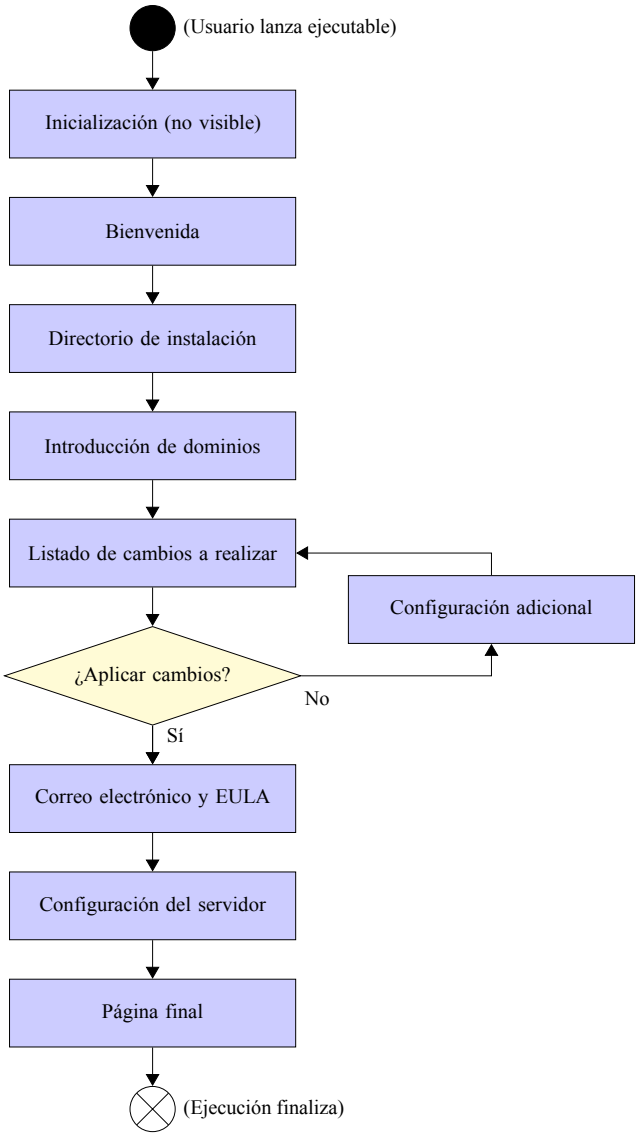


Figura 4.9 Orden de páginas definitivo.

Cada una de las pantallas, a excepción del proceso de inicialización que no es visual, tienen un proceso de visualización como se representa en la Figura 4.10. Se dejan sin describir los parámetros ni grupos de procesos, que se irán detallando en los sucesivos apartados.

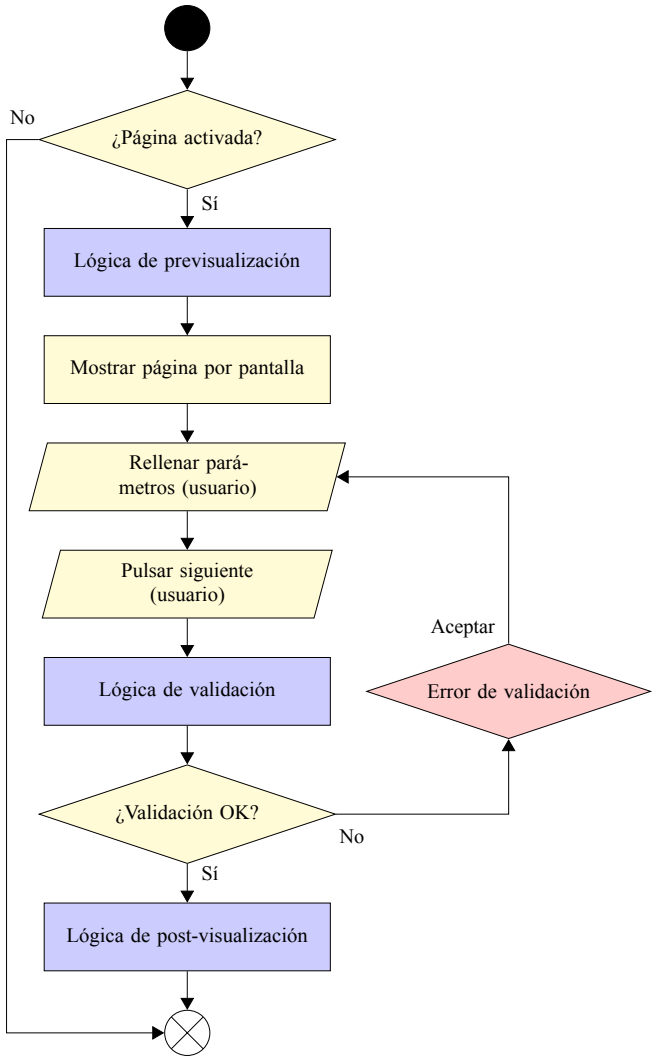


Figura 4.10 Procesos involucrados en una página de VMware InstallBuilder.

4.4.2 Lógica de inicialización

La lógica de inicialización realmente no es una página de VMware InstallBuilder, más bien lógica del proyecto que se ejecuta antes de la visualización de cualquiera de las pantallas. Debido a que en este proyecto tiene una fuerte influencia en la ejecución de la herramienta, se ha considerado interesante describirla.

Primero se procede a detectar el valor del directorio de instalación. Si no es encontrada, termina el proceso. Sin embargo, en caso de detectarse, se realiza la detección de una nueva versión de la herramienta y la actualización automática. Esto se debe a que la herramienta se encuentra incluida dentro de la instalación de Bitnami, y en caso de no conocerse este valor, no tiene sentido actualizar.

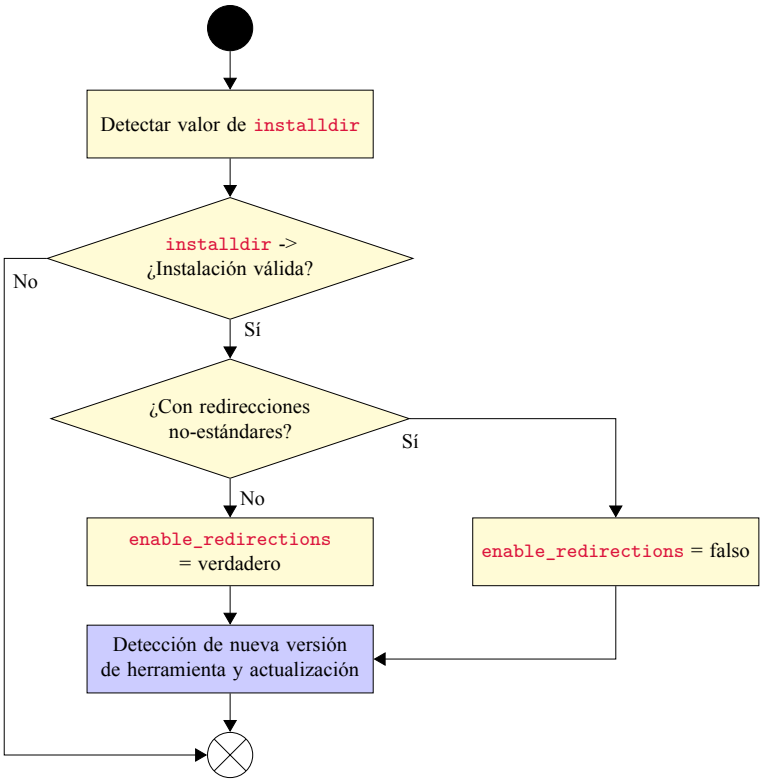


Figura 4.11 Lógica de inicialización.

4.4.3 Página de bienvenida

La página de bienvenida es de obligatoria inclusión con VMware InstallBuilder, y no es personalizable con la excepción de los textos. No contiene, por lo tanto, parámetros ni lógica involucrada.

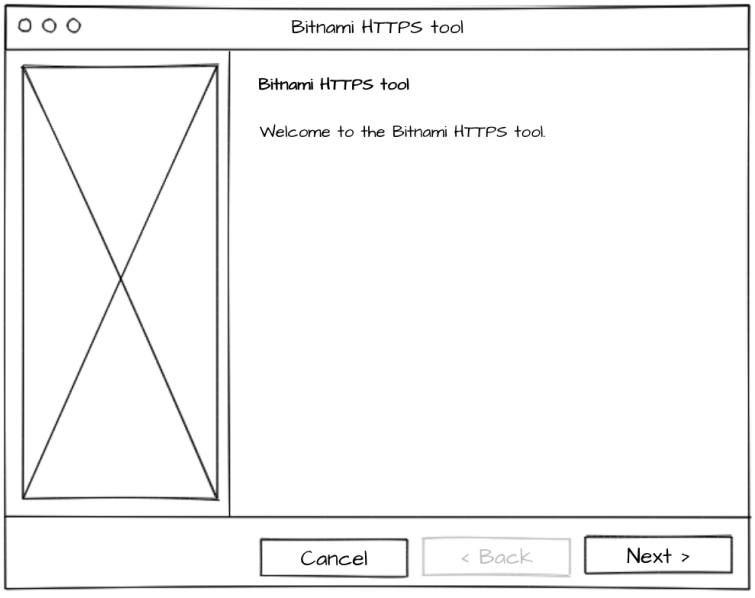


Figura 4.12 Maqueta definitiva de la página de bienvenida.

Configuración

Título	Configuración adicional
Identificador	`welcome_label`
Descripción	Primera página del ejecutable, que incluye una breve introducción a la herramienta.
¿Mostrar?	Siempre.
Página anterior	No aplica (es la primera página).
Página siguiente	`domains_group`

Tabla 4.36 Configuración de la página de bienvenida.

4.4.4 Página de especificación del directorio de instalación

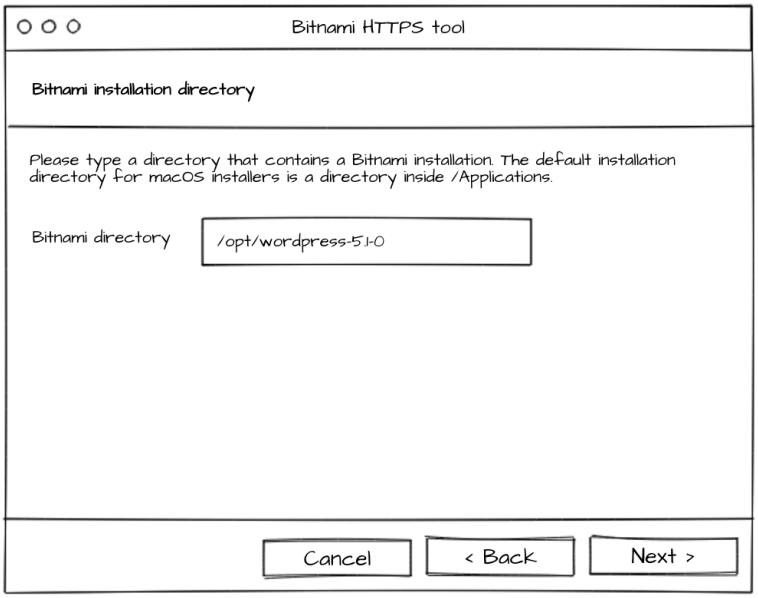


Figura 4.13 Maqueta definitiva de la página de especificación del directorio de instalación.

Configuración

Título	Configuración adicional
Identificador	`installdir`
Descripción	Página dedicada a la especificación del directorio en el que se localiza la instalación, por parte del usuario, donde desea configurar HTTPS.
¿Mostrar?	Si el directorio de instalación detectado en la inicialización no contiene una instalación válida.
Página anterior	`welcome_label`
Página siguiente	`domains_group`

Tabla 4.37 Configuración de la página de introducción de dominios.

Parámetros

Identificador	Tipo	Visible	Descripción
`installdir`	Directorio	Sí	Ruta absoluta al directorio de la instalación de Bitnami donde se desea configurar HTTPS.

Tabla 4.38 Parámetros de la página final.

Lógica de previsualización

Esta página no dispone de lógica de previsualización.

Lógica de validación

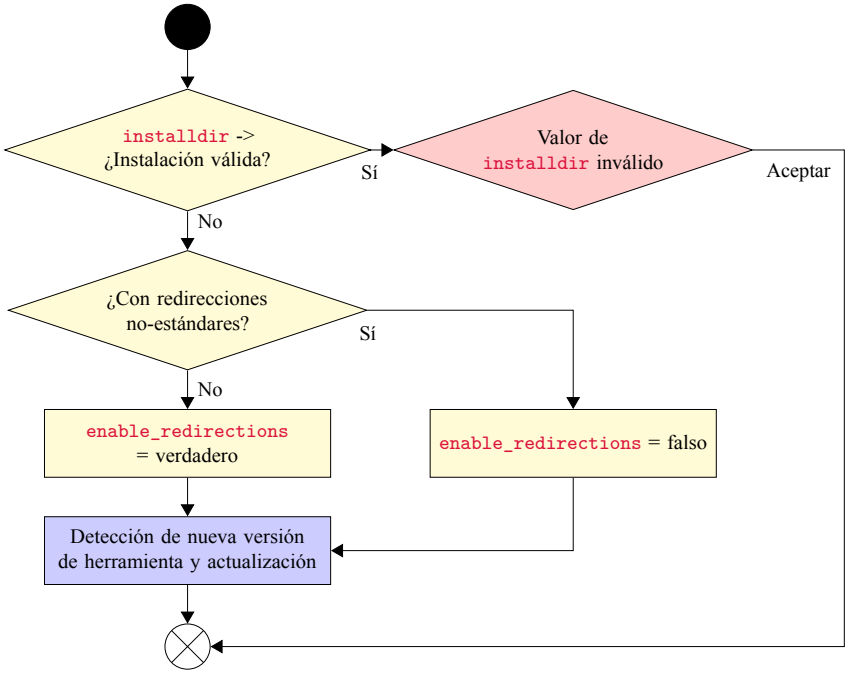


Figura 4.14 Lógica de inicialización de página de especificación del directorio de instalación.

Lógica de post-visualización

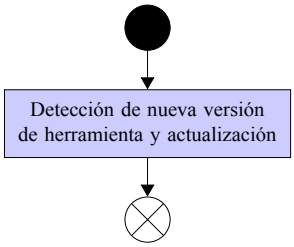


Figura 4.15 Lógica de inicialización de página de especificación del directorio de instalación.

4.4.5 Página de introducción de dominios

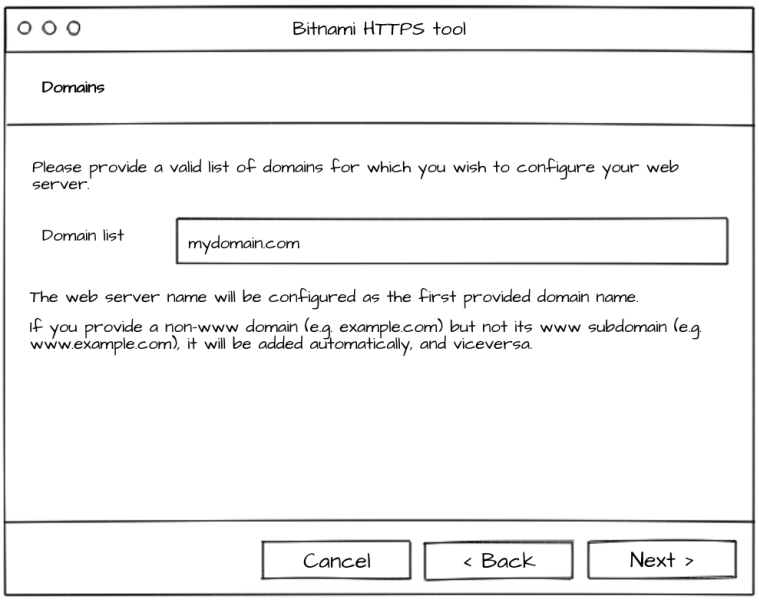


Figura 4.16 Maqueta definitiva de la página de introducción de dominios.

Configuración

Título	Configuración adicional
Identificador	`domains_group`
Descripción	Página dedicada a la introducción de dominios por parte del usuario, para los que se creará un certificado HTTPS de Let's Encrypt.
¿Mostrar?	Siempre.
Página anterior	`installdir`
Página siguiente	`changes_to_perform_group`

Tabla 4.39 Configuración de la página de introducción de dominios.

Parámetros

Identificador	Tipo	Visible	Descripción
`domains`	Texto	Sí	Listado de dominios para los que crear un certificado HTTPS de Let's Encrypt.
`missing_domains`	Texto	No	Listado de dominios www/no-www no especificados en `domains`.
`server_name`	Texto	No	Nombre que se utilizará como dominio por defecto del servidor Web.

Tabla 4.40 Parámetros de la página final.

Lógica de previsualización

Esta página no dispone de lógica de previsualización.

Lógica de validación

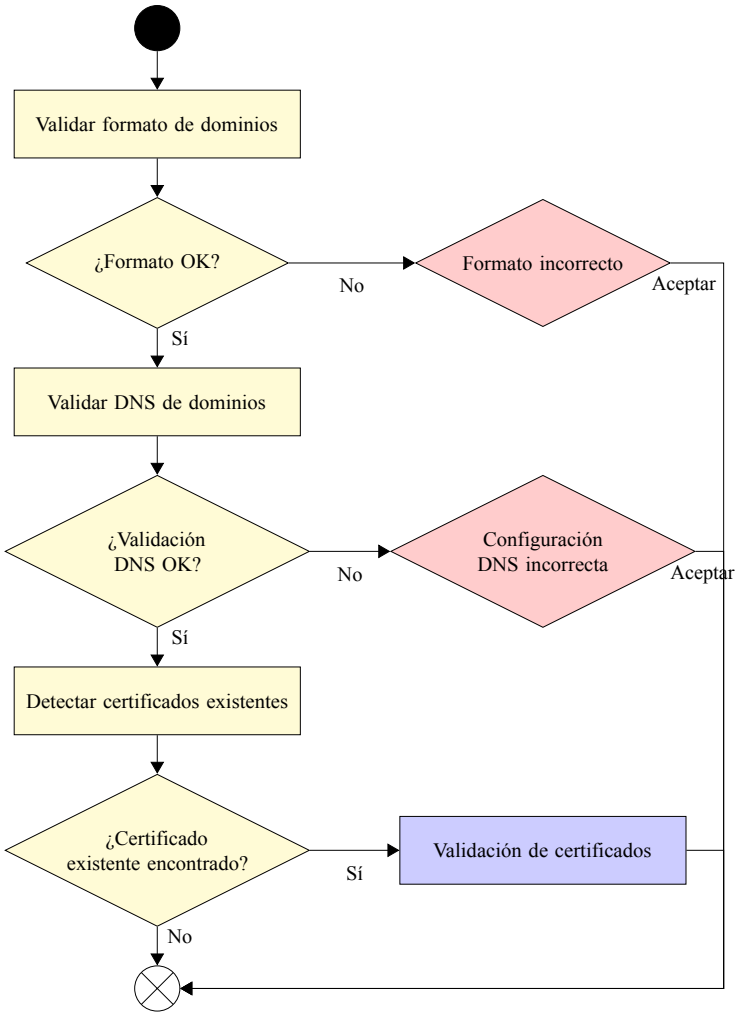


Figura 4.17 Lógica de validación de página de introducción de dominios.

Lógica de post-visualización

Durante la post-visualización se realizará la detección de dominios www o no-www que no hayan sido especificados, cuyo valor se incluirá en el parámetro `missing_domains`, y se definirá como `server_name` el primero de ellos. Ejemplos:

`domains`	`missing_domains` (calculado)	`server_name` (calculado)
`example.com www.example.com`		`example.com`
`example.com`	`www.example.com`	`example.com`
`www.example.com`	`example.com`	`www.example.com`
`abc.xyz www.abc.xyz sub.abc.xyz`	`www.sub.abc.xyz`	`abc.xyz`

Tabla 4.41 Ejemplos de valores de parámetros resultantes según dominios configurados por el usuario.

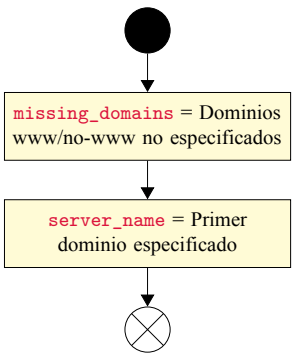


Figura 4.18 Lógica de post-visualización de página de introducción de dominios.

4.4.6 Página de cambios a realizar

Configuración

Título	Configuración adicional
Identificador	`changes_to_perform_group`
Descripción	Descripción de los cambios que se aplicarán a la instalación de Bitnami.
¿Mostrar?	Siempre.
Página anterior	`domains_group`
Página siguiente	`letsencrypt_configuration_group` (si `agree_to_changes` es verdadero) `additional_configuration` (si `agree_to_changes` es falso)

Tabla 4.42 Configuración de la página de cambios a realizar.

Parámetros

Identificador	Tipo	Visible	Descripción
`changes_to_perform_text`	Información	Sí	Listado de cambios propuestos a realizar.
`agree_to_changes`	Booleano	Sí	Si el usuario está de acuerdo con los cambios a realizar. Valor por defecto: `yes`.

Tabla 4.43 Parámetros de la página de cambios a realizar.

Lógica de previsualización

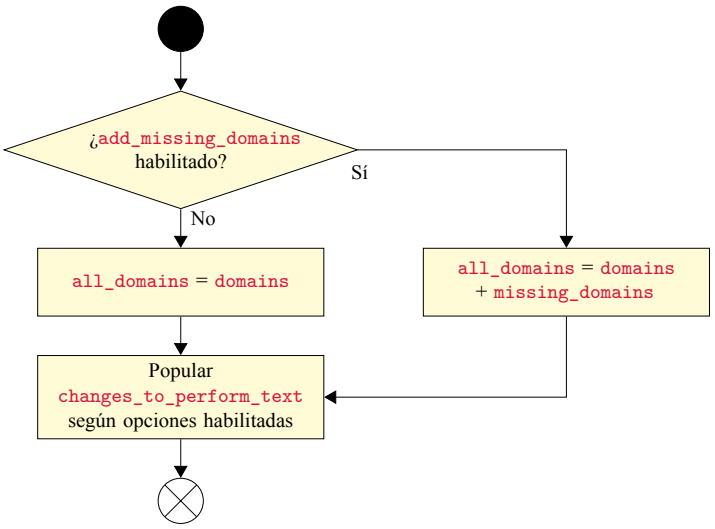


Figura 4.20 Lógica de post-visualización de página de configuración adicional.

Lógica de validación

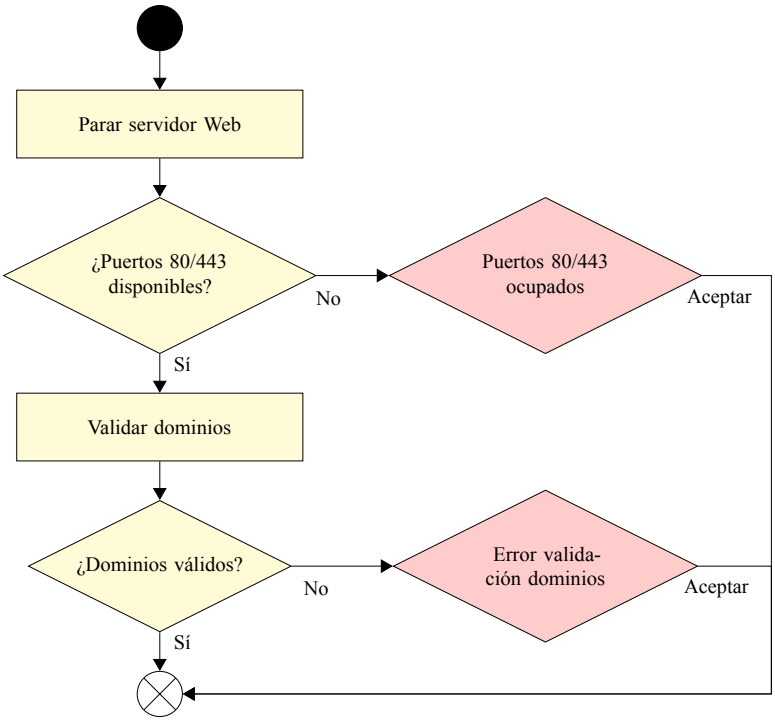


Figura 4.21 Lógica de validación de página de cambios a realizar.

Lógica de post-visualización

En la lógica de post-visualización se jugará con el valor de la variable interna de VMware InstallBuilder `next_page`, que determina cuál es el identificador de la siguiente página. Así, en caso de estar de acuerdo con los cambios se le llevará al usuario a la página de dominios, pero si no, a la página de configuración adicional para modificar las opciones de configuración.

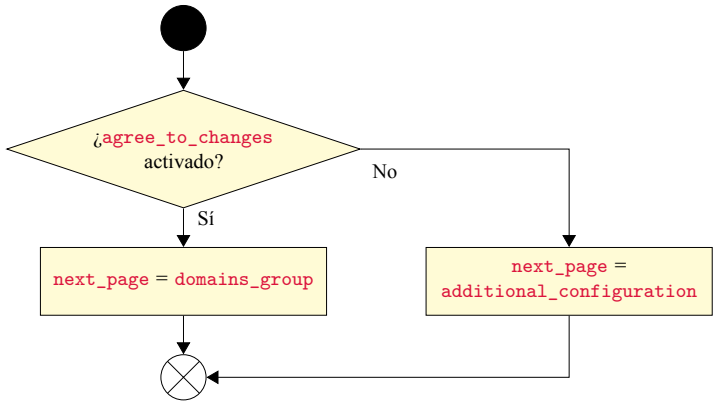


Figura 4.22 Lógica de post-visualización de página de cambios a realizar.

4.4.7 Página de configuración adicional

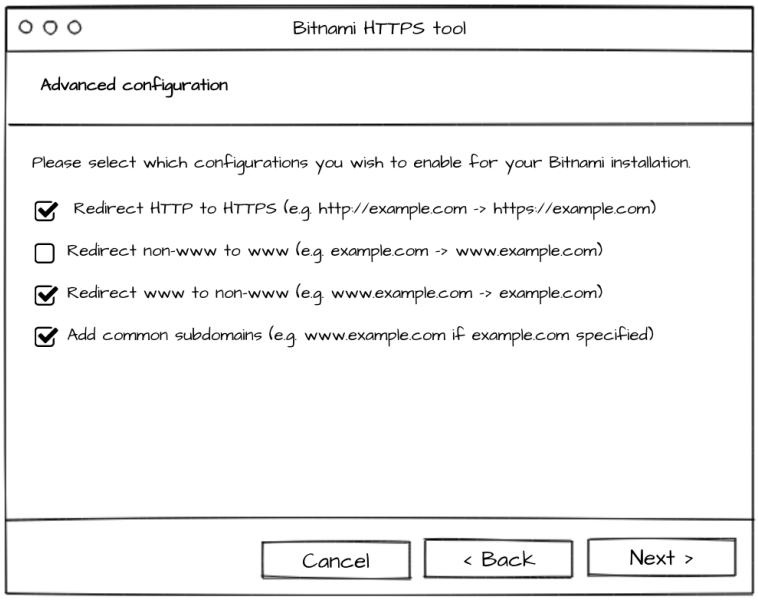


Figura 4.23 Maqueta definitiva de la página de configuración adicional.

Configuración

Título	Configuración adicional
Identificador	`additional_configuration`
Descripción	Listado de cambios a realizar sobre la instalación de Bitnami.
¿Mostrar?	Si `agree_to_changes` es falso.
Página anterior	`changes_to_perform`
Página siguiente	`changes_to_perform`

Tabla 4.44 Configuración de la página de introducción de dominios.

Parámetros

Identificador	Tipo	Visible	Descripción
`enable_https_redirection`	Texto	Sí	Listado de dominios para los que crear un certificado HTTPS de Let's Encrypt.
`enable_nonwww_to_www_redirection`	Texto	No	Listado de dominios www/no-www no especificados en `domains`.
`enable_www_to_nonwww_redirection`	Texto	No	Listado de dominios www/no-www no especificados en `domains`.
`add_missing_domains`	Booleano	Sí	Añadir automáticamente dominios detectados faltantes a la lista especificada por el usuario. Valor por defecto: `yes`

Tabla 4.45 Parámetros de la página de introducción de dominios.

Lógica de previsualización

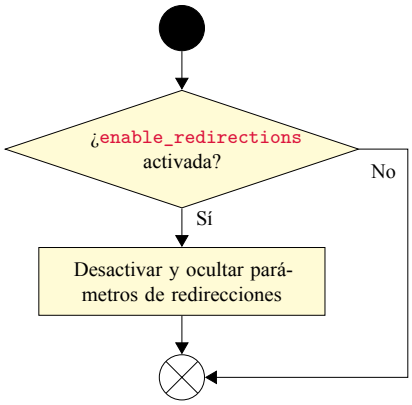


Figura 4.24 Lógica de previsualización de página de configuración adicional.

Lógica de validación

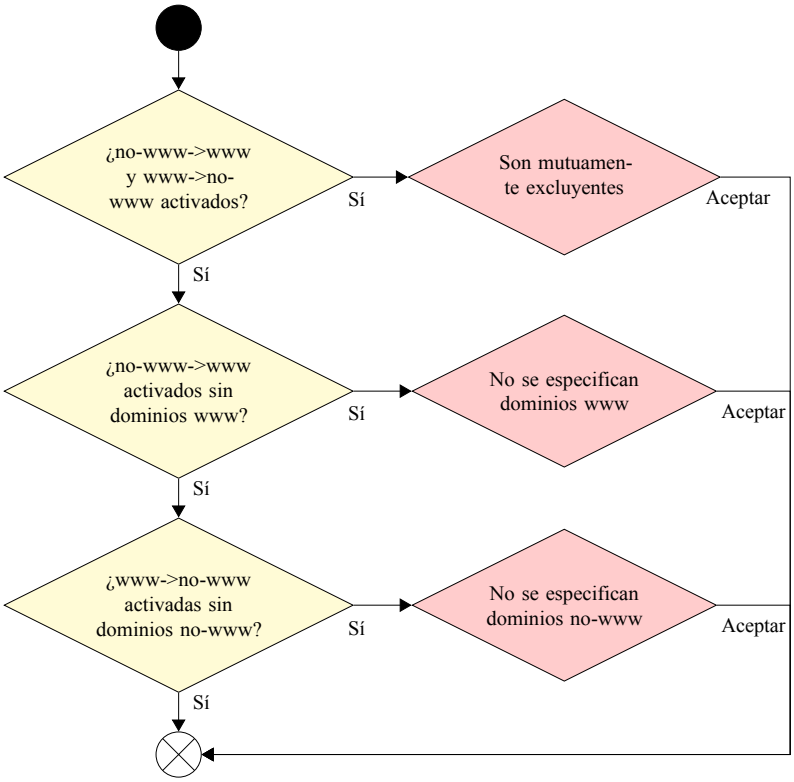


Figura 4.25 Lógica de validación de página de configuración adicional.

Lógica de post-visualización

Esta página no dispone de lógica de post-visualización.

4.4.8 Página de EULA e introducción de correo electrónico

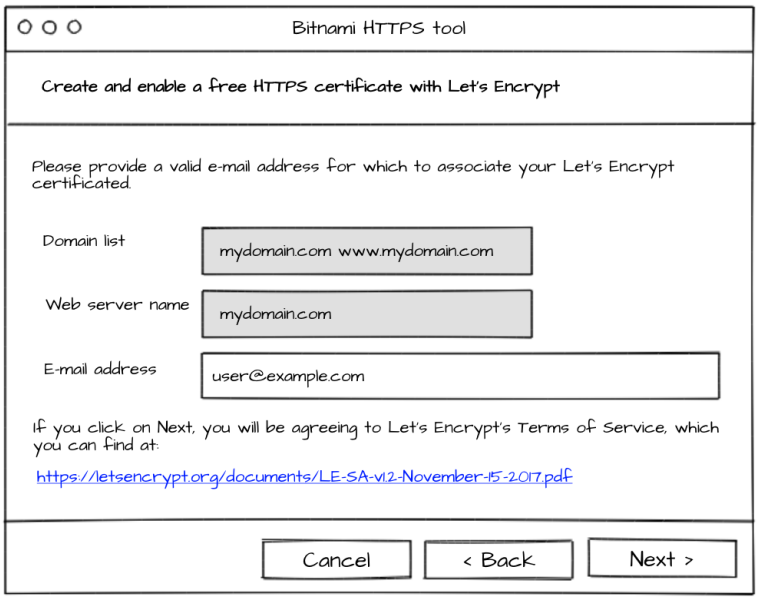


Figura 4.26 Maqueta definitiva de la página de EULA e introducción de correo electrónico.

Configuración

Título	Crear un certificado gratuito con Let's Encrypt
Identificador	`letsencrypt_configuration_group`
Descripción	Configuración necesaria para crear un certificado gratuito con Let's Encrypt.
¿Mostrar?	Siempre.
Página anterior	`changes_to_perform`
Página siguiente	`perform_actions`

Tabla 4.46 Configuración de la página de EULA e introducción de correo electrónico.

Parámetros

Identificador	Tipo	Visible	Descripción
`domains_label`	Etiqueta	Sí	Listado de dominios especificados anteriormente. No es configurable.
`server_name_label`	Etiqueta	Sí	Nombre del servidor especificado anteriormente. No es configurable.
`email`	Booleano	Sí	Correo electrónico del usuario que desea crear/renovar un certificado. Usado para notificación periódica de renovaciones.
`letsencrypt_agree_to_tos`	Booleano	Sí	Consultar al usuario si está de acuerdo con el EULA de Let's Encrypt.

Tabla 4.47 Parámetros de la página de EULA e introducción de correo electrónico.

Lógica de previsualización

Esta página no dispone de lógica de previsualización.

Lógica de validación

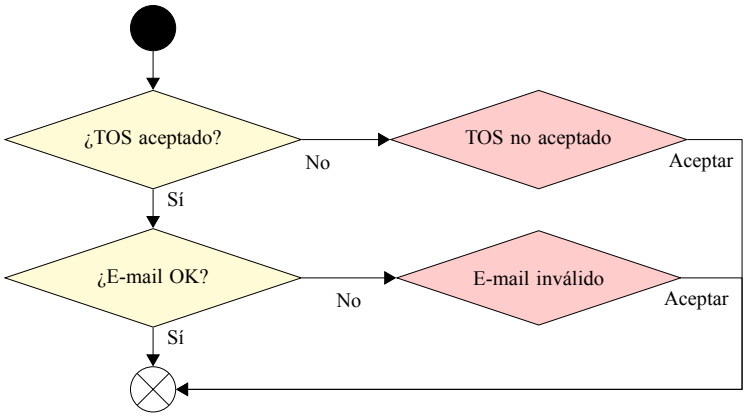


Figura 4.27 Lógica de validación de página de EULA e introducción de correo electrónico.

Lógica de post-visualización

Esta página no dispone de lógica de post-visualización.

4.4.9 Página de configuración del servidor

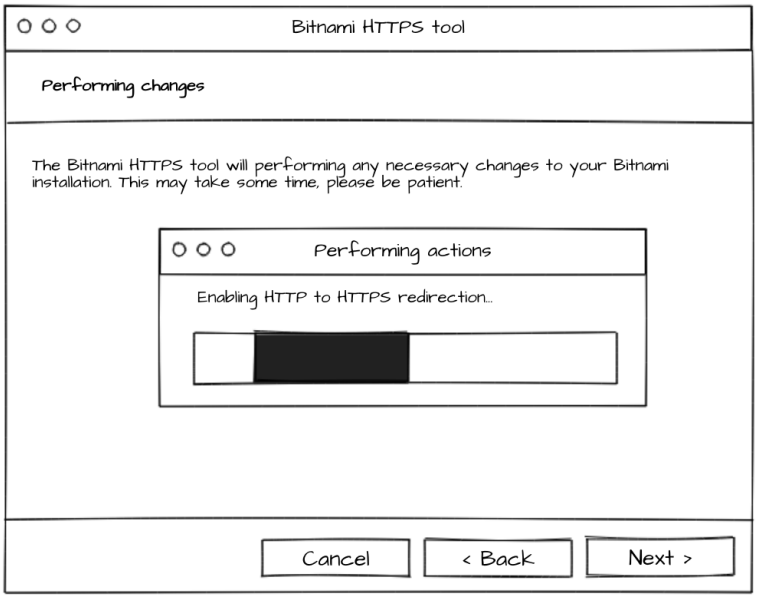


Figura 4.28 Maqueta definitiva de la página de configuración del servidor.

Configuración

Título	Realización de cambios sobre la instalación
Identificador	`perform_actions`
Descripción	Página dedicada a aplicar los cambios necesarias sobre la instalación listadas anteriormente. Al terminar se pasará a la siguiente página.
¿Mostrar?	Siempre.
Página anterior	`letsencrypt_configuration_group`
Página siguiente	`custom_final_page`

Tabla 4.48 Configuración de la página de configuración del servidor.

Parámetros

Identificador	Tipo	Visible	Descripción
`dry_run`	Booleano	No	Permite la ejecución de la herramienta sin modificar la instalación de Bitnami. Será usado extensamente con pruebas. Valor por defecto: `no`.

Tabla 4.49 Parámetros constantes.

Lógica de previsualización

Esta página no dispone de lógica de previsualización.

Lógica de validación

Esta página no dispone de lógica de previsualización.

Lógica de post-visualización

Durante la lógica de post-visualización se ejecutarán todas las acciones necesarias para la configuración de HTTPS deseada en el servidor. En caso de un error durante cualquiera de las acciones, se revertirá la configuración del servidor Web.

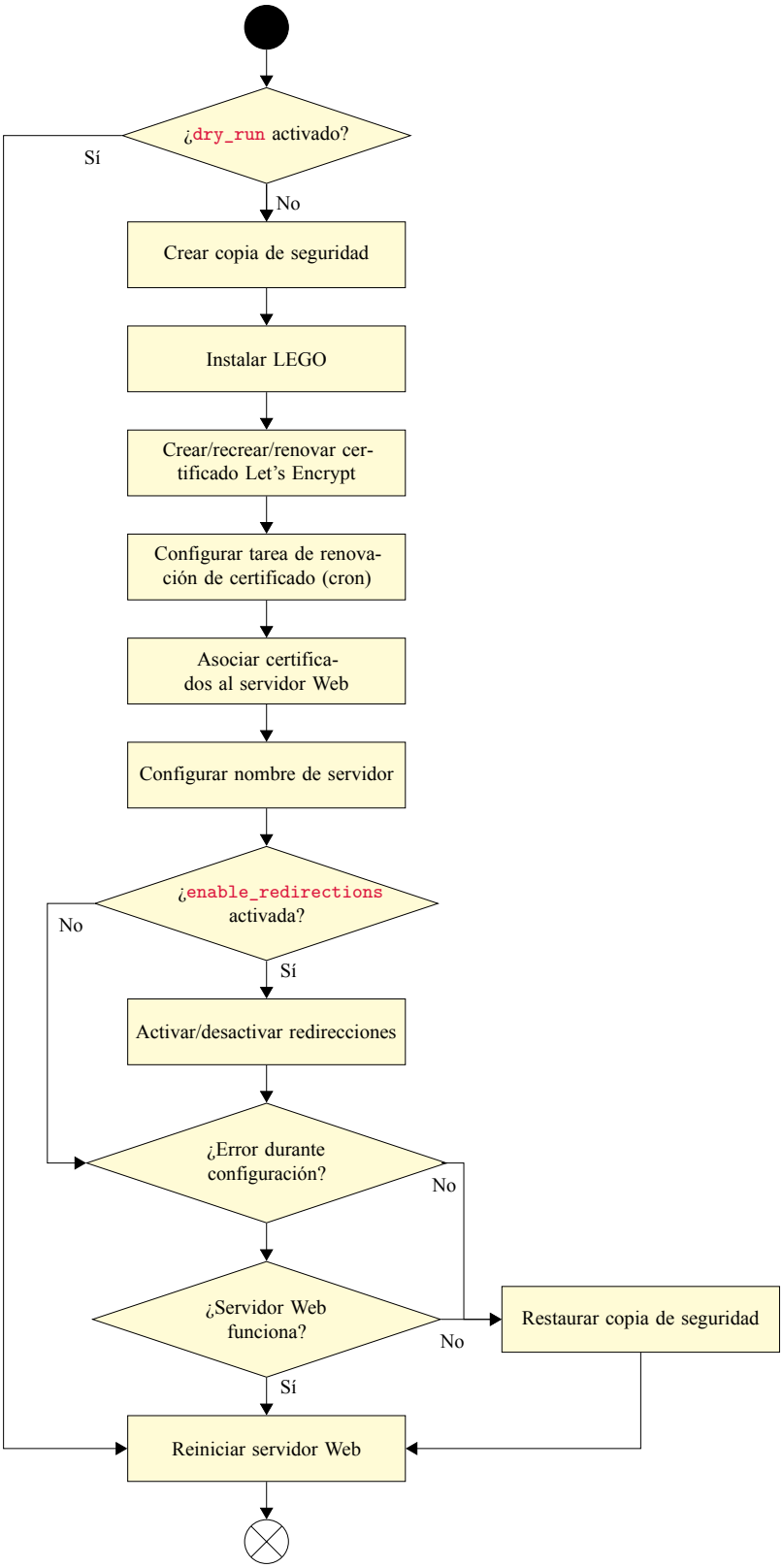


Figura 4.29 Lógica de post-visualización de página de configuración del servidor.

4.4.10 Página final

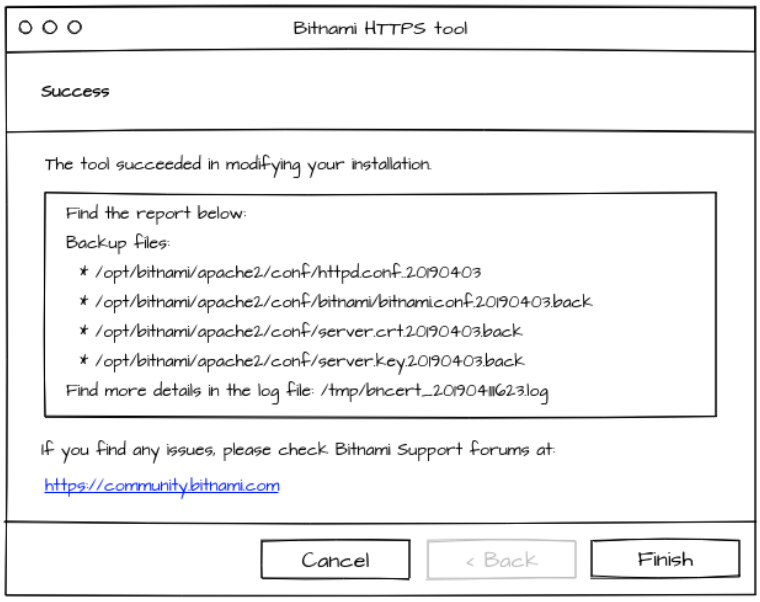


Figura 4.30 Maqueta definitiva de la página final.

Configuración

Título	Éxito (o Error en caso de problema)
Identificador	`custom_final_page`
Descripción	Página final de la herramienta (diferente a la provista por InstallBuilder, permitiendo así una mayor personalización).
¿Mostrar?	Siempre.
Página anterior	`perform_actions`
Página siguiente	No aplica (finalización de la ejecución).

Tabla 4.50 Configuración de la página final.

Parámetros

Identificador	Tipo	Visible	Descripción
`report_text`	Información	Sí	Reporte de los cambios realizados durante la ejecución de la herramienta. No es configurable.

Tabla 4.51 Parámetros de la página final.

Lógica de previsualización

Antes de mostrar la página final, se construirá el reporte de configuración aplicada con la información obtenida de los parámetros de estado.

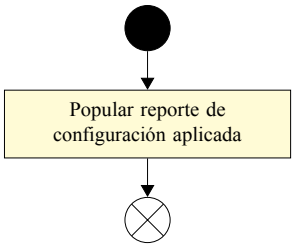


Figura 4.31 Lógica de post-visualización de página final.

Lógica de validación

Esta página no dispone de lógica de previsualización.

Lógica de post-visualización

Tras la post-visualización, se procesará la salida de la herramienta al ser la última página.

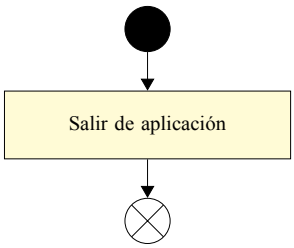


Figura 4.32 Lógica de post-visualización de página final.

4.5 Implementación

4.5.1 Limitaciones

Para agilizar el proceso de implementación, se limitará la primera versión de la nueva herramienta de configuración de HTTPS de Bitnami de la siguiente forma:

- Plataformas soportadas: Linux de 64 bits para las distribuciones Debian 7, Ubuntu 14.04, CentOS/Fedora/RHEL 5 y cualquier versión más moderna de estas distribuciones. Por el momento no se soportará las plataformas Windows o macOS.
- Servidores Web soportados: Apache 2.4. En el futuro cercano se añadirá soporte a NGINX.
- Funcionalidades: Se limitará los modos de configuración a la creación/renovación de certificados HTTPS de Let's Encrypt con LEGO, no así certificados generados de forma externa. El resto de funcionalidades (redirecciones, configuración del dominio principal, etc.) se implementarán en su totalidad.

4.5.2 Configuración del proyecto

Los campos más importantes y relevantes que se usarán para configurar el fichero de proyecto de VMware InstallBuilder se listan en la Tabla 4.52.

Campo	Valor	Notas
`fullName`	Bitnami HTTPS Configuration Tool	
`shortName`	`bncert`	
`vendor`	Bitnami	
`enableSslSupport`	`yes`	Necesario para poder realizar peticiones a sitios Web HTTPS con acciones nativas.

`logoImage`		Icono de la aplicación. Se representa
`leftImage`		Imágen personalizable mostrada a la izquierda de la página de bienvenida.
`height`	393	Configurado a una altura específica para el correcto funcionamiento de `leftImage`.
`disableSplashScreen`	Sí	

Tabla 4.52 Configuración del proyecto de VMware InstallBuilder.

4.5.3 Ficheros externos a empaquetar

Con este proyecto se empaquetará el fichero binario `lego` para Linux de 64-bits, y durante la ejecución de la herramienta se instalará en el directorio `letsencrypt` en la raíz del directorio de instalación de Bitnami. Esto permitirá a usuarios utilizar la herramienta sin tener LEGO instalado anteriormente, y evita así posibles problemas que si se descargase durante el proceso de configuración.

Este fichero se puede obtener desde GitHub[1] descomprimiendo el fichero `lego_VERSION_linux_-amd64.tar.gz` para la versión deseada, por ejemplo `v3.3.0`. Al ser un binario construido desde un proyecto de Go y enlazado de manera estática, no tiene ninguna dependencia con bibliotecas dinámicas de Linux y, por lo tanto, es compatible con todas las distribuciones buscadas.

La licencia empleada en el proyecto es de tipo MIT, muy simple y permisiva, y permite empaquetar el binario mientras se conserve las menciones a los derechos de autor y licencia (que se incluirán en el fichero de instalación en caso de no existir).

4.5.4 Página de bienvenida

La página de bienvenida es de obligatoria inclusión con InstallBuilder, y es poco personalizable, salvo los textos. Por ese motivo, no se describirá como las demás.

Para la configuración de los textos se puede crear un fichero de idiomas como el mostrado en el Código 4.2, para el caso de idioma inglés.

Código 4.2 Fichero de idiomas de ejemplo para la modificación del texto en la página de bienvenida de VMware InstallBuilder.

```
1 Installer.Welcome.Title=Bitnami HTTPS Configuration tool
2 Installer.Welcome.Text=Welcome to the Bitnami HTTPS Configuration tool.
```

Para el uso de este fichero en VMware InstallBuilder, hay que especificar el fichero en el directorio raíz donde se encuentran los ficheros del proyecto. A continuación, es necesario añadir la lógica del Código 4.3 dentro de la etiqueta `<project>` en el fichero principal del proyecto de BitRock InstallBuilder.

[1] Página con enlaces de descarga de la herramienta Lego: https://github.com/go-acme/lego/releases/

Código 4.3 Código necesario para el uso del fichero del Código 4.2 con VMware InstallBuilder.

```
1 <customLanguageFileList>
2     <language code="en" file="bncert-en.lng"/>
3 </customLanguageFileList>
```

También es posible personalizar una imagen en la página de bienvenida que se encuentra a la izquierda, especificando el código de la figura 4.4 dentro de la etiqueta `<project>` en el fichero principal del proyecto de VMware InstallBuilder. En este caso, la imagen debería localizarse en la ruta `images/left.png` desde la carpeta raíz del proyecto.

Código 4.4 Código necesario para el uso de una imagen personalizada en la página de bienvenida con VMware InstallBuilder.

```
1 <leftImage>images/left.png</leftImage>
```

La inclusión de todo esto en un proyecto generaría un instalador con la página de bienvenida mostrada en la Figura 4.33.

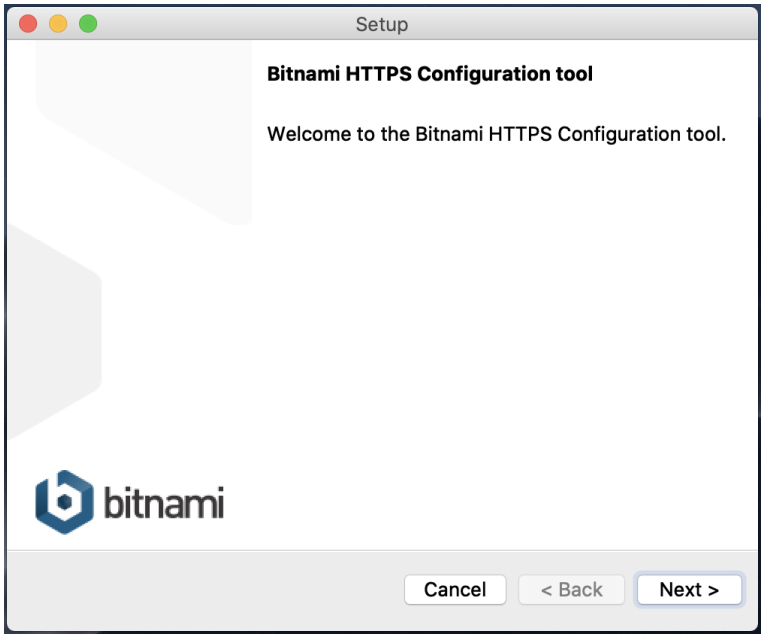


Figura 4.33 Ejemplo de página de bienvenida de VMware InstallBuilder personalizada.

4.5.5 Auto-actualización

Para la implementación del mecanismo de auto-actualización, se hará uso de la herramienta AutoUpdate incluida dentro de VMware InstallBuilder. Para su correcto funcionamiento es necesario que se cumplan una serie de puntos:

- Publicación del fichero de auto-actualización `update.xml`: Es necesario publicar un fichero XML en un enlace público, accesible desde Internet. Este contendrá el enlace a la última versión de la herramienta final para cada plataforma (figura 4.5), como por ejemplo Linux de 64 bits.
- Construcción del binario de auto-actualización: Se debe construir mediante AutoUpdate un binario, específico por cada versión de la herramienta y plataforma (figura 4.6). Para ello, es necesario crear un fichero de proyecto de auto-actualizador con `<autoUpdateProject>`. Esta herramienta permite consultar nuevas versiones de una herramienta y descargar el binario correspondiente en caso de haberlo.

- Creación de fichero `update.ini` (figura 4.7): Contiene configuración del binario de auto-actualización, como por ejemplo enlace al fichero `update.xml` a comprobar, el identificador de la versión actual y el destino de ficheros descargados.
- Inclusión del binario de auto-actualización y fichero `update.ini` dentro de la herramienta final: Una vez construido, se debe incluir dentro de la herramienta. En este caso se hace mediante un componente específico para tal cometido (figura 4.8), que supone que ambos ficheros se encuentran dentro del directorio raíz del proyecto.
- En el proyecto de la herramienta principal, extraer y ejecutar el binario de auto-actualización de la manera deseada. En la implementación, esto se hace en la función `runUpdater` que se ejecuta tras tener un directorio de instalación válido (en la función `bncertPostInstalldirActions`).

Código 4.5 Fichero de auto-actualización bncert-update.xml empleado en el proyecto.

```
<installerInformation>
  <versionId>0100</versionId>
  <version>0.1.0</version>
  <platformFileList>
     <platformFile>
        <filename>bncert-0.1.0-linux-x64.run</filename>
        <platform>linux-x64</platform>
     </platformFile>
  </platformFileList>
  <downloadLocationList>
     <downloadLocation>
        <url>https://downloads.bitnami.com/files/bncert/0.1.0/</url>
     </downloadLocation>
  </downloadLocationList>
</installerInformation>
```

Código 4.6 Comando empleado para construir el binario de auto-actualización autoupdate-linux-x64.run, desde el directorio raíz del proyecto.

```
~/installbuilder-enterprise/autoupdate/bin/customize.run build bncert-auto-
    updater.xml linux-x64
```

Código 4.7 Fichero de configuración del binario de auto-actualización.

```
[Update]
url = https://downloads.bitnami.com/files/bncert/latest/bncert-update.xml
version_id = 0100
check_for_updates = 1
update_download_location = ${system_temp_directory}
```

Código 4.8 Componente de VMware InstallBuilder para incluir el auto-actualizador dentro del ejecutable final.

```
<component>
    <name>autoupdater</name>
    <description>autoupdater</description>
    <folderList>
        <folder>
            <name>autoupdater</name>
            <description>description autoupdater</description>
            <distributionFileList>
                <distributionDirectory>
                    <origin>autoupdater</origin>
                </distributionDirectory>
            </distributionFileList>
            <destination>${system_temp_directory}</destination>
            <platforms>linux linux-x64</platforms>
        </folder>
    </folderList>
</component>
```

4.5.6 Código fuente y construcción

El código fuente y proceso para la construcción del proyecto se describen en el Apéndice D.

4.5.7 Enlaces públicos de descarga

Los binarios de la herramienta de configuración de HTTPS se van a publicar en un repositorio de Amazon S3, y la distribución del contenido a distintas regiones de disponibilidad se realizará mediante la CDN Amazon CloudFront.

Los enlaces de descarga serán los siguientes:

- Enlace asociado a la última versión (`https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run`): Permitirá a los usuarios descargar la última versión de S3 con un enlace único.
- Enlace para versión específica (`https://downloads.bitnami.com/files/bncert/version/bncert-version-linux-x64.run`, donde `version` representa la versión, como por ejemplo `0.4.2`): Con la intención de archivar binarios de versiones antiguas. No obstante, de cara a los usuarios no tendrá mucha utilidad.
- El fichero XML consultado por el auto-actualizador en cada ejecución: Contiene la información acerca de la última versión disponible de la herramienta, y permite actualizar en caso de ser anterior. Se servirá desde el enlace `https://downloads.bitnami.com/files/bncert/latest/bncert-update.xml`.

Nótese que los ficheros se almacenan en S3 a un `bucket` de S3. Con CloudFront se le puede asignar un enlace de descarga a cada fichero. Por ejemplo, la ruta donde se almacena la última versión de la herramienta es `s3://bitnami-downloads-cf/files/bncert/latest/bncert-linux-x64.run`, y CloudFront lo sirve en el enlace https://downloads.bitnami.com/files/bncert/latest/bncert-linux-x64.run.

4.5.8 Renovación automática de certificados

Como se ha mencionado anteriormente, los certificados de Let's Encrypt caducan tras un máximo de 3 meses. Por ello, se hace conveniente configurar renovación automatizada de estos, y lo habitual es emplear un planificador de tareas periódicas como Cron.

Nótese que Let's Encrypt realiza una verificación del dominio antes de proceder a la creación o renovación de un certificado, para comprobar la autenticidad del dominio. El modo de validación por defecto (`TLS-ALPN-01`) lanza un servidor escuchando en el puerto TCP 443, y es el más sencillo de implementar. Esto

cuenta con el inconveniente que es necesario parar el servidor Web en ejecución, ya que estará ocupando el mismo puerto. La solución implementada para crear el certificado con la herramienta de configuración de HTTPS de Bitnami consistía en parar el servidor Web previo a la creación, y arrancarlo de nuevo al terminar.

No obstante, no es buena idea parar y arrancar un servidor Web en tareas periódicas, puesto que puede causar inaccesibilidad durante la renovación, y en el peor caso, que no se llegue a arrancar, causando una caída total del servidor.

Para evitar esto, existen dos tipos adicionales de renovación:

- `DNS-01`: El usuario provee credenciales para que el cliente de Let's Encrypt pueda crear una entrada dinámica y aleatoria tipo `TXT` en el registro DNS del dominio, que los servidores centrales de Let's Encrypt usarán para verificar la autenticidad. No es compatible en muchos entornos.
- `HTTP-01`: El cliente de Let's Encrypt ubica un fichero en un directorio específico, que debe ser accesible desde la ruta `/.well-known/acme-challenge/<TOKEN>` desde el dominio.

El método que se usará será el `HTTP-01`, puesto que se puede automatizar en la mayoría de casos sin requerir de entornos específicos ni ajustes por parte del usuario, y es compatible con todas las instalaciones de Bitnami. Puede, sin embargo, no ser compatible con una instalación que cuente con configuración propia introducida por el usuario, en cuyo caso durante el proceso de configuración se le notificará con un enlace hacia documentación que describa cómo solucionarlo.

Para la renovación automatizada de certificados con Let's Encrypt usando validación `HTTP-01`, será necesario asociar la ruta `/.well-known` a una carpeta del sistema de ficheros con el mismo nombre, de forma que ficheros dentro de esta carpeta se puedan acceder por la URL de manera pública, y añadir una tarea programada para la renovación de certificados automatizada con la herramienta de Let's Encrypt a usar (LEGO).

Configuración en instalaciones de Bitnami

Configurar el servidor Web para que la ruta `/.well-known` se asocie a una carpeta dentro del sistema de ficheros es bastante sencillo, y con el Web Apache eso se puede conseguir con la directiva `Alias` y permitiendo el acceso del servicio a la carpeta asociada. Una configuración válida se muestra en la Figura 4.9.

Código 4.9 Configuración necesaria para renovar certificados con el servidor Web Apache.

```
1  Alias /.well-known "/opt/bitnami/apps/letsencrypt/.well-known"
2  <Directory "/opt/bitnami/apps/letsencrypt/.well-known">
3      Options +MultiViews
4      AllowOverride None
5      <IfVersion < 2.3 >
6          Order allow,deny
7          Allow from all
8      </IfVersion>
9      <IfVersion >= 2.3>
10         Require all granted
11     </IfVersion>
12 </Directory>
```

El ejemplo de la Figura 4.9 se puede activar añadiendo la configuración mencionada al fichero `/opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf`. Para que la renovación funcione, también será necesario crear la carpeta `/opt/bitnami/apps/letsencrypt/.well-known`, y cambiar los permisos de la carpeta para que el usuario que vaya a ejecutar la acción de renovar certificados pueda escribir en ella.

Tarea periódica de Cron

La configuración del trabajo periódico para la renovación de certificados automatizada hará uso de la herramienta LEGO. En particular, nos interesan las siguientes opciones del comando `lego renew`:

- `--http`: Activar validaciones tipo `HTTP-01`.
- `--http.webroot value`: Permite configurar la ruta a la carpeta que contiene el directorio `.well-known` (cuyo valor es representado por `value`).

Los trabajos periódicos de Cron permiten ejecutar un comando específico durante la hora especificada en la entrada de configuración. Todas las entradas tienen el siguiente formato:

- Minuto: De 0 a 59.
- Hora: De 0 a 23.
- Día (del mes): De 1 a 31.
- Mes: De 1 a 12.
- Día (de la semana): De 0 (domingo) a 6 (sábado).
- Comando a ejecutar.

Cron permite además una serie de modificadores como `*` (todos los valores), `,` (separar lista de valores), `-` (rango de valores), `/` (valores de paso).

Una entrada de Cron para renovar certificados compatible con instalaciones de Bitnami se muestra en el ejemplo de la Figura 4.10, y consistiría en la ejecución de un comando para renovar el certificado de Let's Encrypt con LEGO y recargar la configuración del servidor. Se observa que está programado para ejecutarse todos los días, lo cual es posible gracias a que Let's Encrypt no realiza la renovación de un certificado que no esté a punto de caducar (mínimo 30 días antes de la fecha de renovación, de 90 días).

Código 4.10 Entrada de Cron para renovación de certificados.

```
1 0 0 * * * sudo /opt/bitnami/letsencrypt/lego --path /opt/bitnami/
      letsencrypt --email="user@example.com" --http --http.webroot /opt/
      bitnami/apps/letsencrypt --domains=example.com renew && sudo /opt/
      bitnami/apache2/bin/httpd -f /opt/bitnami/apache2/conf/httpd.conf -k
      graceful
```

5 Pruebas y publicación

Una vez completado el ciclo de desarrollo, se hace necesario definir una batería de pruebas que permitan evaluar el correcto funcionamiento de la solución implementada. A continuación, se definirá una forma de automatizar el proceso de pruebas y que se pueda implantar dentro de la infraestructura de Bitnami. Finalmente, se describirá el proceso de publicación de la herramienta de configuración de HTTPS de Bitnami, aplicando durante este proceso los cambios de documentación que se identificaron en capítulos anteriores.

5.1 Plan de pruebas

5.1.1 Pruebas unitarias

La implementación de pruebas unitarias en VMware InstallBuilder es complejo, ya que no lo soporta de forma nativa. Su implementación requeriría crear distintos ficheros de proyecto por cada prueba unitaria, y la gestión de estas pruebas sería compleja. Por este motivo, nos centraremos en las pruebas de integración.

5.1.2 Pruebas de integración

Misceláneos

PI-01	Requiere de ejecución por superusuario
Descripción	Se lanza el ejecutable.
Parámetros	`--dry_run 1`
Resultado	Muestra la página de bienvenida si se lanza como un superusuario, en caso contrario muestra un mensaje de error.

Tabla 5.1 PI-01.

PI-02	Menú de ayuda
Descripción	Lanzar el ejecutable.
Parámetros	`--help`
Resultado	Muestra el menú de ayuda.

Tabla 5.2 PI-02.

PI-03	Modo desatendido (o automatizado) no soportado
Descripción	Ejecutar el programa.
Parámetros	`--mode unattended`
Resultado	Muestra un error indicando que el modo desatendido (o automatizado) no está soportado.

Tabla 5.3 PI-03.

Página de directorio de instalación

La página de directorio de instalación no se mostrará para la mayoría de usuarios, pues la intención es solo mostrarla cuando no se encuentre un directorio de instalación de Bitnami válido, simplificando así el uso de la herramienta para los usuarios.

PI-04	Página de directorio de instalación se muestra en caso de haber especificado un directorio inválido
Descripción	Sin existir una instalación de Bitnami, y con la carpeta vacía `/opt/installdir` y se ejecuta la herramienta.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	Se debe mostrar la página de directorio de instalación.

Tabla 5.4 PI-04.

PI-05	Página de directorio de instalación no se muestra en caso de haber especificado un directorio válido
Descripción	Existiendo una instalación de Bitnami WordPress Stack en `/opt/installdir`, se copia el ejecutable a este directorio y se lanza.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	No se muestra la página de directorio de instalación, puesto que `/opt/installdir` ha sido validado correctamente.

Tabla 5.5 PI-05.

PI-06	Detección automática de dirección de instalación
Descripción	Existiendo una instalación de Bitnami WordPress Stack en `/opt/bitnami`, se lanza el ejecutable.
Parámetros	`--dry_run 1`
Resultado	No se muestra la página de directorio de instalación, puesto que ha sido detectado como `/opt/bitnami`.

Tabla 5.6 PI-06.

PI-07	Detección automática de directorio de instalación según ubicación de ejecutable
Descripción	Existiendo una instalación de Bitnami WordPress Stack en `/opt/installdir`, se copia el ejecutable a este directorio y se ejecuta.
Parámetros	`--dry_run 1`
Resultado	No se muestra la página de directorio de instalación, puesto que ha sido autodetectado como `/opt/installdir`.

Tabla 5.7 PI-07.

PI-08	Página de directorio de instalación se muestra en caso de no encontrar una instalación de Bitnami
Descripción	Sin que exista una instalación de Bitnami en `/opt/bitnami` ni en el directorio donde se encuentre el ejecutable, el cual se lanza.
Parámetros	`--dry_run 1`
Resultado	Se debe mostrar la página de directorio de instalación.

Tabla 5.8 PI-08.

Página de dominios

La página de dominios permite especificar la lista de dominios para los que se desea crear un certificado HTTPS.

Para las pruebas a continuación, se debe tener una instalación de Bitnami WordPress Stack (o similar) en la ruta `/opt/bitnami`. Al lanzar el ejecutable, detectará este directorio de instalación y la primera página observada será la página de especificación de dominios.

Además, será necesario tener un dominio asociado a la dirección IP de la máquina que ejecute las pruebas. Para nuestro caso, serán `bncert.bntestdomain.cf`, `www.bncert.bntestdomain.cf` y `bncert-no-www.bntestdomain.cf` (este último dominio sin un subdominio `www` asociado), para que las validaciones DNS se puedan probar.

PI-09	Permitir un único dominio válido
Descripción	En la página de introducción de dominios, se especifica un único dominio válido, `bncert.bntestdomain.cf` y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	El dominio es validado correctamente y se ha pasado a la página siguiente.

Tabla 5.9 PI-09.

PI-10	Permitir múltiples dominios (separados por espacio)
Descripción	En la página de introducción de dominios, se especifican los dominios `bncert.bntestdomain.cf www.bncert.bntestdomain.cf` y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	Los dominios han sido validados correctamente y se ha pasado a la página siguiente.

Tabla 5.10 PI-10.

PI-11	Se puede especificar uno o varios dominios (separados por espacio) con la opción `--domains`
Descripción	En la página de introducción de dominios se pulsa el botón siguiente.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	El dominio ha sido validado correctamente y se ha pasado a la siguiente página.

Tabla 5.11 PI-11.

PI-12	No se puede especificar un dominio inválido
Descripción	En la página de introducción de dominios, se especifica el valor incorrecto `dom@!n.com` y se puilsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	La validación del dominio muestra un error acerca del formato de este.

Tabla 5.12 PI-12.

PI-13	Los dominios deben tener menos de 64 caracteres (por limitaciones de Let's Encrypt)
Descripción	En la página de introducción de dominios, se especifica un dominio con más de 64 caracteres y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	La validación del dominio muestra un error acerca de la longitud de este.

Tabla 5.13 PI-13.

PI-14	No se permiten subdominios de nip.io ni xip.io (por limitaciones de Let's Encrypt)
Descripción	En la página de introducción de dominios, se especifica un subdominio de nip.io y/o xip.io y se pulsa el botón 'Siguiente'
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	La validación del dominio muestra un error acerca de que no se permiten subdominios de nip.io y/o xip.io.

Tabla 5.14 PI-14.

PI-15	Se debe comprobar que un dominio resuelva a una dirección IP
Descripción	En la página de introducción de dominios, se especifica `thisdomaindoesnotresolve.com` y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	La validación del dominio muestra un error acerca del dominio no siendo resoluble a una dirección IP.

Tabla 5.15 PI-15.

PI-16	Se debe comprobar que un dominio resuelva a la dirección IP actual
Descripción	En la página de introducción de dominios, se especifica `bitnami.com` y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	La validación del dominio muestra un error acerca de que el dominio no resuelve a la dirección IP de la máquina actual.

Tabla 5.16 PI-16.

PI-17	Detección de certificado Let's Encrypt existente
Descripción	Existiendo un certificado pre-configurado con los dominios `bncert.bntestdomain.cf www.bncert.bntestdomain.cf`, se introduce la misma lista de dominios y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	Se muestra un mensaje de aviso acerca de que ya existe un certificado para estos dominios, y que en lugar de crear uno nuevo, ejecutará una renovación. A continuación se accede a la página siguiente.

Tabla 5.17 PI-17.

PI-18	Reemplazo de certificado Let's Encrypt existente en caso de no coincidir los dominios especificados
Descripción	Existiendo un certificado pre-configurado con los dominios `bncert.bntestdomain.cf www.bncert.bntestdomain.cf`, se introduce `bncert.bntestdomain.cf bncert-no-www.bntestdomain.cf` y se pulsa el botón 'Siguiente'.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	Se muestra un mensaje de aviso acerca de que ya existe un certificado para estos dominios, y que la lista de dominios no coincide. Por ello, se deja al usuario la opción de volver a introducir la lista de dominios, o seguir a la página siguiente y que se reemplace el certificado.

Tabla 5.18 PI-18.

Página de cambios a realizar

PI-19	Acciones a realizar por defecto, dado un dominio válido
Descripción	Se ejecuta el programa y se comprueba la lista de acciones a realizar.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	Muestra el listado de acciones por defecto, incluyendo redirecciones de HTTP a HTTPS y no-www a www activadas.

Tabla 5.19 PI-19.

PI-20	Desactivar redirección HTTP a HTTPS
Descripción	Se ejecuta el programa. En la página de configuración de redirecciones, se desactiva la redirección de HTTP a HTTPS.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	En la página de cambios a realizar, la redirección de HTTP a HTTPS no está activada.

Tabla 5.20 PI-20.

PI-21	Desactivar redirección no-www a www

Descripción	Se ejecuta el programa. En la página de configuración de redirecciones, se desactiva la redirección de no-www a www.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	En la página de cambios a realizar, la redirección de no-www a www no está activada.

Tabla 5.21 PI-21.

PI-22	Activar redirección www a no-www
Descripción	Se ejecuta el programa. En la página de configuración de redirecciones, se activa la redirección de www a no-www.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	En la página de cambios a realizar, la redirección de www a no-www está activada.

Tabla 5.22 PI-22.

PI-23	No se pueden activar redirecciones de no-www a www y viceversa de manera simultánea
Descripción	Se ejecuta el programa. En la página de configuración de redirecciones, se activa la redirección de no-www a www y de www a no-www.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	El programa muestra un error, indicando que no es posible activar las dos redirecciones a la vez.

Tabla 5.23 PI-23.

Página de configuración de Let's Encrypt

PI-24	Validación de correo electrónico
Descripción	Se ejecuta el programa, introduciendo un dominio válido y usando las opciones recomendadas. En la página de configuración de Let's Encrypt, se introduce un correo electrónico no válido.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	Se muestra un error, indicando que el correo electrónico no es válido.

Tabla 5.24 PI-24.

PI-25	Es necesario aceptar el acuerdo de suscripción de Let's Encrypt
Descripción	Se ejecuta el programa, introduciendo un dominio válido y usando las opciones recomendadas. En la página de configuración de Let's Encrypt, el usuario no acepta el acuerdo de suscripción de Let's Encrypt.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`

Resultado	El programa muestra un error, indicando que es obligatorio aceptar el acuerdo de suscripción de Let's Encrypt.

Tabla 5.25 PI-25.

PI-26	Se puede continuar a la siguiente página si las opciones son correctas
Descripción	Se ejecuta el programa, introduciendo un dominio válido y usando las opciones recomendadas. En la página de configuración de Let's Encrypt, se introduce un correo electrónico válido y se acepta el acuerdo de suscripción de Let's Encrypt.
Parámetros	`--dry_run 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	El programa pasa a la página de confirmación.

Tabla 5.26 PI-26.

5.1.3 Pruebas funcionales

PF-01	Modo de ejecución en seco no modifica la instalación existente
Descripción	Se ejecuta el programa y se usa la configuración por defecto. Se continúa hasta la finalización de la ejecución de la herramienta.
Parámetros	`--dry_run 1 --use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	No se ha modificado el fichero de `cron`.

Tabla 5.27 PF-01.

PF-02	Creación de copias de seguridad
Descripción	Se realizan copias de seguridad de ficheros al lanzar el programa.
Parámetros	`--installdir /opt/installdir`
Resultado	Existen ficheros con la extensión `.back`, copiados de ficheros de configuración de Apache, creados una vez alcanzada la página de introducción de dominios.

Tabla 5.28 PF-02.

PF-03	No se crean de copias de seguridad con la opción de ejecución en seco
Descripción	No se realizan copias de seguridad de ficheros con la opción de ejecución en seco.
Parámetros	`--dry_run 1 --installdir /opt/installdir`
Resultado	No existe ningún fichero con la extensión `.back` una vez alcanzada la página de introducción de dominios.

Tabla 5.29 PF-03.

PF-04	Ejecución completa sin redirecciones
Descripción	Se ejecuta el programa con las opciones por defecto, pero desactivando todas las redirecciones.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	La instalación contiene un certificado válido. El certificado está configurado correctamente en la instalación, de forma que una petición HTTP es correcta.

Tabla 5.30 PF-04.

PF-05	Ejecución sobre instalación ya configurada
Descripción	Se ejecuta el programa sobre una instalación ya configurada con la herramienta, con las opciones por defecto.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	El certificado no se ha modificado, al coincidir la lista de dominios. Tampoco se ha realizado ningún cambio en la instalación.

Tabla 5.31 PF-05.

PF-06	Ejecución completa con redirección de HTTP a HTTPS sobre instalación ya configurada
Descripción	Se ejecuta el programa sobre una instalación ya configurada con la herramienta, con las opciones por defecto, salvo redirecciones, activando solo de HTTP a HTTPS.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	La instalación contiene configuración válida de redirección de HTTP a HTTPS.

Tabla 5.32 PF-06.

PF-07	Ejecución completa con redirección de no-www a www
Descripción	Se ejecuta el programa sobre una instalación ya configurada con la herramienta, con las opciones por defecto, salvo redirecciones, activando solo de no-www a www.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	La instalación contiene configuración válida de redirección de no-www a www.

Tabla 5.33 PF-07.

PF-08	Ejecución completa con redirección de www a no-www
Descripción	Se ejecuta el programa sobre una instalación ya configurada con la herramienta, con las opciones por defecto, salvo redirecciones, activando solo de www a no-www.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf --email testbitnamismtp@gmail.com`
Resultado	La instalación contiene configuración válida de redirección de www a no-www.

Tabla 5.34 PF-08.

PF-09	No se pueden configurar redirecciones si han sido configuradas por otro medio
Descripción	Se ejecuta el programa en una instalación con redirecciones ya configuradas de forma manual.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	En la página de configuración de redirecciones, se muestra un aviso indicando que no es posible configurar redirecciones en esta instalación.

Tabla 5.35 PF-09.

PF-10	El fichero de cron se configura para activar renovación automatizada del dominio
Descripción	Se ejecuta el programa. Una vez finalizado, se comprueba el fichero de `cron`.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	El fichero de `cron` contiene una línea para la renovación automatizada del dominio.

Tabla 5.36 PF-10.

PF-11	El fichero de cron no se vuelve a configurar para la renovación automatizada del dominio
Descripción	Se ejecuta el programa sobre una instalación ya configurada con la herramienta. Una vez finalizado, se comprueba el fichero de `cron`.
Parámetros	`--use_staging 1 --installdir /opt/installdir --domains bncert.bntestdomain.cf`
Resultado	Existe solo una línea de `cron` para la renovación automatizada del dominio.

Tabla 5.37 PF-11.

5.1.4 Pruebas de aceptación

PA-01	Superación de pruebas de integración y pruebas funcionales
Descripción	Se realiza una comprobación, ya sea manual o automática, del cumplimiento de todas las pruebas definidas con anterioridad.
Resultado	Superación de todas y cada una de las pruebas.

Tabla 5.38 PA-01.

5.2 Pruebas automatizadas

Una vez definidas todas las pruebas, se procede a desarrollar en un segundo plano un sistema de pruebas automatizado, sin bloquear a la publicación de la herramienta para que los usuarios puedan ir aportando sus comentarios de uso.

En esta sección se describirá de forma resumida el proceso de diseño e implementación del sistema de pruebas, comenzando por un listado de requisitos básicos, una propuesta técnica y la implementación. Finalmente, se describirá cómo ejecutarlo y el proceso de definición de nuevas pruebas.

5.2.1 Requisitos

El sistema de pruebas automatizado debe cumplir con los siguientes requisitos:

- Probar herramientas interactivas en modo texto: Es la forma recomendada de uso de la herramienta de configuración de HTTPS de Bitnami, y por ello será en la que nos centraremos en probar. Para ello deberá ser capaz de enviar texto por entrada estándar y ser capaz de esperar (y comprobar) una respuesta de este ejecutable.
- Sencillo de implementar en el sistema de pruebas de Bitnami: Se desea que todo el proceso de construcción, pruebas y publicación se automatice en un futuro próximo. Para ello, deberá ser sencillo implementar el sistema de pruebas en el entorno de Bitnami.
- Ejecución de varios escenarios de pruebas: Se desea que lanzar el sistema pueda ejecutar toda una batería de pruebas, sin tener que ir una a una.
- Forma sencilla de añadir nuevas pruebas: Añadir nuevas pruebas deberá evitar requerir de conocimientos avanzados de programación.
- Preparación de escenario de pruebas avanzado: Deberá permitir preparar un escenario para una prueba específica, por ejemplo, configurar la máquina para conocer un nombre de host, y deshacer el cambio tras la finalización de esta.
- De código abierto: Por aspectos legales, para que se pueda implementar dentro del sistema de construcción/pruebas de Bitnami, deberá estar basado en código abierto.

5.2.2 Propuesta técnica

Se va a recurrir al uso de la herramienta Expect [8], basada en TCL, que es utilizada para probar ejecutables interactivos en modo texto. El uso de esta solución cuenta con varios puntos positivos:

- La idea principal consiste en probar binarios ejecutables en modo texto, permitiendo enviar un comando y esperar una respuesta determinada, fallando en caso de ser distinta a la deseada.
- El sistema de construcción y pruebas actual de Bitnami está basado en TCL. Será, por lo tanto, posible implementarlo de forma nativa dentro del sistema sin requerir de grandes cambios.
- Al estar basado en TCL y ser de código abierto, se tiene acceso a un lenguaje de programación interpretado completo con el que se pueden realizar acciones tanto básicas como complejas, por ejemplo, crear una interfaz para definir pruebas sencillo y preparar escenarios avanzados.

No obstante, cuenta con una desventaja importante, y es que por defecto solo ejecuta un escenario de pruebas. Por ello, habrá que adaptarlo a permitir ejecutar una batería de pruebas, que tras analizarlo se considera sencillo.

5.2.3 Implementación

Una vez definida una propuesta técnica que cumpla con los requisitos básicos establecidos, se procede a la implementación del sistema de pruebas. Para ello, antes de comenzar, se necesita definir y construir las dependencias necesarias del proyecto. A continuación, se definirá la estructura de ficheros del proyecto, la configuración necesaria y finalmente se describirá cómo se realiza la definición de pruebas y la ejecución de estas.

Dependencias

Se hará uso de los proyectos Tclkit [7] y Expect [8], empaquetándose en un binario resultante `tclkit` que contenga las bibliotecas necesarias y que permita ejecutar ficheros con extensión `.tcl`.

Para construir el ejecutable `tclkit` es necesario ejecutar el Código 5.1, generando el fichero deseado en la carpeta `output`, que deberá ubicarse en uno de los directorios definidos en la variable de entorno `PATH` del sistema Linux.

Código 5.1 Comandos para construir e instalar el ejecutable tclkit.

```
1 $ cd src/tclkit && ./build.sh
2 $ mv ./output/tclkit /usr/local/bin/
```

Estructura de directorios

- `bin/`: Binarios del proyecto. Contiene el ejecutable `run` para lanzar la batería de pruebas.
- `inputs_for_tests/`: Carpeta que contiene ficheros a utilizar en las pruebas. En esta se incluye el binario de ejecución de la herramienta de configuración de HTTPS de Bitnami, la carpeta comprimida de una instalación de Bitnami válida (Bitnami WordPress Stack) y certificados HTTPS de ejemplo.
- `lib/`: Ficheros de bibliotecas para ejecución de pruebas.
- `src/`: Ficheros necesarios para construir binarios del proyecto. En particular, contiene la carpeta `tclkit` que permite construir el ejecutable al que da nombre.
- `tests/`: Ficheros de pruebas del proyecto; en particular están organizados en la carpeta `integration` para pruebas de integración y `functional/` para pruebas funcionales.
- `env.tcl`: El fichero de configuración del sistema de pruebas.

Configuración

Debido a la variedad de escenarios a ejecutar, se ha creado el fichero de configuración `env.tcl` en la raíz del proyecto del sistema de pruebas automatizado, cuyos ajustes deben ser adecuados para una satisfactoria ejecución de este. Contiene la siguiente configuración:

- Configuración de carpetas (por norma general no será necesario cambiarlo, puesto que se configuran de manera automática).
- Ruta absoluta al binario que se desea probar. Por defecto, se espera que exista un único fichero con la extensión `.run` en la carpeta `inputs_for_tests`.
- Un dominio resoluble que apunta a la instancia actual, incluyendo su par `www`. Por defecto es `bncert.bntestdomain.cf` (asociado a `www.bncert.bntestdomain.cf`).
- Un dominio resoluble que apunte a la instancia actual, pero sin un par `www` asociado. Por defecto es `bncert-no-www.bntestdomain.cf`.
- Un correo de electrónico válido, utilizado para la creación de un certificado con Let's Encrypt.

Definición de nuevas pruebas

Definir una nueva prueba es muy sencillo; para ello es necesario crear un fichero de pruebas que realice las acciones listadas a continuación:

- Cargar el fichero de configuración `env.tcl`, descrito anteriormente.

- Lógica de preparación de escenarios (opcional). El lenguaje de programación TCL es bastante potente, permitiendo así realizar una amplia gama de acciones, desde ejecutar comandos del sistema, crear o modificar directorios/ficheros, etc.
- Lógica de restauración de escenarios (opcional). Tras realizar un cambio en el sistema, se recomienda revertir el cambio para no afectar a otras pruebas.
- Definición de un escenario mediante `scenario`. Contiene dos argumentos; una descripción y un bloque de código. Dentro de este se pueden realizar distintas acciones:
  - Lanzar un proceso con `spawn`.
  - Comprobar que la salida obtenida del proceso corresponde con la deseada con `expect_test`.
  - Enviar datos por entrada estándar mediante `send`.
  - Ejecutar código en formato TCL en caso de que fuera necesario. Las tres acciones anteriores están basadas, de hecho, en este lenguaje de programación.

Ejemplo de fichero de pruebas

Como ilustración vamos a basarnos en un ejemplo sencillo que comprueba que el binario de ejecución muestra un error si no se ejecuta como superusuario, en `tests/integration/user.tcl` (Código 5.2). En este fichero se definen dos escenarios:

- El binario no se puede ejecutar como un usuario sin privilegios: Se lanza el binario sin privilegios y se espera a un mensaje de error específico. En caso de que muestre el error, la prueba terminará exitosamente, y en caso contrario el sistema mostraría un error.
- El binario se puede ejecutar como un superusuario: Se lanza el binario con privilegios de superusuario vía `sudo`, y se comprueba que el proceso muestre el texto correspondiente a la página de bienvenida.

Código 5.2 Comando requerido para ejecutar las pruebas individuales sobre el menú de ayuda.

```
1  #!/usr/bin/expect
2
3  source env.tcl
4
5  scenario "Cannot be launched as a normal user" {
6      spawn $tool --dry_run 1
7      expect_test "Can not be launched by normal users" "*This installer
           requires root privileges*Press \\\[Enter\\\] to continue:"
8      send "\r"
9      expect_test "Process exited" eof
10 }
11
12 scenario "Can be launched as a superuser" {
13     spawn sudo $tool --dry_run 1
14     expect_test "Can be launched by superusers" "*Welcome*"
15 }
```

Código fuente

En la Subsección D.4 se describen los ficheros de código fuente asociados al sistema de pruebas automatizado.

Ejecución del sistema de pruebas

El proceso de ejecución del sistema de pruebas consiste en ejecutar el comando mostrado en Código 5.3, que permitirá ejecutar todas las pruebas definidas en la carpeta `tests` de manera ordenada:

Código 5.3 Comando requerido para lanzar toda la batería de pruebas del sistema de pruebas automático.

```
1  $ tclkit bin/run
```

Por el diseño del sistema de pruebas, es posible además lanzar un grupo de pruebas individual mediante la ejecución del fichero donde están definidos. En el Código 5.4 se muestra cómo ejecutar los grupos de pruebas relacionadas con el menú de ayuda, entendiéndose que todos se encuentran definidos dentro del fichero `tests/integration/help.tcl`.

Código 5.4 Comando requerido para ejecutar las pruebas individuales sobre el menú de ayuda.

```
1 $ tclkit tests/integration/help.tcl
```

5.2.4 Mejoras futuras

Se planifican como mejoras futuras al sistema de pruebas automatizado los siguientes elementos:

- Ejecución en un entorno controlado vía Docker, de forma que no se modifiquen ficheros del sistema de ficheros de la instancia actual, y se tenga acceso a las dependencias.
- Configuración mediante parámetros y/o variables de entorno, evitando tener que recurrir a un fichero de configuración.

5.3 Publicación

Como se ha mencionado en la sección anterior, la publicación se realiza de manera prioritaria al diseño e implementación del sistema de pruebas automatizado, ya que resulta de especial interés el que los usuarios puedan hacer uso de la nueva solución para configurar HTTPS en sus instalaciones de Bitnami.

5.3.1 Proceso de publicación

Previa publicación inicial de la herramienta de configuración de HTTPS de Bitnami, se realiza además una presentación interna a todo el equipo de Bitnami enfocada a la creación de un certificado HTTPS en menos de un minuto, obtieniendo muy buena respuesta.

A continuación, se define el proceso de publicación, que contiene los siguientes pasos:

- Construcción del binario: Se construye el binario de Linux de 64-bits de la herramienta de configuración de HTTPS de Bitnami con VMware InstallBuilder (tal como se describe en la Subsección D.3).
- Pruebas sobre el binario construido: Se realizan las pruebas descritas anteriormente (de forma manual mientras no esté implementado el sistema de pruebas automatizado), asegurando que todo funciona correctamente y se puede proceder con el sistema de publicación.
- Publicación de nueva versión: Se suben los ficheros mencionados en la Subsección 4.5.7 a Amazon CloudFront, vía repositorio de Amazon S3 y asociado al servidor Amazon CloudFront correspondiente al dominio https://downloads.bitnami.com/. Se actualizan también los ficheros necesarios para hacer funcionar el auto-actualizador de versiones antiguas de la herramienta.
- Actualización de documentación: Se procede a actualizar la documentación pública relacionada con la creación de certificados en instalaciones de Bitnami, y documentación interna de soporte y mantenimiento de la herramienta. Ver Subsección 5.3.2.

5.3.2 Cambios en documentación

El último paso antes de hacer pública la versión a los usuarios consiste en documentar extensamente, tanto a nivel público de uso, como interno para permitir el mantenimiento por otros miembros del equipo de la herramienta de configuración de HTTPS de Bitnami.

Documentación pública

Los cambios realizados sobre la documentación pública de Bitnami, que se encuentra disponible en el enlace https://docs.bitnami.com/, se actualiza de la siguiente forma:

- Creación de una página dedicada a la herramienta de configuración de HTTPS de Bitnami. Contiene instrucciones de instalación, una guía básica de uso y un apartado de solución de problemas más comunes.
- Actualizar la guía general de creación de certificados HTTPS con Let's Encrypt, para hacer menciones a la mejorada herramienta de configuración de HTTPS de Bitnami en lugar de la anterior, basada en Bash y mencionada con anterioridad en este proyecto.
- Actualizar la guía resumida de configuración de un certificado HTTPS de Let's Encrypt, disponible en la página individual de cada Stack de Bitnami. A diferencia de la anterior, esta se incluye para las páginas de documentación específicas para cada aplicación, y, por lo tanto, es más sencilla. Se incluye un ejemplo básico de uso de la herramienta y se enlaza a las anteriores páginas.

Documentación interna

Se procede a crear documentación interna sobre los siguientes aspectos:

- Notas de implementación y diseño, con la intención de facilitar a otros miembros del equipo de ingeniería desarrollar mejoras a la solución.
- Guía básica de construcción de binarios.
- Guía de publicación de binarios construidos.

5.3.3 Publicación inicial

Para la publicación de la primera versión se ha decidido no publicitarla en canales públicos, sino recurrir de forma exclusiva a páginas de documentación. De esta forma, se espera que el uso de la herramienta aumente gradualmente y se pueda detectar problemas de forma temprana, en caso de haberlos.

En este punto se considera que el binario es final, todas las pruebas están definidas y todo está listo para comenzar el proceso de publicación. Así, en la Tabla 5.39 se listan todas las pruebas definidas anteriormente, con la anotación del resultado obtenido y cualquier comentario adicional. La publicación requiere el cumplimiento de todas ellas, salvo casos justificados.

Prueba	Superada	Comentarios
PI-01: Requiere de ejecución por superusuario	Sí	
PI-02: Menú de ayuda	Sí	
PI-03: Modo desatendido (o automatizado) no soportado	Sí	
PI-04: Página de directorio de instalación se muestra en caso de haber especificado un directorio inválido	Sí	
PI-05: Página de directorio de instalación no se muestra en caso de haber especificado un directorio válido	Sí	
PI-06: Detección automática de dirección de instalación	Sí	
PI-07: Detección automática de directorio de instalación según ubicación de ejecutable	Sí	
PI-08: Página de directorio de instalación se muestra en caso de no encontrar una instalación de Bitnami	Sí	
PI-09: Permitir un único dominio válido	Sí	
PI-10: Permitir múltiples dominios (separados por espacio)	Sí	
PI-11: Se puede especificar uno o varios dominios (separados por espacio) con la opción `--domains`	Sí	
PI-12: No se puede especificar un dominio inválido	Sí	
PI-13: Los dominios deben tener menos de 64 caracteres (por limitaciones de Let's Encrypt)	Sí	
PI-14: No se permiten subdominios de nip.io ni xip.io (por limitaciones de Let's Encrypt)	Sí	
PI-15: Se debe comprobar que un dominio resuelva a una dirección IP	Sí	
PI-16: Se debe comprobar que un dominio resuelva a la dirección IP actual	Sí	

PI-17: Detección de certificado Let's Encrypt existente	Sí	
PI-18: Reemplazo de certificado Let's Encrypt existente en caso de no coincidir los dominios especificados	Sí	
PI-19: Acciones a realizar por defecto, dado un dominio válido	Sí	
PI-20: Desactivar redirección HTTP a HTTPS	Sí	
PI-21: Desactivar redirección no-www a www	Sí	
PI-22: Activar redirección www a no-www	Sí	
PI-23: No se pueden activar redirecciones de no-www a www y viceversa de manera simultánea	Sí	
PI-24: Validación de correo electrónico	Sí	
PI-25: Es necesario aceptar el acuerdo de suscripción de Let's Encrypt	Sí	
PI-26: Se puede continuar a la siguiente página si las opciones son correctas	Sí	
PF-01: Modo de ejecución en seco no modifica la instalación existente	Sí	
PF-02: Creación de copias de seguridad	Sí	
PF-03: No se crean de copias de seguridad con la opción de ejecución en seco	Sí	
PF-04: Ejecución completa sin redirecciones	Sí	
PF-05: Ejecución sobre instalación ya configurada	Sí	
PF-06: Ejecución completa con redirección de HTTP a HTTPS sobre instalación ya configurada	Sí	
PF-07: Ejecución completa con redirección de no-www a www	Sí	
PF-08: Ejecución completa con redirección de www a no-www	Sí	
PF-09: No se pueden configurar redirecciones si han sido configuradas por otro medio	Sí	
PF-10: El fichero de cron se configura para activar renovación automatizada del dominio	Sí	
PF-11: El fichero de cron no se vuelve a configurar para la renovación automatizada del dominio	Sí	

Tabla 5.39 Superación de pruebas para la publicación.

Tras la confirmación de que todo es correcto, se da luz verde a la publicación y se procede a hacer los cambios de documentación públicos, y a que la herramienta esté disponible para descarga en los enlaces definidos con anterioridad.

La herramienta de configuración de HTTPS de Bitnami, o Bncert, se publicó el 10 de mayo del 2019.

6 Validación de resultados

Tras la publicación de la herramienta de configuración de HTTPS de Bitnami, Bncert, y la actualización de guías y tutoriales relacionados, se ha realizado un nuevo análisis de casos de soporte para estudiar el impacto de la solución. Esto permitirá comprender si la herramienta ha mejorado la situación, además de encontrar mejoras que realizar para maximizar el impacto positivo causado.

6.1 Segundo análisis de casos de soporte

El primer análisis de casos de soporte se realizó para los meses de septiembre y octubre del 2018, y está descrito con detalle en el Apéndice A. Este análisis dio resultado a la herramienta de configuración de HTTPS de Bitnami, Bncert, que se publicó en el mes de mayo del 2019.

Para poder observar los cambios de tendencia, que nos permitirá estudiar el impacto causado por Bncert, se ha realizado un segundo análisis de casos de soporte siguiendo los mismos criterios adoptados en el análisis inicial del año 2018:

- La fuente de casos escogida es la del foro oficial de soporte de Bitnami.
- Todos los casos afectando a Bitnami WordPress Stack y Bitnami WordPress Multisite Stack que hacen uso del servidor Web de Apache.
- Los meses escogidos para el análisis son septiembre y octubre del año 2019, los mismos del análisis anterior y además tres meses posteriores a la publicación de la herramienta, dando tiempo para ser adoptada por usuarios de Bitnami.

El análisis completo, caso por caso, se encuentra en el Apéndice B. En dicho análisis se estudian los siguientes aspectos:

- La cantidad de nuevos casos en comparación con el año anterior.
- Para todos los casos: La temática principal de cada caso (como configuración de HTTPS o instalación de estilos de WordPress), junto con un breve resumen de cada uno.
- Para los casos de configuración de HTTPS:
  - La complejidad de cada uno en cuanto a posibilidades de automatización. Un caso se podrá resolver con una automatización sencilla, compleja o no habrá automatización posible.
  - El objetivo de cada caso; de creación de certificados, renovación de certificados o relacionado con redirecciones creadas por la herramienta.
  - El problema principal encontrado por el usuario en cada caso.
  - Si hace uso de la nueva herramienta de configuración de HTTPS de Bitnami, o Bncert, en cuyo caso se estudia también el correcto funcionamiento de esta.

6.1.1 Vista generalizada

Entre los meses de septiembre y octubre del 2019 hubo 314 casos de soporte, 103 más que en el análisis de la misma fecha del año anterior, suponiendo un incremento prácticamente del 50 % con respecto al año anterior (cuando hubo 211).

Los principales temas encontrados coinciden en gran parte con los del análisis anterior:

- Configuración de certificados HTTPS creados con Let's Encrypt: 18.15 % (+4.41 %): 57 casos. Crecimiento en términos absolutos del 96 % con respecto al año anterior.
- Configuración de WordPress: 7.64 % (-1.36 %): 24 casos.
- Configuración de Apache: 7.32 % (-0.26 %): 23 casos.
- Extensiones (plug-ins) de WordPress: 6.69 % (-1.84 %): 21 casos.
- Misceláneos: 6.05 % (-2.01 %): 19 casos.
- Rendimiento: 5.73 % (+0.32 %): 18 casos.
- Redirecciones: 4.78 % (-3.28 %): 15 casos.

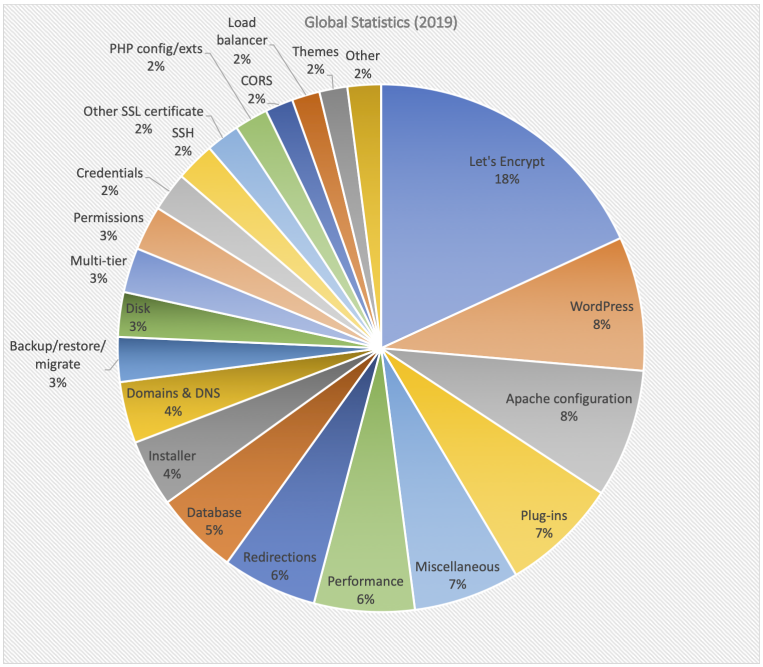


Figura 6.1 Porcentaje de casos de cada temática en el análisis de casos de soporte (2019).

6.1.2 Análisis de casos de configuración de HTTPS

Con los resultados mostrados en el apartado anterior, se observa un crecimiento muy significativo de la proporción de casos de soporte relacionado a configuración de HTTPS en instalaciones de Bitnami con Let's Encrypt, calculado en un del 4.41 % en términos relativos, y 96 % en términos absolutos.

A continuación se estudiarán estos resultados más a fondo, tratando de determinar factores externos que han podido influir en estos resultados, y si la publicación de Bncert puede haber afectado a esta cifra.

Crecimiento del uso de Let's Encrypt

La popularización de Let's Encrypt como autoridad de certificación está en constante aumento. En la Figura 6.2 se muestra la evolución del uso de Let's Encrypt desde su creación hasta abril del 2020, y se incluyen a continuación las estadísticas publicadas para el día de 1 de septiembre de 2018 y 2019 [56]:

- Nombres de dominio: 128M (2018) y 180M (2019), con crecimiento del 40 %.
- Certificados activos: 80M (2018) y 109M (2019), con crecimiento del 36 %.
- Dominios registrados activos: 40M (2018) y 54M (2019), con crecimiento del 35 %.

Teniendo en cuenta el crecimiento aproximado del 50 % de nuevos casos en el foro de soporte de Bitnami, y del 35 % de nuevos certificados de Let's Encrypt, en ambos casos suman un total del 85 %. Esto es compatible con el crecimiento en términos absolutos del 96 % de nuevos casos de soporte de Let's Encrypt identificados anteriormente.

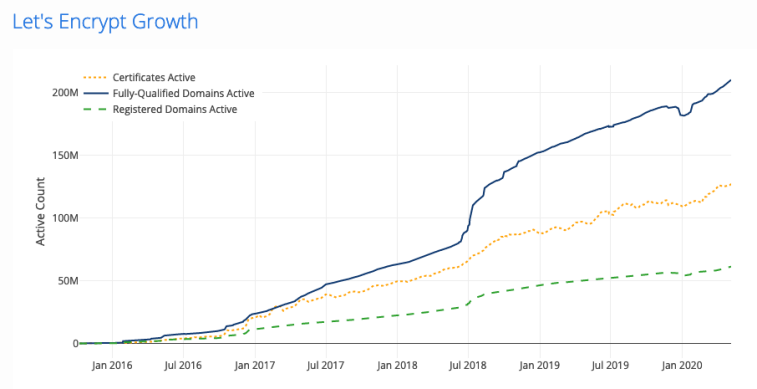


Figura 6.2 Evolución del uso de Let's Encrypt desde 2016 hasta abril del 2020 (fuente: Let's Encrypt) [56].

Evolución de la complejidad de los casos

A continuación se va a proceder a analizar la evolución de la complejidad de los casos sobre configuración de HTTPS, que permitirán observar si la publicación de Bncert ha tenido un impacto. En la Figura 6.3 se muestran los resultados del análisis del año 2018, y en la Figura 6.4 los del actual análisis.

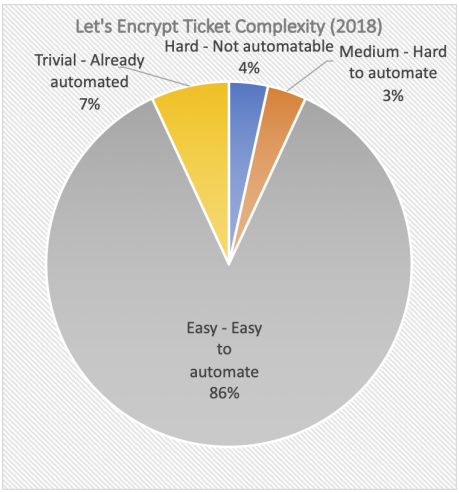


Figura 6.3 Estadísticas de complejidad de casos de configuración de HTTPS (2018).

En estas figuras se han tenido en cuenta las siguientes categorías:

- `Trivial - Already automated`: Casos triviales que se refieran a automatizaciones que ya están disponibles, pero de las cuales el usuario no ha hecho uso.
- `Easy - Easy to automate`: Casos sencillos que se pueden automatizar de forma sencilla, cuya implementación en Bncert sería deseable.
- `Medium - Hard to automate`: Complejidad media, cuya automatización es compleja pero factible.
- `Hard - Not automatable`: Casos de categorización compleja, que no pueden ser automatizados o que no tendría sentido. Esto se puede deber a requisitos muy específicos, requerir configuración de servicios externos a la máquina fuera de las posibilidades de Let's Encrypt, entre otros.

Se puede observar un cambio de tendencia muy importante, que se resumirá en un par de puntos:

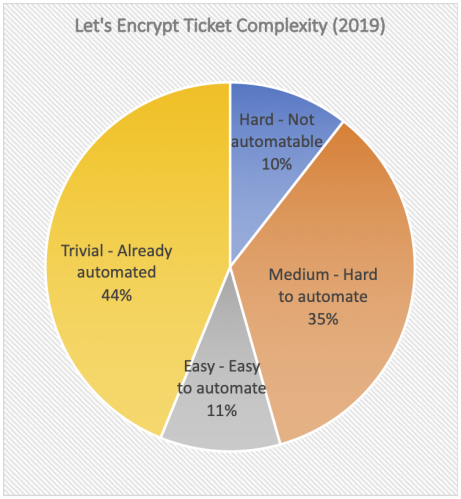


Figura 6.4 Estadísticas de complejidad de casos de configuración de HTTPS (2019).

- Destaca un 44 % de casos que se consideran triviales (en comparación con el 7 % del 2018), lo cual significa que el usuario ya dispone de una automatización con Bncert. Dentro de esta categoría pueden incluirse algunos casos en los que el usuario hizo uso de Bncert desde el principio, pero no lo ejecutó correctamente. Estos casos merecen la pena estudiarlos para mejorar la usabilidad de cara al usuario.
- Los casos sencillos y fáciles de automatizar han bajado desde el 86 % en 2018, a un 11 %. Mientras, los casos de automatización compleja y no automatizables han pasado de representar el 7 % a más del 45 %. Esto muestra que la complejidad de los casos de configuración de HTTPS ha crecido en este año.

Evolución del objetivo principal de los casos

Interesa estudiar el objetivo principal de los usuarios en cada ticket, para observar la evolución entre el 2018 y 2019. Se propone la siguiente categorización:

- `Creation`: Creación de un nuevo certificado HTTPS con Let's Encrypt, y configuración necesaria para habilitar HTTPS en la instalación de Bitnami.
- `Renewal`: Configuración de la renovación automatizada de un certificado HTTPS existente de Let's Encrypt.
- `Redirection`: Sobre configuración de redirecciones tras activar HTTPS.

En la Figura 6.5 y la Figura 6.6 se muestran los resultados del 2018 y 2019, respectivamente. Se observa un gran aumento respecto a la configuración de renovación automatizada de certificados HTTPS, pasando de representar un 3 % en 2018 a un 44 % en 2019.

Es importante hacer notar que durante el proceso de implementación se observó que el enfoque utilizado con la utilidad `generate-certificates.sh`, previa a Bncert, no funcionaba correctamente. Además, en Bncert, la implementación escogida, que usa el mecanismo de validación `HTTP-01` de Let's Encrypt, requiere configuración adicional en la instalación de Bitnami y puede dar problemas en casos especiales.

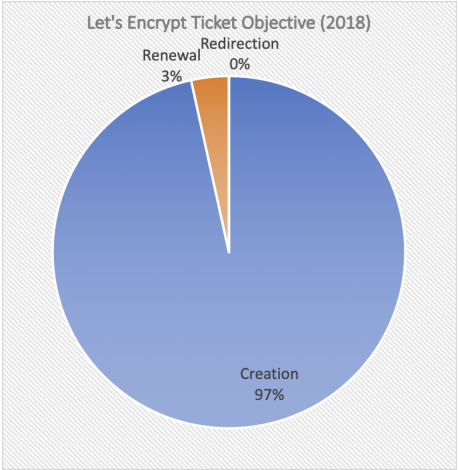


Figura 6.5 Estadísticas del objectivo principal de casos de configuración de HTTPS (2018).

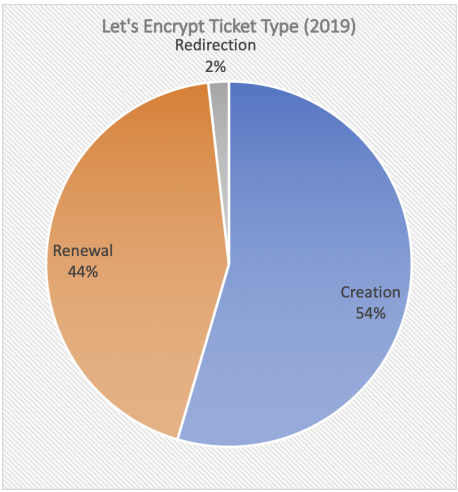


Figura 6.6 Estadísticas del objectivo principal de casos de configuración de HTTPS (2019).

Uso de Bncert

No se disponen de estadísticas individuales de uso de Bncert por decisión de diseño. No obstante, sí que nos es posible obtener la cantidad de descargas (Figura 6.7), que pese a ser un indicador muy básico, es compatible asociar una descarga con al menos un uso individual.

Para observar el impacto en los foros de soporte de Bitnami, se han recopilado datos de los casos que han hecho uso de la herramienta, cuyos resultados se muestran en la Figura 6.8 y categorizados de la siguiente forma:

- `Yes` (45.61 %, 26 casos): El caso de soporte ha usado Bncert en algún punto.
- `No` (45.61 %, 26 casos): No se ha hecho uso de Bncert, en su lugar se ha utilizado la utilidad `generate-certificates.sh`, `certbot` o cualquier otra herramienta.
- `Unknown` (8.77 %, 5 casos): No se sabe con certeza qué herramienta ha utilizado para generar el certificado de Let's Encrypt.

En la Figura 6.9 se refleja si Bncert fue útil en el caso de soporte, o si, por el contrario, no fue suficiente para resolver el problema principal. Se divide en las siguientes categorías:

- `Yes` (45.16 %, 14 casos): Se observa un correcto funcionamiento de Bncert.
- `Improvement` (41.94 %, 13 casos): Se han identificado algunas mejoras que se podrían realizar (pese al correcto funcionamiento general).

- `Bug` (12.90 %, 4 casos): Se ha encontrado problemas que han impedido el uso de la herramienta.

Los resultados obtenidos muestran que se ha logrado un uso extenso de la herramienta, cercano a la mayoría de casos de soporte sobre la configuración de HTTPS. Además, se han identificado mejoras que potencialmente podrían mejorar esta ratio.

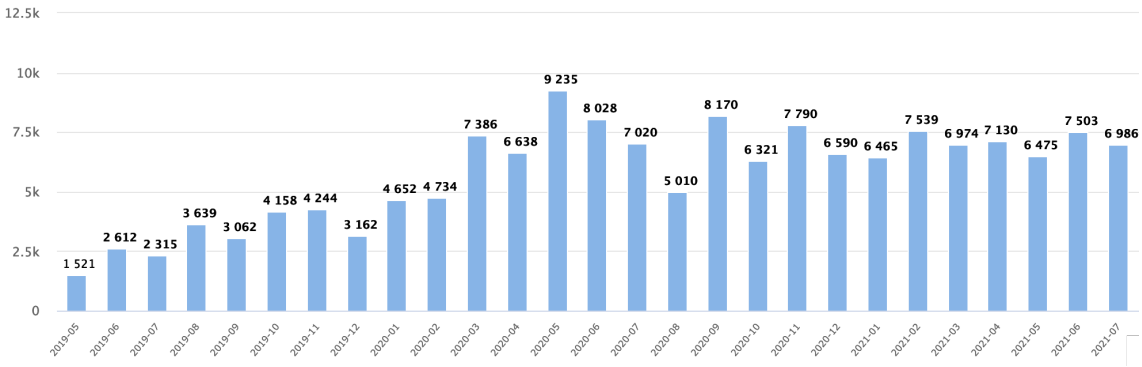


Figura 6.7 Cantidad de descargas de Bncert por mes.

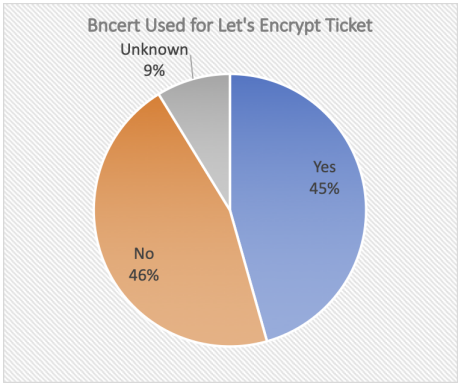


Figura 6.8 Uso de Bncert (2019).

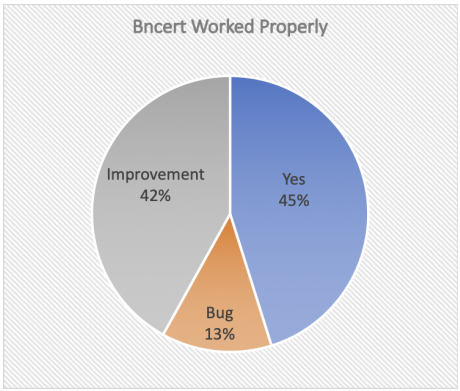


Figura 6.9 Funcionamiento correcto de Bncert (2019).

Evolución de los problemas principales encontrados

La Figura 6.11 recopila los principales problemas encontrados en los casos de configuración de HTTPS donde se hace uso de Bncert, donde las siguientes tres categorías incluyen más del 50 % de todos los casos:

- `Redirections` (23 %, 6 casos): Problemas tras ejecutar Bncert por funcionamiento incorrecto o no deseado de las redirecciones.
- `DNS` (19 %, 5 casos): Configuración de DNS o dominio incorrecto.

- `Automatic certificate renewal` (11%, 3 casos): Problemas relacionados con la renovación automatizada de un certificado.

Comparando con el año 2018 (Figura 6.10), sin Bncert, se puede observar un gran cambio, puesto que las siguientes categorías de problemas de usuario eran presentes en más del 85% de todos los casos de configuración de HTTPS:

- `Enabling certificates for Apache` (45%, 13 casos): Problemas relacionados con configurar un certificado en el servidor Web Apache.
- `Lego validation error` (24%, 7 casos): Problema de validación de Lego (habitualmente error de configuración DNS errónea, pero también pueden estar relacionados con errores tras alcanzar límites de Let's Encrypt).
- `generate-certificates.sh usage` (17%, 5 casos): Problemas de uso de la utilidad `generate-certificates.sh`.

Así, se puede ver cómo con Bncert ha desaparecido el primer problema, relacionado a activar certificados para el servidor Web Apache, pero ha aparecido la problemática de redirecciones, que en caso de solucionarse correctamente permitiría disminuir la cantidad de nuevos casos en una cuarta parte, aproximadamente. La categoría de errores de validación de Let's Encrypt ha sido intercambiada por errores de validación de DNS, que tienen relación entre sí (una configuración incorrecta de DNS causaría fallos en ambos casos), y ha notado una leve bajada.

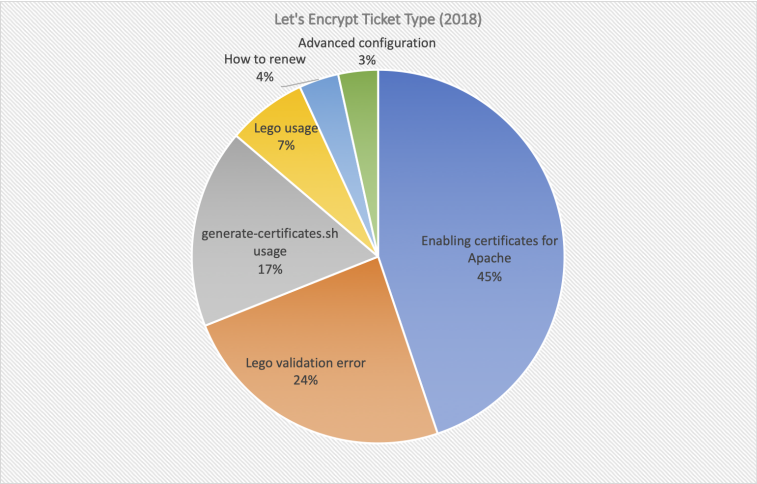


Figura 6.10 Estadísticas de la evolución de los problemas principales encontrados en los casos de configuración de HTTPS (2018).

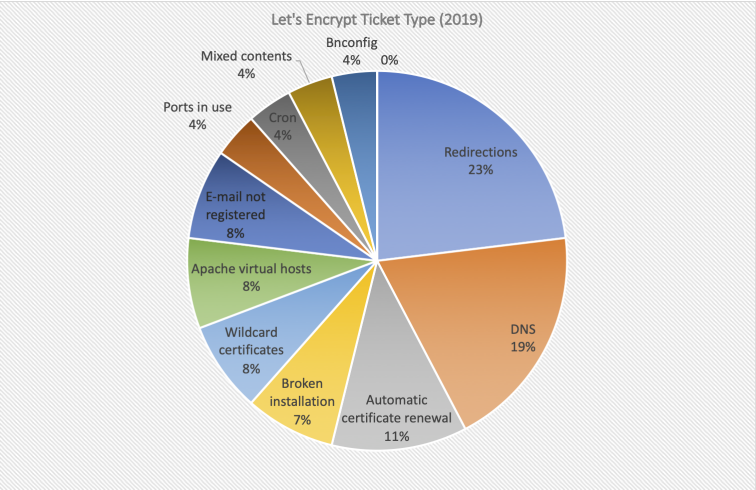


Figura 6.11 Estadísticas de la evolución de los problemas principales encontrados en los casos de configuración de HTTPS (2019).

Estimación del impacto de Bncert en cuanto a la disminución de casos

Con todos los resultados anteriores, se quiere comprender si la herramienta Bncert ha impactado en cuanto a la disminución de casos de soporte, que es el objetivo principal de este proyecto. Para ello, se partirá de los siguientes datos:

- Se hizo uso de Bncert en 26 casos de soporte, de un total de 57 relacionados a la configuración de HTTPS (Figura 6.8).
- Los problemas de DNS, que se incluían dentro de errores de validación de Let's Encrypt en 2018 (Figura 6.10), representan 7 de un total de 29 casos. En el análisis de 2019 (Figura 6.11) solamente los errores de DNS representaban 5 de un total de 26 casos específicos de Bncert. No se ha identificado ningún caso de DNS donde la herramienta no hubiese funcionado correctamente.
- Sumando los problemas de configuración de Apache (45 %) con los de validación de Let's Encrypt (24 %), muy relacionados con errores de validación de DNS, se obtiene que aproximadamente un 70 % de todos los casos de soporte del año 2018 habrían sido resueltos por Bncert.

Todo esto significa que solo un 30 % de los casos serían de nueva creación, y que por cada caso de Bncert habría una equivalencia de unos 3 nuevos, si no se hubiera publicado la herramienta. Ello implicaría que los 26 casos de soporte de WordPress creados entre septiembre y octubre del 2019, que hicieron uso de Bncert, pasarían a ser aproximadamente 78 con las nuevas tendencias.

Sumando los otros 31 casos que no hicieron uso de Bncert, se obtendría un total de 109 casos, un aumento aproximado del 90 % sobre la cantidad original de 57. Dicho de otra forma, Bncert habría permitido reducir un 50 % el número de nuevos casos de soporte de sobre configuración de HTTPS con certificados de Let's Encrypt.

Esta cifra sería aún mayor, puesto que aquellos usuarios para los que les funcionó correctamente no llegarían ni a crear un nuevo caso de soporte. Sin embargo, no se disponen de estos datos, por lo que se considerará el escenario más conservador.

6.2 Solución de fallos encontrados en Bncert

A continuación se describirán los principales problemas encontrados en Bncert, y una solución propuesta para ser implementada. La motivación de implementar esto sería reducir la cantidad de nuevos casos de soporte con problemas, que llegaron a hacer uso de Bncert.

6.2.1 Problemas encontrados

Problemas de redirecciones tras ejecutar Bncert

Algunos usuarios han reportado problemas de redirecciones que no funcionan correctamente tras ejecutar Bncert. En este caso, vamos a considerar los siguientes escenarios:

- Cambio de dominio en el servidor Web no reflejado en la configuración de la aplicación: En caso de activar una redirección permanente, se debería configurar la aplicación principal a usar ese dominio destino, para evitar problemas de bucles de redirección o redirección a un dominio incorrecto: El servidor redirige al dominio deseado, pero la aplicación Web está configurado para usar otro dominio. Para ello habrá que ejecutar la herramienta `Bnconfig` de Bitnami para cambiar el dominio principal.
- Redirección de una dirección IP a HTTPS. No se debería redireccionar una dirección IP a HTTPS, puesto que Let's Encrypt no soporta tal configuración.
- Redirección de una dirección IP tipo localhost a otro dominio. No se debería redireccionar una dirección IP tipo localhost a otro dominio, puesto que suelen ser usados para acceder a servicios ocultos (como por ejemplo phpMyAdmin o estadísticas del servidor Web).

Problemas para configurar de renovación automática de certificados

La renovación de certificados no se está configurado correctamente en los ficheros de configuración de Apache. Los problemas principales identificados son:

- Configuración que no se añade correctamente a Apache: Se ha detectado que en algunos tipos de instalación ni siquiera los llega a añadir, en otros lo añade mal (pudiendo romper la configuración de Apache), y en otros muchos casos añade contenido duplicado. Todo esto está causando que la renovación de certificados automatizada no llegue a funcionar, en cuyo caso al usuario le llega una notificación al final del proceso de ejecución de la herramienta.
- Configuración que no funciona pese a estar añadida a Apache: En algunas instalaciones de Bitnami, como de Bitnami Odoo Stack, se ha observado que pese a tener la configuración esperada no se llega a activar la configuración necesaria para la renovación de certificados automática. Se ha asociado estos fallos a problemas con la prioridad de directivas Apache tipo `ProxyPass`.

Usabilidad de la herramienta

Se han observado los siguientes problemas de usabilidad de la herramienta:

- Evitar añadir dominios tipo www (o no-www) automáticamente: En lugar de añadirlos automáticamente, que se ha visto que resulta confuso para los usuarios, se les preguntará en la página de introducción de dominios acerca de incluir aquellos no especificados por el usuario de forma automática, pero de manera opcional.
- Mostrar siempre la página de configuración de redirecciones: En el diseño original de la herramienta se había decidido suponer que un usuario siempre querría habilitar la redireccion de dominios no-www a www. Esto se podría configurar más adelante en una página opcional. A partir de ahora se configurará esta página para mostrarse siempre que se puedan habilitar redirecciones, y posterior a la página de introducción de dominios.
- Uso del modo texto por defecto: Algunos usuarios han reportado problemas al usar el modo interactivo con algunos entornos de interfaz gráfica de Linux. Para solucionarlo, se activará el modo texto por defecto, pero dejando a los usuarios la posibilidad de usar el modo gráfico especificando parámetro `--mode` al ejecutar la herramienta.

Picos de carga en los servidores de Let's Encrypt causados por Bncert

El 25 de junio del 2022, ingenieros de Let's Encrypt abrieron un tique de soporte [57] en el repositorio de máquinas virtuales de Bitnami[1], reportando que estaban sufriendo picos de carga en servidores de Let's Encrypt causado por soluciones de Bitnami. Los picos se producían a diario cada medianoche, y causaba errores de renovación que empeoraban el pico de la siguiente medianoche.

[1] Repositorio de soporte de máquinas virtuales de Bitnami en GitHub: https://github.com/bitnami/vms/

La investigación de su parte reveló que un 60 % del pico era provocado por Lego, lo que se puede observar en un tique de soporte que reportaron a los mantenedores de la utilidad [58], y tras inspeccionar varias direcciones IP asociadas al pico encontraron que la mayoría consistían en aplicaciones Web populares desplegadas con Bitnami.

A continuación, desplegaron una instancia para intentar reproducir el problema, y lo encontraron rápidamente: Para la renovación de los certificados con Bncert, se estaba creando una tarea periódica de Cron a diario a las 00:00 horas para renovar el certificado, en cada uno de los clientes. Con ello, cerraron la investigación y procedieron a reportar el problema a Bitnami.

Figura 6.12 Picos de peticiones observados en servidores de Let's Encrypt entre el 10 y el 15 de junio del 2022 (fuente: Jacob Hoffman-Andrews, ingeniero de Let's Encrypt) [57].

De los datos proporcionados por los ingenieros de Let's Encrypt podemos sacar la siguiente información:

- El 15 de julio del 2022, hubo más de 173 mil peticiones de renovación usando el cliente de Lego, más del 60 % del total. El segundo contribuyente fue de poco menos de 20 mil.
- El principal cliente de Let's Encrypt, usado a lo largo todo el día, es el oficialmente mantenido: CertBot.
- Lego se usa de forma masiva en muy pocas instalaciones: Bitnami y VMware Tanzu Community Edition. Aparte de estos, se usan de manera más discreta en proyectos de código abierto como Erda u OpenYurt.
- Gracias a los puntos anteriores, y sabiendo Bncert está diseñado para soportar un máximo de una renovación de certificados por cliente y día, podemos concluir la práctica mayoría de los 173.000 clientes son usuarios Bitnami que utilizaron la herramienta Bncert.

6.2.2 Implementación de la solución a los fallos identificados

La mayoría de fallos identificados en el punto anterior se solucionaron en la versión 0.5.0 de Bncert, publicada el 23 de octubre del 2019.[2] Tras la publicación de esta versión, no se han vuelto a recibir reportes de errores relacionados, entendiéndose así que los principales problemas han sido solucionados.

Los fallos que provocaron picos de carga en servidores de Let's Encrypt fueron solucionados en la versión 1.0.0 de la herramienta, que incluía las siguientes características nuevas:

- Adición de un campo de agente de usuario (o user agent) por cada petición de Let's Encrypt. Esto permite a Let's Encrypt identificar las peticiones causadas por nuevas soluciones de Bitnami.
- Renovar los dominios en tareas periódicas con hora y minutos aleatorios en el día, para evitar nuevos picos.
- Actualizar la versión de Lego a 4.8.0. Esta versión añade una espera de duración aleatoria para renovaciones de certificados para evitar los problemas de carga en una hora determinada, en entornos no interactivos (como por ejemplo Cron). Además, incluye soporte para el nuevo campo de agente de usuario que fue contribuido por ingenieros de Let's Encrypt.

[2] Nótese que la primera versión disponible fue la 0.1.0, y las sucesivas versiones se debieron a actualizaciones de la utilidad Lego.

Nótese que gracias al diseño de la herramienta, será posible solucionar estos problemas en instalaciones existentes de los usuarios. Esto es así gracias al sistema de auto-actualización para la versión de Bncert, el reemplazo automático de las entradas de Cron y el reemplazo del binario de Lego por el de la versión más reciente. Para obtener estas mejoras, es suficiente con que los usuarios vuelvan a ejecutar la herramienta en su instalación.

6.3 Resultados

De los anteriores puntos, se resumen las conclusiones obtenidas en los siguientes puntos:

- Ha habido un aumento muy importante de casos entre el 2018 y 2019, prácticamente del 50%. Esto se explica con el crecimiento orgánico del foro de Bitnami, y con la popularización de Let's Encrypt.
- La complejidad de los casos relacionados ha aumentado según los resultados de este análisis, indicando que los casos más sencillos han sido solucionados gracias a la herramienta.
- El principal problema identificado en el análisis de casos de soporte de 2018 (configuración de certificados para el servidor Web Apache) ha desaparecido prácticamente por completo.
- Los principales problemas identificados en el último análisis de casos de soporte fueron resueltos con éxito, y no se han recibido reportes de errores relacionados desde entonces.
- Se estima que la publicación de Bncert ha permitido reducir un 60% la cantidad de casos de soporte sobre la configuración de HTTPS. Contando con que se emplea una media de 15 minutos por caso de soporte de configuración de HTTPS, son 25 horas mensuales que se pueden dedicar a otras tareas, es decir, un ingeniero a jornada parcial.
- La herramienta está teniendo mucho uso, con una media de 7.000 descargas al mes y, a día de 2022, más de 170.000 usuarios activos.

Con ello, se determina que la solución implementada, Bncert, ha permitido reducir la frecuencia de nuevos casos de soporte relacionados a la configuración de HTTPS en un 60% aproximadamente, cumpliendo con el objetivo principal de este proyecto. Esto también implica que se ha tenido que emplear menos tiempo en soporte, y se observa de parte de los usuarios que han aceptado la solución, ambos puntos siendo objetivos secundarios.

7 Conclusiones y líneas de avance

7.1 Conclusiones

Este proyecto comenzó en Bitnami con la realización de un análisis de casos en el foro oficial de soporte, con el objetivo de encontrar posibles formas de reducir la carga de soporte por parte del equipo de ingeniería, además de mejorar la experiencia de los usuarios usando soluciones de Bitnami.

Se encontró que una parte importante de ellos estaban directamente relacionados con la configuración de HTTPS con Let's Encrypt, pese a la existencia de soluciones y documentación con el fin de resolver este mismo problema. Ello dio paso a un análisis de estas soluciones que permitió encontrar varias deficiencias en estas, y que tendría sentido re-implementarlas como una nueva herramienta de configuración de HTTPS para instalaciones de Bitnami, denominada Bncert.

Así, dio comienzo proceso para mejorar estas soluciones mediante un análisis de requisitos, implementación y pruebas, finalizando con la publicación de la herramienta y su inclusión en la mayoría de las máquinas virtuales de Bitnami para la nube.

Tres meses tras su publicación, se realizó un nuevo análisis de casos de soporte que encontró un aumento de la cantidad de casos de configuración de HTTPS con Let's Encrypt, que se asoció a una mayor popularización de Let's Encrypt. Esto dio lugar a solucionar los fallos más importantes e implementar las características más criticas, con vistas a mejorar la experiencia de los usuarios a corto plazo.

Finalmente, con estos cambios, se ha observado la validación de todo el trabajo realizado en este proyecto, por los siguientes motivos:

- La herramienta está teniendo muy buenos datos de uso. Datos internos muestran que tiene una media de 7.000 descargas al mes, y en el capítulo anterior se estimó que dispone actualmente de más de 170.000 usuarios activos, gracias a datos proporcionados por ingenieros de Let's Encrypt.
- Una estimación interna calcula que el uso de Bncert ha permitido reducir más de un 50 % la cantidad de nuevos casos de soporte sobre la configuración de HTTPS, cifras muy positivas que permiten notar el gran impacto que ha tenido. A efectos prácticos, esto supone una reducción de más de 100 casos de soporte al mes a día de 2022, reduciendo así más de 25 horas mensuales el tiempo necesario para dedicar a soporte, contando con el empleo de una media de 15 minutos por caso de soporte, que se pueden emplear en otras tareas.

Todo esto permite posicionar las soluciones de Bitnami en un mundo donde HTTPS es esencial para cualquier página Web, mejorando la experiencia de los usuarios a la vez que reduciendo la carga de trabajo del equipo de ingeniería.

7.2 Líneas de avance

Futuros análisis de casos de soporte

Como se ha venido realizando estos últimos años, se propone seguir con los análisis de casos de soporte en Bitnami, observando cambios de tendencia y estudiando los casos de configuración de HTTPS, para identificar puntos de mejora y mejorar la herramienta Bncert.

Soporte del servidor Web NGINX

Actualmente, Bncert solo soporta el servidor Web Apache, que es el mayoritario en instalaciones de Bitnami. Se viene observando un crecimiento de uso de aquellas con NGINX, en los cuales se debería poder hacer uso de esta herramienta.

Soporte de opciones avanzadas para la creación y renovación de certificados de Let's Encrypt

Let's Encrypt soporta distintos modos para la creación y renovación de certificados. En este proyecto se ha usado `TLS-ALPN-01` para la creación y `HTTP-01` para la renovación, pero existe también el modo `DNS-01` que permite renovar un certificado sin necesidad de parar servicios ni requerir modificaciones en la configuración del servidor Web. Así, sería de especial interés permitir a los usuarios seleccionar qué modos usar, permitiendo a usuarios aplicar configuraciones avanzadas con Bncert.

Configuración de HTTPS con certificados externos

Actualmente, la herramienta Bncert solo soporta creación o renovación de certificados de Let's Encrypt. Se propone extender su uso para permitir certificados externos, que no tengan por qué ser de Let's Encrypt.

Apéndice A
Análisis inicial

En este capítulo vamos a realizar un análisis inicial de casos de soporte para identificar las tendencias y los problemas más comunes.

Para ello, primero se establecerán las pautas a seguir para el análisis. Con el análisis se definirá la categorización y se incluirán los casos analizados.

Una vez concluido, se identificarán posibles herramientas de usuario a desarrollar, que permitan resolver los problemas principales.

A.1 Pautas

A.1.1 Ámbito

Con el fin de simplificar el análisis y reducir ruido, se reducirá el análisis a una única fuente de casos de soporte y de un solo producto.

Para que el análisis sea aplicable al resto del catálogo de Bitnami se deben dar dos sucesos:

- La fuente de casos de soporte debe ser la mayoritaria y abarcar un periodo extenso de tiempo.
- El producto escogido debe ser popular, y debe haber una proporcionalidad con en el número de casos sobre este. Así, si el escogido es popular, el análisis seguiría siendo aplicable para gran parte del catálogo de Bitnami.

La fuente escogida es Bitnami Community[1] y el producto Bitnami WordPress stack (que incluye la aplicación WordPress). Hay una serie de razones que indican que este es el producto adecuado para ello:

- WordPress es la aplicación que más casos de soporte recibe, como se observa en la Figura A.1.
- WordPress es la aplicación más popular del catálogo de aplicaciones ofrecidas Bitnami.
- Al igual que la mayoría del catálogo de aplicaciones de Bitnami, requiere Apache, PHP y MySQL.
- La configuración es muy sencilla, en comparación con otras aplicaciones.

[1] Ya no está en línea. Ubicación original: https://community.bitnami.com

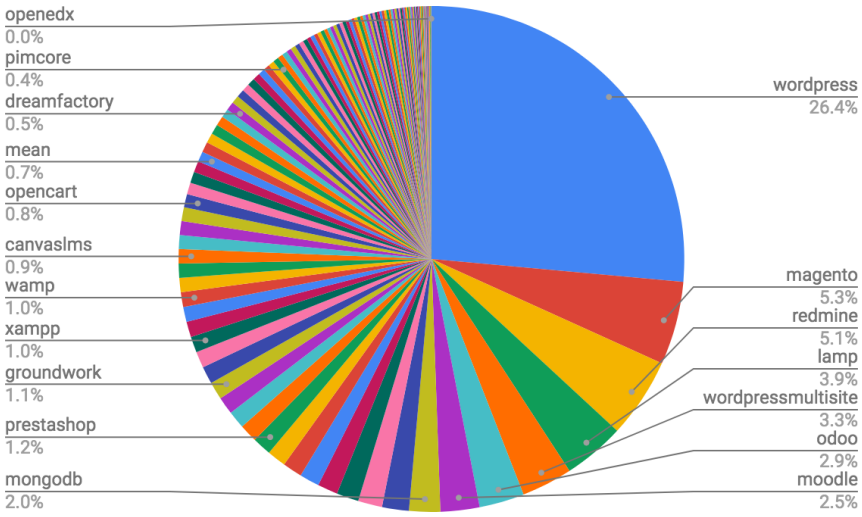


Figura A.1 Aplicaciones con mayor porcentaje de casos de soporte en Bitnami Community.

A.1.2 Parámetros

En el análisis de cada caso, se incluirán los siguientes datos:

- Fecha de creación del caso.
- El identificador del caso de soporte.[2]
- Título.
- Categorías aplicables.
- Sub-categoría (en caso de estar relacionado a configuración de HTTPS).
- Principal problema encontrado (en caso de estar relacionado a configuración de HTTPS).

A.1.3 Categorización

La lista de categorías identificadas en el análisis son:

- `Let's Encrypt`: Configuración de HTTPS con Let's Encrypt.
- `Other SSL certificate`: Configuración de HTTPS sin Let's Encrypt.
- `WordPress`: Específicos de la aplicación WordPress.
- `Plug-ins`: Específicos de extensiones de WordPress.
- `Redirections`: Configuración de redirecciones.
- `Apache configuration`: Configuración de Apache.
- `Performance`: Rendimiento.
- `PHP config/exts`: Configuración de PHP.
- `Domains & DNS`: Dominios y DNS.
- `Installer`: Específico del instalador de WordPress.
- `Backup/restore/migrate`: Copias de seguridad y migración de servidor.
- `CORS`: Contenido mezclado y errores CORS.
- `Database`: Específicos de la base de datos.

[2] El identificador del caso permite construir su URL. Por ejemplo, el caso de soporte con identificador 1234 se puede acceder desde la URL https://community.bitnami.com/t/1234. Se recomienda usar el Wayback Machine de archive.org para acceder a los enlaces.

- `PageSpeed`: Configuración de PageSpeed.
- `phpMyAdmin`: Acceso a phpMyAdmin.
- `Application URL prefix`: Configuración del prefijo de la URL de acceso a la aplicación.
- `Network`: Configuración de red.
- `Permissions`: Permisos.
- `Upgrades`: Actualizaciones.
- `Cache`: Configuración de caché.
- `Bitnami banner`: Logo de Bitnami y página de inicio rápido.
- `Credentials`: Credenciales.
- `FTP/SFTP`: Acceso vía FTP o SFTP.
- `Multi-tier`: Específicos de soluciones multi-nodo.
- `Security`: Configuraciones de seguridad.
- `SMTP`: Configuración de SMTP en WordPress.
- `Themes`: Estilos de WordPress.
- `Cron`: Configuración de tareas periódicas vía Cron.
- `Load balancer`: Configuración de balanceador de carga.
- `Old version`: Petición de versión antigua.
- `SSH`: Acceso vía SSH.
- `Miscellaneous`: Misceláneos.
- `Other`: Otros.
- `Custom application`: Aplicación propia (no WordPress).

A.2 Análisis

Se han analizado todos los casos de soporte creados en relación con WordPress creados entre septiembre y octubre del 2018, sumando más de 200 casos en total. Los resultados completos se muestran a continuación[3]:

[3] La URL del tique de soporte se puede construir de la siguiente manera: `https://community.bitnami.com/t/ID`, siendo `ID` el identificador del tique. Se recomienda usar el Wayback Machine de archive.org para acceder a los enlaces.

Fecha	ID tícket	Título	Grupo	Tipo (HTTPS)	Principal problema (HTTPS)
2018-09-01T00:37	60211	Problem Install VestaPanel or Webuzo in my VPS Debian 8 64bit	Miscellaneous	N/A	
2018-09-01T03:00	60213	Enable Keep-Alive Grade keeps on flickering. Is there any permanent	Performance Let's Encrypt	N/A	
2018-09-02T12:45	60234	Unable to make changes to plugin files	Permissions	N/A	
2018-09-02T18:12	60237	Can not edit theme with subdomain. Getting Blocked by security Cor	CORS Themes	N/A	
2018-09-02T22:03	60242	Issue valid SSL certificate for both non-www and www domain	Let's Encrypt	Creation	Lego usage
2018-09-03T08:22	60250	Problème d'installation de Ioncube Loader	Plug-ins PHP config/exts	N/A	
2018-09-03T16:09	60268	How can I list currently running modules in my stack?	Miscellaneous	N/A	
2018-09-03T23:12	60274	How to turn off Stackdrive monitoring	Miscellaneous	N/A	
2018-09-04T12:03	60281	Imagick enabled but not working on locally hosted wordpress site	PHP config/exts Plug-ins	N/A	
2018-09-05T04:49	60297	Cannot login to phpmyadmin	phpMyAdmin Credentials	N/A	
2018-09-05T15:14	60320	WordPress could not establish a secure connection to WordPress.org	Let's Encrypt Plug-ins	Creation	Enabling certificates for Apache
2018-09-05T19:46	60330	Cloned WordPress VM shows Apache2 Debian Default Page	Miscellaneous	N/A	
2018-09-06T14:25	60344	Restrict linux user to htdocs directory	FTP/SFTP Permissions	N/A	
2018-09-06T15:43	60345	I want to copy a file from parent theme to child theme	Themes	N/A	
2018-09-07T17:36	60365	Not able to complete instructions to install SSL certificate on LightSa	Let's Encrypt Permissions	Creation	Enabling certificates for Apache
2018-09-07T22:13	60374	Change the value of the max_input_vars	PHP config/exts	N/A	
2018-09-08T03:12	60376	The $cfg['TempDir'] (./tmp/) is not accessible	phpMyAdmin Permissions	N/A	
2018-09-09T01:02	60384	How to Select PHP version via PHPMYADMIN via Wordpress by BITN	Miscellaneous	N/A	
2018-09-09T03:58	60385	Cant access phpmyadmin for amazon AWS (behind load balance) via	phpMyAdmin	N/A	
2018-09-09T20:24	60393	The $cfg['TempDir'] (./tmp/)is not accessible.phpMyAdmin is not abl	phpMyAdmin Permissions	N/A	
2018-09-09T22:35	60397	After installing NGINX Amplify, Phpmyadmin not working with 404 e	Plug-ins	N/A	
2018-09-10T05:09	60404	Bitnami and WampServer	Miscellaneous	N/A	
2018-09-10T16:45	60422	Google Cloud SQL and MySQL	Database	N/A	
2018-09-10T17:08	60423	Lets Encrypt Expired	Let's Encrypt	Renewal	Automatic certificate renewal
2018-09-10T22:00	60427	Error when trying to install ioncube loaders on google cloud	PHP config/exts	N/A	
2018-09-11T00:16	60429	Website not responding and took too long to respond, high CPU usag	Performance	N/A	
2018-09-11T05:09	60431	My banners aren't getting displayed	Miscellaneous	N/A	
2018-09-11T11:16	60439	WordPress URL gives Internal server error HTTP 500	Custom application	N/A	
2018-09-11T14:49	60444	Site is Crashing After WP Update 4.9.8	WordPress	N/A	
2018-09-11T19:28	60448	Import / Export MariaDB Databases on Bitnami WordPress Multi-tie	Multi-tier Backup/restore/migrate	N/A	
2018-09-11T21:21	60453	Enabling WordPress Multisite causes wp-admin to redirect to 127.0.(	WordPress	N/A	
2018-09-12T23:19	60477	Non-www to www with https AWS Lightsail wordpress help	Redirections	N/A	
2018-09-13T01:35	60482	Missing Headers	CORS	N/A	
2018-09-13T03:41	60484	Httpd could not be started after modifying htaccess.conf	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-13T08:10	60487	2002 Code Error When Trying Import / Export MariaDB Databases ir	Multi-tier Backup/restore/migrate	N/A	
2018-09-13T15:50	60506	Unstable Wordpress website based on AWS Bitnami Instance - 403 F	Domains & DNS	N/A	
2018-09-13T16:31	60509	How To Connect A Domain To A Bitnami Google Cloud Platform Wor	Domains & DNS	N/A	
2018-09-13T21:22	60516	Website downloads as Gzip file after adding W3 Cache rewrites to ht	Plug-ins Apache configuration	N/A	
2018-09-13T23:21	60519	Redirect to https://www	Redirections	N/A	
2018-09-14T04:08	60524	My domain showing too many redirects	Redirections	N/A	
2018-09-14T06:09	60528	Bitnami not installing on Xampp windows 7, Problem running post-in	Installer	N/A	
2018-09-14T12:11	60538	Cannot connect to the site via sFTP / ssh and after change woocomm	WordPress Domains & DNS	N/A	
2018-09-14T16:42	60545	Increase Memory Limit	PHP config/exts	N/A	
2018-09-14T22:58	60555	Move Bitnami Stack to other Computer?	Backup/restore/migrate	N/A	
2018-09-15T12:20	60567	Unable to load phpMyAdmin via SSH tunnel	Backup/restore/migrate	N/A	
2018-09-15T15:34	60572	Redirect from mydomain.com/tools to subdomain.mydomain.com/t	Redirections	N/A	
2018-09-15T15:43	60573	Let's Encrypt SSL cert install problem	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-15T21:20	60578	I would like to set up dev.mydomain.com for wordpress developmen	Miscellaneous	N/A	
2018-09-16T12:44	60589	Setting up API access to WordPress on AWS EC2 instance	Plug-ins Apache configuration	N/A	
2018-09-16T17:26	60593	Leverage browser from Cache	Apache configuration	N/A	
2018-09-17T04:39	60604	Minimize Redirects remove the redirect chain if possible	Redirections	N/A	
2018-09-17T06:01	60608	Two wordpress instances, second one redirects to foo.com/foo	Miscellaneous	N/A	
2018-09-17T08:27	60613	Redirection not working properly	Redirections	N/A	
2018-09-17T12:28	60623	W3 Total Cache Error, can't find the solution anywhere	Permissions Plug-ins	N/A	
2018-09-17T16:11	60628	Unable to start Apache (Apache config test fails, aborting), Site Dow	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-18T06:38	60637	Message : The requested URL was not found on this server	WordPress	N/A	
2018-09-18T07:46	60639	Install and configure VSFTP on AWS Bitnami Wordpress Stack	FTP/SFTP	N/A	
2018-09-18T16:03	60655	Bitnami + EC2 AWS - JS Browser Caching Issue	Performance	N/A	
2018-09-18T16:09	60656	Cron job specified for root does not run	Cron	N/A	
2018-09-18T17:02	60658	AWS Bitnami WordPress SSL	Let's Encrypt	Creation	Lego validation error
2018-09-18T18:46	60662	Error message on Wordpress: Can't connect to AWS! Check your cre	Plug-ins	N/A	

2018-09-18T23:52	60664	Error Failed to start Raise network interfaces	Network	N/A	
2018-09-19T02:09	60669	I am using Google Cloud with bitname and I was trying to clean cach	WordPress	N/A	
2018-09-19T10:54	60683	Sudo /opt/bitnami/ctlscript.sh start fails following SSL set up	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-19T14:05	60694	How to upgrade to the latest version of Bitnami?	Upgrades Security	N/A	
2018-09-19T14:14	60696	Loading error on website - Message: ERR_CONNECTION_RESET on C	Performance	N/A	
2018-09-19T14:20	60698	[ssl] error in the bitnami wiki causing the google cloud VM to crush	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-19T17:11	60701	How to find the domain root directory on bitnami wordpress on Ama	Apache configuration	N/A	
2018-09-19T21:02	60703	Pagespeed module problem with image	PageSpeed	N/A	
2018-09-20T05:37	60707	AWS Bitnami instance not launching server after update	Miscellaneous	N/A	
2018-09-20T07:38	60711	Several security vulnerabilities: SegmentSmack, L1 Terminal Fault an	Security Upgrades	N/A	
2018-09-20T07:50	60712	Could not start Apache	Apache configuration	N/A	
2018-09-20T09:59	41571	“server reached MaxRequestWorkers” error on AWS	Performance	N/A	
2018-09-20T10:17	60717	Removing WordPress Multisite Bitnami Banner on sub domains (not	Bitnami banner	N/A	
2018-09-20T19:59	60726	Css changes made to theme take too long to load	Themes	N/A	
2018-09-21T09:32	60736	Could not obtain certificates	Let's Encrypt	Creation	Lego validation error
2018-09-21T11:08	60740	Wordpress Event plugin to display based on Tabs	WordPress	N/A	
2018-09-21T15:51	60743	Patch the operating system	Security	N/A	
2018-09-21T18:58	60746	Error 500 on AWS LAMP Wordpress installation	Plug-ins	N/A	
2018-09-22T06:40	60756	Unable to retrieve new password on wordpress	SMTP	N/A	
2018-09-22T11:15	60759	Enable WordPress Multisite for the WP + NGINX + SSL stack	WordPress	N/A	
2018-09-22T16:54	60765	Amazon Lightsail WordPress: Redirect HTTPS to HTTP	Redirections	N/A	
2018-09-23T09:24	60773	Possibility to connecto to Wordpress Bitnami VM outside of the netw	Network	N/A	
2018-09-23T09:38	60775	Google maps API error for wordpress website hosted in AWS using E(	CORS	N/A	
2018-09-23T17:12	60782	/var/www/html/index.html is gone after stopping AWS machine	Miscellaneous	N/A	
2018-09-23T20:19	60785	AWS to Bitnami Cloud Migration - Wordpress Site Down?	Backup/restore/migrate	N/A	
2018-09-24T04:55	60792	AWS Wordpress Bitnami Stack: mod_pagespeed filters dont appear f	PageSpeed	N/A	
2018-09-24T10:06	60795	Site cannot be reached after generating new certificates	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-24T12:40	60798	Cannot obtain SSL certificates	Let's Encrypt	Creation	Lego validation error
2018-09-24T14:02	60801	Want to migrate bitnami wordpress theme to live wordpress site (He	Backup/restore/migrate Themes	N/A	
2018-09-25T06:20	60821	Issue with Vhost in Google cloud Vm instance	Custom application Apache configuration	N/A	
2018-09-25T14:28	60833	Website Server down multiple time	Performance	N/A	
2018-09-26T05:59	60858	WordPress cache problem	Cache Plug-ins	N/A	
2018-09-26T06:23	60859	Installing Let's Encypt certificate - chown: cannot dereference '/opt/	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-26T09:10	60862	Trying to change the favicon from bitnami's to my custom	Apache configuration	N/A	
2018-09-26T16:02	60875	I need help for my bitnami wordpress instance hosted on aws	Performance	N/A	
2018-09-26T16:29	60878	Special character rewrites to htaccess.conf file cause 500 error	Apache configuration	N/A	
2018-09-26T18:23	60884	Bitnami WordPress AWS redirect IP to Domain insecure issue in edge	Redirections	N/A	
2018-09-28T16:40	60931	PLEASE HELP! Wordpress on Google Cloud. Images over 1mb not upl	WordPress	N/A	
2018-09-29T06:26	60938	Varnish Resource problem.(Eating up-to 99% of CPU)	Performance	N/A	
2018-09-30T10:26	60956	Made mistake for Bitnami AWS wordpress LetsEncrypt, site down no	Let's Encrypt	Creation	Enabling certificates for Apache
2018-09-30T11:57	60957	Bitnami Wordpress Multisite GCP: self-signed certificates - where to	Let's Encrypt Domains & DNS	Creation	Lego validation error
2018-10-01T07:05	60969	Unable leverage Browser Caching on AWS Bitnami stack (Apache) th	Cache	N/A	
2018-10-01T12:14	60981	Old version of the WordPress installer for macOS 10.11	Old version	N/A	
2018-10-02T21:13	61032	Errors on EC2 Wordpress	Plug-ins	N/A	
2018-10-02T23:18	61037	Important Notification Regarding Your AWS Marketplace Subscriptio	Upgrades Security	N/A	
2018-10-03T07:47	61045	Problems with my ssl certificate	Other SSL certificate	N/A	
2018-10-03T12:10	61059	AWS Load Balancer Health Check Fails	Load balancer	N/A	
2018-10-04T08:11	61094	Problem with installing a Let's Encrypt SSL Certificate	Let's Encrypt	Creation	Enabling certificates for Apache
2018-10-04T09:30	61098	Client denied by server configuration: /opt/bitnami/apps/phpmyadm	phpMyAdmin	N/A	
2018-10-04T14:48	61109	Upgrade site to SSL	Let's Encrypt	Creation	Lego validation error
2018-10-04T20:21	61116	Trying to enable HTTPS has broken my site, now apache won't start	Let's Encrypt	Creation	Enabling certificates for Apache
2018-10-04T20:43	61117	WordPress Multisite Domain Mapping - native or plugin?	WordPress	N/A	
2018-10-05T07:19	61124	Not able access webpage	Plug-ins	N/A	
2018-10-05T12:55	61143	Different domains for different wordpress modules on Lamp Stack	Domains & DNS	N/A	
2018-10-06T06:39	61161	Unable to rewrite wp-config for W3 Total Cache	Plug-ins	N/A	
2018-10-06T12:35	61167	Ssh connection failed	SSH	N/A	
2018-10-06T22:03	61175	Localhost WordPress All Pages Not Loading	WordPress	N/A	
2018-10-07T08:33	61178	Error creating new order (domain)	Let's Encrypt	Creation	Lego validation error
2018-10-07T11:18	61181	Redirect loop after changing database	Redirections	N/A	
2018-10-07T11:34	61184	Letsncrypt path not found	Let's Encrypt	Creation	generate-certificates.sh usage
2018-10-07T19:32	61196	Adding additional wordpress app	Miscellaneous	N/A	
2018-10-07T20:52	61198	Bad Request for Wordpress SSL	Plug-ins	N/A	
2018-10-08T07:10	61203	Wordpress xml doc importing	WordPress	N/A	
2018-10-08T10:43	61212	Https support to my instance hosted on aws	Let's Encrypt	Creation	generate-certificates.sh usage
2018-10-08T10:53	61214	ACM SSL certificate not working on Bitnami Wordpress site hosted o	Let's Encrypt	Creation	Advanced configuration
2018-10-08T16:05	61225	A record without IP	Domains & DNS	N/A	
2018-10-08T16:47	61227	I've increased the memory limit to 8GB and continues Fatal error: Al	PHP config/exts	N/A	
2018-10-08T18:33	61228	413 error while upload wp theme i already change maximum upload	PHP config/exts	N/A	
2018-10-08T18:38	61231	(413 large file nginx) error while upload wordpress theme step by ste	PHP config/exts	N/A	
2018-10-08T19:32	61234	I don't find the scripts to generate my SSL certificates at my deploy v	Let's Encrypt	Creation	generate-certificates.sh usage
2018-10-08T20:30	61236	Website loading very slow	Performance	N/A	
2018-10-08T23:00	61237	Apache [pagespeed:error] Failed to make directory: Permission deni	PageSpeed Permissions	N/A	

2018-10-09T02:12	61239	ERR_CONNECTION_REFUSED on fresh Install on VirtualBox	Network	N/A	
2018-10-09T07:22	61243	Issue with CDN set up	Domains & DNS	N/A	
2018-10-09T16:28	61275	How to convert Bitnami Wordpress on AWS to Wordpress Multisite	WordPress	N/A	
2018-10-10T00:41	61285	HOW-TO: Migrating from Let's Encrypt to Cloudflare Origin certificat	Other SSL certificate	N/A	
2018-10-10T09:14	61302	Changing Domain Name Cause Error	Domains & DNS	N/A	
2018-10-10T14:37	61319	Moving upload files	WordPress	N/A	
2018-10-10T21:27	61332	Change directory wordpress	Application URL prefix	N/A	
2018-10-11T19:06	61347	Vanilla Lightsail / Let's Encrypt Chaos	Let's Encrypt	Creation	Enabling certificates for Apache
2018-10-12T13:36	61369	(Xampp + Wordpress) Change URL to domain	Application URL prefix Domains & DNS	N/A	
2018-10-12T18:30	61372	AWS WP Images are not loaded	CORS	N/A	
2018-10-13T12:43	61385	Add a second virtual host to bitnami wordpress apache configuratior	Apache configuration	N/A	
2018-10-15T06:13	61395	Redirecting all http/https://www.domain.com requests to https://d	Redirections	N/A	
2018-10-15T06:38	61398	Wordpress pages - cant edit after using Duplicator to back up site	Plug-ins	N/A	
2018-10-15T12:04	61410	I need help PLEASE	Apache configuration	N/A	
2018-10-15T12:44	61413	No Letsencrypt folder and script	Let's Encrypt	Creation	generate-certificates.sh usage
2018-10-15T13:13	61416	Moodle and Wordpress MS Active Directory Integration	WordPress	N/A	
2018-10-15T13:41	61418	Problem accessing wp-admin after changing url and modifying php.ir	WordPress	N/A	
2018-10-15T21:42	61432	Cannot login to AWS Lightsail/Bitnami Wordpress Instance (Linux)	Credentials	N/A	
2018-10-16T01:15	61437	Public_html in Google Cloud (GCE)	Apache configuration	N/A	
2018-10-16T01:41	61438	Error UID of script /home/httpd/html/index.php is smaller than min_	Apache configuration	N/A	
2018-10-16T06:21	40159	Create CSR in ec2 wordpress	Other SSL certificate	N/A	
2018-10-16T08:21	61454	I am generating REST API to integrate with shipping solution(an onli	Plug-ins	N/A	
2018-10-16T12:42	61464	MySql shut down it self periodically	Database	N/A	
2018-10-16T15:18	61468	How to remove a bitnami user?	Miscellaneous	N/A	
2018-10-16T22:30	61473	Rewrite rule in bitnami.conf	Redirections	N/A	
2018-10-17T00:43	61475	Bitnami: How Do I Start Again?	Installer	N/A	
2018-10-17T04:46	61479	8d865e96-dbde-350e-11b5-48b707827105 My site cannot be reache	Apache configuration	N/A	
2018-10-17T12:18	61495	Mysql keeps crashing; cannot restart	Database	N/A	
2018-10-17T12:42	61497	Remove Bitnami banner. Still shows on Apple Ipad and IPhone	Bitnami banner	N/A	
2018-10-17T13:18	61500	Syntax error on line 1 of /opt/bitnami/apps/wordpress/conf/htaccess	Apache configuration	N/A	
2018-10-17T23:07	61515	The proper path to require php files	PHP config/exts	N/A	
2018-10-18T02:20	61520	Unable to start app on Mac	Installer	N/A	
2018-10-18T15:29	61538	EC2 Instance Reboots - Stuck on Booting from Hard Disk	Performance	N/A	
2018-10-18T18:11	61543	Deleted the back up of S3 and I don't see my site data	Plug-ins	N/A	
2018-10-19T02:44	61547	Wordpress installed as root gets apache 403 forbidden access	Apache configuration	N/A	
2018-10-19T09:17	61556	Can't find my WordPress home page	Apache configuration	N/A	
2018-10-19T17:35	61573	I cant find the pagespeed module	PageSpeed	N/A	
2018-10-19T23:53	61575	Can't add new plugins in child site of WP multisite	WordPress	N/A	
2018-10-20T06:19	61579	Home Page link set to IP address	WordPress	N/A	
2018-10-20T10:56	61585	Apache starting problem	Apache configuration	N/A	
2018-10-20T10:56	61586	Amazon-Lightsail Wordpress instance	Miscellaneous	N/A	
2018-10-20T15:35	61590	AWS / Wordpress Install - Cannot Connect to MySQL via Sequel Pro a	Database	N/A	
2018-10-20T23:24	61595	FrontCloud cause domain name problem, only show IP address	Apache configuration Domains & DNS	N/A	
2018-10-21T06:47	61607	Install FFMPEG-PHP	Miscellaneous	N/A	
2018-10-21T17:51	61612	Errors while installing Wordpress. Please Help!	Installer	N/A	
2018-10-22T16:15	61636	Redirect https://example.com to https://www.example	Redirections	N/A	
2018-10-22T18:54	61642	Server won´t start anymore. Please help,	Installer	N/A	
2018-10-23T08:05	61657	How to do force https? (Step by step)	Redirections	N/A	
2018-10-23T15:53	61674	An error occurred while updating (APPLICATION NAME HERE): Down	Upgrades	N/A	
2018-10-23T18:31	61687	AWS Lightsail / WP initial login doesn't work	Credentials	N/A	
2018-10-23T21:25	61694	Download fresh install (need wp-config.php)?	Installer	N/A	
2018-10-23T22:24	61695	Install Mailserver on Wordpress	SMTP	N/A	
2018-10-24T07:06	61704	'DNS_PROBE_FINISHED_NXDOMAIN' Error. The webpage is not ava	Domains & DNS	N/A	
2018-10-24T11:44	61720	HTTP ERROR 5OO after updating woocommerce	Plug-ins	N/A	
2018-10-24T14:30	61725	Plugins will not activate: fatal error	Plug-ins	N/A	
2018-10-24T14:31	61726	Not able to create SSL certificate	Let's Encrypt	Creation	Lego validation error
2018-10-24T18:53	61735	Website wont load!	Performance	N/A	
2018-10-24T22:42	61737	How do i install an SSL from 1and 1 to my wordpress running on azur	Other SSL certificate	N/A	
2018-10-25T06:14	61744	Apache Redirection - https://serveripaddress --> https://domain.com	Redirections	N/A	
2018-10-25T06:19	61746	Error Log Stopped Working (after I deleted it)	Apache configuration	N/A	
2018-10-25T15:12	61768	Wordpress Single Tier Doubts	Miscellaneous	N/A	
2018-10-25T18:06	61773	How to block access IP	Redirections	N/A	
2018-10-25T19:30	61774	Getting a 403 Forbidden Error on all images on website	Permissions	N/A	
2018-10-25T19:45	61775	FcgidIOTimeout setting WP All Import Plugin	Plug-ins	N/A	
2018-10-26T06:53	61783	Single user sign on to multiple bitnami apps on AWS	WordPress	N/A	
2018-10-27T22:56	61811	Wordpress Plugin Update / Delete Error Google Cloud	WordPress	N/A	
2018-10-28T00:01	61813	WP Super Cache Issue on AWS Bitnami Stack	Plug-ins	N/A	
2018-10-28T00:19	61814	Problem comand / Stop / Reboot Webim	Miscellaneous	N/A	
2018-10-28T21:30	61832	Installation prompts for folder that contains an installation of Bitnam	Installer	N/A	
2018-10-29T01:55	61837	Auto-configure Let's Encrypt certificate error: Error reading file /opt	Let's Encrypt	Creation	generate-certificates.sh usage
2018-10-29T09:06	61843	My website on Wordpress Multisite (bitnami) using SSL and CloudFro	Other SSL certificate Domains & DNS	N/A	
2018-10-29T16:08	61855	Website showing as insecure even after the certificate has been issu	Other SSL certificate	N/A	
2018-10-29T19:50	61865	Redirect 301 isn't working on server	Redirections	N/A	
2018-10-29T23:06	61868	How to set the upload limit to unlimited	PHP config/exts	N/A	
2018-10-30T01:18	61870	No image capchat	Plug-ins	N/A	
2018-10-30T12:13	61878	CSS, JS and other scripts not loading when Wordpress is moved to a d	Application URL prefix	N/A	
2018-10-30T13:46	61880	IP to domain redirect?	Redirections	N/A	
2018-10-30T15:48	61882	Add www domain to ssl after already having added non-www	Let's Encrypt	Creation	Lego usage

A.2.1 Resultados

Las siguientes categorías son aquellas que han tenido más cantidad de casos, como se observa en la Figura A.2:

- Let's Encrypt: 13.74 %.
- WordPress: 9 %.
- Plug-ins: 8.53 %.
- Redirección: 8.06 %.
- Misceláneos: 8.06 %.
- Configuración de Apache: 7.58 %.

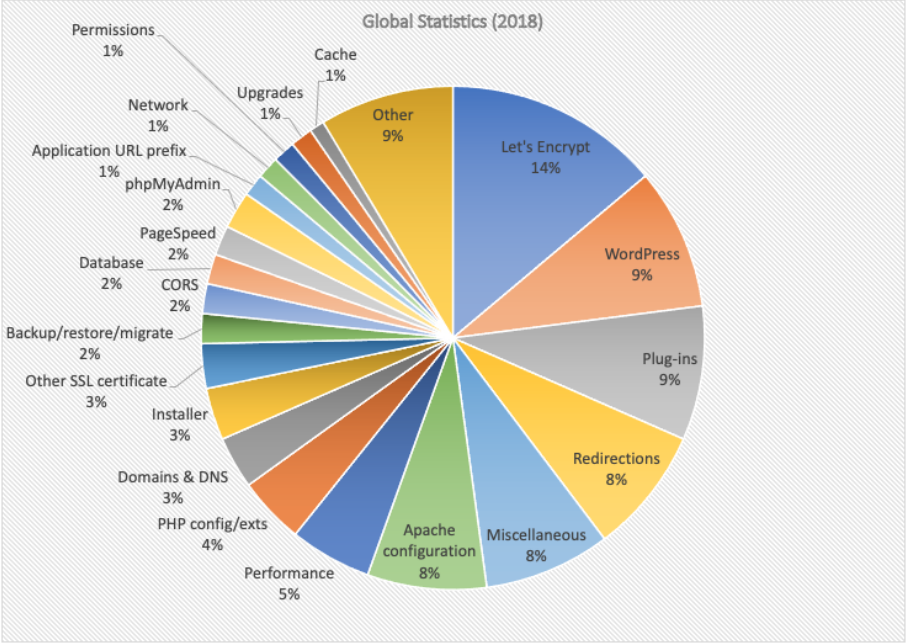


Figura A.2 Categorías con mayor porcentaje de casos de soporte en Bitnami Community.

A.3 Conclusión

Con los resultados del análisis, se observa que la configuración del servidor web (por ejemplo, Apache) es uno de los grandes obstáculos que encuentran los usuarios al usar soluciones de Bitnami, en este caso los más inexpertos.

Hay que destacar los casos de configuración del servidor web para activar HTTPS, lo cual requiere crear, configurar y mantener un certificado SSL válido. Esto agrupa más del 20 % de todos los casos, y se lista una serie de motivos a continuación:

- El usuario debe tener configurado un dominio válido, apuntando a la dirección IP donde será accesible el producto. Esto es necesario para el habitual proceso de verificación previo a la creación de certificados con Let's Encrypt, el único servicio actualmente gratuito y soportado en todos los navegadores Web populares.
- Los cambios DNS normalmente suelen tardar mucho tiempo en propagarse, pudiendo llegar a tardar hasta 48 horas, según el proveedor de dominios.
- Los certificados SSL tienen fecha de expiración (normalmente entre 3 meses y un año), y obliga al usuario a renovarlos. Este proceso suele ser manual, aunque Let's Encrypt recomienda automatizar este proceso.

- Y lo más destacable, Let’s Encrypt cuenta con restricciones y límites para dominios y usuarios. Esto puede provocar errores en la instalación de la solución.

Apéndice B
Desglose del análisis final

En este capítulo vamos a incluir el desglose del análisis final de casos de soporte para identificar los cambios de tendencias respectos al primer análisis. La metodología empleada está descrita en el Capítulo 6 Análisis de resultados.

B.1 Parámetros

En el análisis de cada caso, se incluirán los siguientes datos:

- Fecha de creación del caso.
- El identificador del caso de soporte.[1]
- Título.
- Categorías aplicables.
- Sub-categoría (en caso de estar relacionado con configuración de HTTPS).
- Principal problema encontrado (en caso de estar relacionado con configuración de HTTPS).

B.2 Categorización

La lista de categorías identificadas en el análisis son:

- `Let's Encrypt`: Configuración de HTTPS con Let's Encrypt.
- `Other SSL certificate`: Configuración de HTTPS sin Let's Encrypt.
- `WordPress`: Específicos de la aplicación WordPress.
- `Plug-ins`: Específicos de extensiones de WordPress.
- `Redirections`: Configuración de redirecciones.
- `Apache configuration`: Configuración de Apache.
- `Performance`: Rendimiento.
- `PHP config/exts`: Configuración de PHP.
- `Domains & DNS`: Dominios y DNS.
- `Installer`: Específico del instalador de WordPress.
- `Backup/restore/migrate`: Copias de seguridad y migración de servidor.
- `CORS`: Contenido mezclado y errores CORS.

[1] El identificador del caso permite construir su URL. Por ejemplo, el caso de soporte con identificador 1234 se puede acceder desde la URL https://community.bitnami.com/t/1234. Se recomienda usar el Wayback Machine de archive.org para acceder a los enlaces.

- `Database`: Específicos de la base de datos.
- `PageSpeed`: Configuración de PageSpeed.
- `phpMyAdmin`: Acceso a phpMyAdmin.
- `Application URL prefix`: Configuración del prefijo de la URL de acceso a la aplicación.
- `Network`: Configuración de red.
- `Permissions`: Permisos.
- `Upgrades`: Actualizaciones.
- `Cache`: Configuración de caché.
- `Bitnami banner`: Logo de Bitnami y página de inicio rápido.
- `Credentials`: Credenciales.
- `FTP/SFTP`: Acceso vía FTP o SFTP.
- `Multi-tier`: Específicos de soluciones multi-nodo.
- `Security`: Configuraciones de seguridad.
- `SMTP`: Configuración de SMTP en WordPress.
- `Themes`: Estilos de WordPress.
- `Cron`: Configuración de tareas periódicas vía Cron.
- `Load balancer`: Configuración de balanceador de carga.
- `Old version`: Petición de versión antigua.
- `SSH`: Acceso vía SSH.
- `Miscellaneous`: Misceláneos.
- `Other`: Otros.
- `Custom application`: Aplicación propia (no WordPress).

B.3 Análisis

Se han analizado todos los casos de soporte creados en relación con WordPress creados entre septiembre y octubre del 2019, sumando más de 300 casos en total. Los resultados completos se muestran a continuación[2]:

[2] La URL del tique de soporte se puede construir de la siguiente manera: `https://community.bitnami.com/t/ID`, siendo `ID` el identificador del tique. Se recomienda usar el Wayback Machine de archive.org para acceder a los enlaces.

Fecha	ID	Título	Categoría	Tipo	Usó Bncert	Funcionó?	Acción
2019-09-01T19:51	70771	What do these security logs mean?	Plug-ins	N/A	N/A	N/A	
2019-09-02T09:05	70775	DNS record removed, IP address now throws DNS_PROBE_FINISHED	Domains & DNS	N/A	N/A	N/A	
2019-09-02T12:38	70778	Page Migration: AWS EC2 - Upload folder is not writable. Export and	Permissions	N/A	N/A	N/A	
2019-09-02T12:51	70779	Ssh connexion to EC2 Bitnani Wordpress on AWS Marketplacen not re	SSH	N/A	N/A	N/A	
2019-09-02T18:45	70784	Lightsail - Bitnami Wordpress - Renewed Let's Encrypt Certificate but	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-09-02T23:00	70785	Can't install wordpress 5.2.2-3 on Mac OS	Installer	N/A	N/A	N/A	
2019-09-03T00:24	70787	How Can I Reinstall Wordpress without starting from scratch?	Miscellaneous	N/A	N/A	N/A	
2019-09-03T05:46	70790	Error establishing a database connection wordress bitnami google clo	Database	N/A	N/A	N/A	
2019-09-03T15:26	70793	Why ip address is displayed with www like https://www.xx.xx.xxx.xxx	Let's Encrypt Redirections	Redirection	Yes	Bug	Don't redirect IP addresses
2019-09-03T23:28	70799	Changed Primary Site per Documentation, how to enable HTTPS?	Redirections	N/A	N/A	N/A	
2019-09-04T06:22	39323	WP Multisite AWS Stack - Redirect Loop Error (After changing subdor	Application URL Prefix	N/A	N/A	N/A	
2019-09-04T06:24	70803	My site starts and stops within one-minute loading	Performance	N/A	N/A	N/A	
2019-09-04T08:11	70805	32-bit Virtual Machines for Bitnami WordPress Stack	Installer	N/A	N/A	N/A	
2019-09-04T11:58	70809	Menu vertically not centred	WordPress	N/A	N/A	N/A	
2019-09-04T13:36	70810	Error Establishing Database Connection. Wp-Config info correct, and	Database	N/A	N/A	N/A	
2019-09-04T15:33	70812	This site can't be reached - refused to connect	Domains & DNS	N/A	N/A	N/A	
2019-09-04T17:18	70814	Theme caused wp-admin issue,Also how to meet theme requirement	Themes	N/A	N/A	N/A	
2019-09-04T22:52	70816	WordPress and OwnCloud instances on same VM	Installer	N/A	N/A	N/A	
2019-09-05T03:21	70818	Wordpress site crashed after let's encrypt installation	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-05T09:23	70822	I want to path for root directory and index.html location AWS EC2 ins	Apache configuration	N/A	N/A	N/A	
2019-09-05T09:30	70823	Trying to install letsencrypt certificate but shows resolving to differer	Let's Encrypt Domains & DNS	Creation	Yes	Yes	None
2019-09-05T09:51	70824	Extremely high page loading times with 50 users	Performance	N/A	N/A	N/A	
2019-09-05T13:01	70826	Couldn't open site page after ssl auto-configuration	Let's Encrypt Cache	Creation	Yes	Improvement	Document? Message in the tool to refresh?
2019-09-05T13:02	70827	Multiple wordpress instalations with bitnami	WordPress	N/A	N/A	N/A	
2019-09-05T15:43	70830	Configuring virtual hosts for three websites on the same IP under Var	Let's Encrypt	Renewal	Yes	Improvement	Support vhosts
2019-09-05T16:08	70831	Data re-write occurring in wp-config.php and MySQL tables	Domains & DNS	N/A	N/A	N/A	
2019-09-05T17:35	70833	Fonts Not Loading Properly After Updating the Theme	Themes	N/A	N/A	N/A	
2019-09-05T21:14	70834	Issue enabling Wordpress Multisite	WordPress	N/A	N/A	N/A	
2019-09-05T23:05	70837	Failure to update WordPress Multisite - unable to copy some files	Upgrades Permissions	N/A	N/A	N/A	
2019-09-06T09:50	70841	Images only showing if logged in	Themes Permissions	N/A	N/A	N/A	
2019-09-06T12:38	70847	Create a MySQL database failure	Database	N/A	N/A	N/A	
2019-09-06T14:23	70849	SSL not working on my bitnami WordPress hosted on AWS CloudFront	Domains & DNS	N/A	N/A	N/A	
2019-09-06T16:57	70851	Unable to restart PHP after reboot	Apache configuration	N/A	N/A	N/A	
2019-09-06T21:21	70852	How to create WordPress into a site	WordPress	N/A	N/A	N/A	
2019-09-06T21:42	70853	How to Configure Cron Job (File type:- PHP) on Google Cloud Wordpr	Cron	N/A	N/A	N/A	
2019-09-07T02:39	70854	Activating Varnish Results in ERR_TOO_MANY_REDIRECTS	Miscellaneous	N/A	N/A	N/A	
2019-09-07T06:37	70855	Snapshot restore on AWS - TOO many redirect error after correct cor	Cache	N/A	N/A	N/A	
2019-09-07T08:35	70856	Renew the self signed SSL and it worked, but sadly on next day i can't	Miscellaneous	N/A	N/A	N/A	
2019-09-07T10:58	70858	Permissions on WordPress /plugins/ folder not correct	Permissions	N/A	N/A	N/A	
2019-09-07T13:49	70859	Permissions seem correct - Cant install/update plugins or add pages t	Permissions	N/A	N/A	N/A	
2019-09-07T14:54	70860	Adding a subdomain to bitnami AWS instance	Domains & DNS	N/A	N/A	N/A	
2019-09-07T16:34	70861	Can't acces localhost from outside my network anymore	Network	N/A	N/A	N/A	
2019-09-08T08:33	70866	Undefined index: title_dektop_fsize	Plug-ins	N/A	N/A	N/A	
2019-09-08T13:58	70870	Comodo positive SSL installation on wordpress	Other SSL certificate	N/A	N/A	N/A	
2019-09-08T14:04	70871	AWS Wordpress Multisite Forbidden 403, How can I Reinstall Wordpr	WordPress	N/A	N/A	N/A	
2019-09-08T18:19	70872	SSL_ERROR_BAD_CERT_DOMAIN domain: www.chatexplore.com	Other SSL certificate	N/A	N/A	N/A	
2019-09-08T21:58	70873	WordPress Multi-Tier Data Disk (SDB) not keeping links & not keeping	Multi-tier Backup/restore/migrate	N/A	N/A	N/A	
2019-09-09T06:23	70875	How to Rate limits: fixing	Let's Encrypt	Renewal	Unknown	Yes	(Not using Bncert?)
2019-09-09T09:43	70879	Unable to complete certificate renewal after expiration	Let's Encrypt	Renewal	Yes	Improvement	Check for services using port 80
2019-09-09T10:19	70880	Hi,I configure two websites using the link https://docs.bitnami.com/a	Custom application	N/A	N/A	N/A	
2019-09-09T10:29	70881	Site down after running Bitnami HTTPS Configuration Tool	Let's Encrypt	Creation	Yes	Improvement	Support wildcard certificates and other validation modes
2019-09-10T01:13	70889	Wildcard SSL setup for a WP multisite with subdomains and custom d	Let's Encrypt	Creation	Yes	Improvement	Support wildcard certificates and other validation modes
2019-09-10T07:05	70891	Unable to log into word press admin after changing user name and te	WordPress	N/A	N/A	N/A	
2019-09-10T07:19	70892	Website is slow, after activating ssl	Performance	N/A	N/A	N/A	
2019-09-10T10:29	70894	Wp-cli paths should be fixed in Wordpress module	WordPress	N/A	N/A	N/A	
2019-09-10T10:41	70895	Unable to change main site's Site Address (URL) - Is this the cause to	WordPress	N/A	N/A	N/A	
2019-09-10T14:54	70898	Accessibility Standards	Miscellaneous	N/A	N/A	N/A	
2019-09-10T19:18	70900	504 gateway time out - Wordpress Multi-Site	Performance	N/A	N/A	N/A	
2019-09-10T21:26	70902	Help with Autorenew SSL certificate	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-09-10T22:51	70904	Wordfence Plugin REVOKE admin rights on my Administrator user	WordPress Security	N/A	N/A	N/A	
2019-09-11T04:29	70905	Installing vips extension (php) (extension=vips.so)	PHP config/exts	N/A	N/A	N/A	
2019-09-11T04:44	70906	Using the SSH into Bitnami but I'm being asked for sudo password	SSH	N/A	N/A	N/A	
2019-09-11T06:28	70907	Unmonitored apacheAH00526: Syntax error on line 55 of /opt/bitnan	Let's Encrypt Apache configuration	Creation	No	Improvement	Bncert idea: Reset certificate if Apache certificates are not found
2019-09-11T13:36	70912	Permission settings for Wordpress all wrong while trying to access wp	Permissions	N/A	N/A	N/A	
2019-09-11T14:11	70913	I can not issue a new certificates for www.tight-binding.com using ge	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-11T17:48	70918	Revoke sftp access with a shared ppk	SSH	N/A	N/A	N/A	
2019-09-11T18:35	70919	Can't access my wordpress after update on wp-config.php	WordPress	N/A	N/A	N/A	
2019-09-11T18:44	70922	Can't access my wordpress HTTP 500 after trying to update upload_fi	Permissions	N/A	N/A	N/A	
2019-09-11T22:27	70925	link expired but site still gets deleted successfully	WordPress	N/A	N/A	N/A	
2019-09-11T23:10	70927	Apache not restarting	Apache configuration	N/A	N/A	N/A	
2019-09-12T00:33	70928	Aws problem -Error establishing a database connection	Database	N/A	N/A	N/A	
2019-09-12T04:26	70929	Lightsail WP Upgrade PHP7	Backup/restore/migrate	N/A	N/A	N/A	
2019-09-12T13:08	70935	Unable to force redirect site to https	Redirections Load balancer	N/A	N/A	N/A	
2019-09-12T14:13	70938	Configuring WP Hide & Security Enhancer htaccess	Plug-ins	N/A	N/A	N/A	
2019-09-12T15:43	70941	Max_input_vars php.ini set to 3000 but still i see 1000	PHP config/exts	N/A	N/A	N/A	
2019-09-12T16:35	70943	Slow memory leak with httpd in bitnami wordpress multisite	Performance	N/A	N/A	N/A	
2019-09-12T17:17	70944	Non-WWW is Secure and Valid SSL WWW is Not Secure and Expired S	Let's Encrypt	Creation	Unknown	N/A	
2019-09-12T19:26	70946	Problema de Conexión compartida | Problema a editar temas y plugi	Themes	N/A	N/A	N/A	
2019-09-12T22:09	70947	How to paste output of BN Support Tool	Installer	N/A	N/A	N/A	
2019-09-13T07:10	70948	How to choose EC2 for Wordpress Bitnami?	Performance	N/A	N/A	N/A	
2019-09-13T15:08	70952	Restored VM WordPress in Azure, unable to access wp-admin	Multi-tier Backup/restore/migrate	N/A	N/A	N/A	
2019-09-13T20:03	70956	How to Install a Second WordPress Site in a Subdirectory (Google Clou	Installer	N/A	N/A	N/A	
2019-09-13T23:00	70957	Root directory location AWS Lightsail Instance with Bitnami & Wordp	Apache configuration	N/A	N/A	N/A	
2019-09-14T19:02	70960	Too Many SSL Certificates Issued (all previous instances/deployments	Let's Encrypt	Creation	No	Improvement	(Not using Bncert) - Add NGINX support
2019-09-15T07:52	70963	Error uploading HTTP images in wp-admin	WordPress	N/A	N/A	N/A	
2019-09-15T10:25	70964	Proper non-www to www, and http to https redirects	Redirections	N/A	N/A	N/A	
2019-09-16T09:57	70967	AWS Lightsail, Bitnami Wordpress - Non www to HTTPS www redirec	Redirections Domains & DNS	N/A	N/A	N/A	

2019-09-16T10:31	70968	Site Can't Be Reached, took too long to respond	Performance	N/A	N/A	N/A	
2019-09-16T12:49	70971	Used BNcert tool - how do I remove www. subdomain for dev server?	Let's Encrypt	Creation	Yes	Improvement	Improve the way we suggest users to add cert for www subdomain
2019-09-16T15:59	70974	Server too slow when loads	Performance	N/A	N/A	N/A	
2019-09-16T16:11	70975	Virtual Host Config for Multiple Bitnami WordPress Installation(Not M	Apache configuration	N/A	N/A	N/A	
2019-09-16T20:29	70977	WordPress High Availability by Bitnami Apache issue	Multi-tier	N/A	N/A	N/A	
2019-09-17T00:03	70979	Wordpress ajax issue, possibly memory?	Plug-ins	N/A	N/A	N/A	
2019-09-17T04:30	70981	Getting HTTP ERROR 500 when trying to access my site	Apache configuration	N/A	N/A	N/A	
2019-09-17T06:46	70982	Bitnami-wordpress site showing some blank pages	Plug-ins	N/A	N/A	N/A	
2019-09-17T10:00	70984	WordPress with Azure Database for MariaDB Azure template broken	Multi-tier	N/A	N/A	N/A	
2019-09-17T21:09	70991	Adding a 3rd site to multi-site but DNS is not resolving	Domains & DNS	N/A	N/A	N/A	
2019-09-17T22:52	70992	Issues Renewing Let's Encrypt SSL Cert	Let's Encrypt	Renewal	Yes	Bug	Fix the way we remove previous cron entries
2019-09-18T02:53	70995	Certificate generated are not reflected on the website	Let's Encrypt	Creation	Yes	Improvement	Add support for modifying vhosts
2019-09-18T03:11	70996	Convert www to non-www (none of these have worked)	Redirections	N/A	N/A	N/A	
2019-09-18T03:46	70997	FileZilla is Limiting Transfer of wpress File to around 5MB	Disk	N/A	N/A	N/A	
2019-09-18T08:17	71003	Multiple errors - ./bncert-tool warnings	Let's Encrypt	Creation	Yes	Yes	None
2019-09-18T09:11	71004	Change Wordpress Location in ubuntu 16.04	Miscellaneous	N/A	N/A	N/A	
2019-09-18T09:45	71005	Receiving “ERR_TOO_MANY_REDIRECTS” after HTTPS config in Wor	Let's Encrypt Redirections	Creation	Yes	Bug	Don't supoport redirections for WordPress Multisite
2019-09-18T12:02	71007	Strange error in error_log	Apache configuration Cron	N/A	N/A	N/A	
2019-09-18T19:58	71011	Email issues - business - need Bitmani GCP MX records updated	Domains & DNS	N/A	N/A	N/A	
2019-09-19T09:40	71017	CORS headers issue	CORS	N/A	N/A	N/A	
2019-09-19T10:53	71018	SIGTERM error on running container	Containers	N/A	N/A	N/A	
2019-09-20T11:24	71025	No Virtual Machines showing in Azure Launchpad	Miscellaneous	N/A	N/A	N/A	
2019-09-20T11:24	71026	Unable to install apache	Installer	N/A	N/A	N/A	
2019-09-20T20:48	71031	Apache keeps failing anytime edits/customization is done in wordpres	Apache configuration	N/A	N/A	N/A	
2019-09-20T21:15	71032	Set Up Load Balancer for GCP Bucket Using CloudFlare	Load Balancer	N/A	N/A	N/A	
2019-09-21T03:01	71034	Server down after I blast users with push notifications	Miscellaneous	N/A	N/A	N/A	
2019-09-21T08:56	71035	Accessing phpMyAdmin not working	phpMyAdmin Credentials	N/A	N/A	N/A	
2019-09-21T16:01	71036	Where can find bitnami wordpress exe download for 32 bit windows?	Old version	N/A	N/A	N/A	
2019-09-22T10:16	71040	Setting up a staging subdomain on the production AWS instance	Apache configuration	N/A	N/A	N/A	
2019-09-22T17:54	71044	Error during Let's Encrypt installation - mismatching IP addresses in D	Let's Encrypt Mixed content	Creation	Yes	Yes	Add option for enabling HTTPS with Bnconfig, and run with Bncert
2019-09-23T01:05	71046	Rewriterule ignored	Apache configuration	N/A	N/A	N/A	
2019-09-23T07:10	71048	Using a single instance in Lightsail as hosting of multiple wordpress sit	WordPress	N/A	N/A	N/A	
2019-09-23T09:25	71050	Unable to delete cache from w3 total cache	Plug-ins Cache	N/A	N/A	N/A	
2019-09-23T09:42	71051	Cant Open the bitnami application after installation	Miscellaneous	N/A	N/A	N/A	
2019-09-23T13:41	71056	I installed a Lets Encrypt certificate, but it still showing Your connecti	Let's Encrypt Mixed content	Creation	Yes	Yes	Add option for enabling HTTPS with Bnconfig, and run with Bncert
2019-09-24T01:55	71061	Issue configuring Let's Encrypt to auto-renew	Let's Encrypt Cron	Renewal	Yes	Yes	None
2019-09-24T03:14	71062	Remove Let's Encrypt Certificate from Bitnami stack on Azure	Let's Encrypt	N/A	No	Improvement	(Not using Bncert) - Support removing certificates
2019-09-24T13:57	71069	In the menu my home page is pointing to ip address instead of my do	WordPress	N/A	N/A	N/A	
2019-09-24T15:05	71070	Wp-admin error - white screen of death	Plug-ins Redirections	N/A	N/A	N/A	
2019-09-24T15:34	71071	Unable to start the apache and ssl error	Let's Encrypt	Renewal	No	Improvement	Support Let's Encrypt validation for CloudFlare and other DNS providers
2019-09-24T18:42	71075	Mixed content problems (AWS, ELB, WordPress)	Mixed content	N/A	N/A	N/A	
2019-09-24T20:39	71076	After installation of plugin error accessing Wordpress	Plug-ins	N/A	N/A	N/A	
2019-09-25T09:05	71081	Your connection to this site is not fully secure	Mixed content	N/A	N/A	N/A	
2019-09-25T11:29	71084	AWS Lightsail Load Balancer Health Check Fails	Load Balancer	N/A	N/A	N/A	
2019-09-25T12:48	71086	When i changed aws volume limit, site lost css and url got affected	WordPress	N/A	N/A	N/A	
2019-09-25T14:30	71088	Http returns ERR_CONNECTION_REFUSED, https works fine	Apache configuration	N/A	N/A	N/A	
2019-09-25T16:47	71090	The site is experiencing technical difficulties. Please check your site ad	Themes	N/A	N/A	N/A	
2019-09-25T18:50	71091	How to change Wordpress Site and Home URL	WordPress	N/A	N/A	N/A	
2019-09-25T22:05	71093	Lightsail Static IP Inaccessible After DNS Zone Creation	Domains & DNS	N/A	N/A	N/A	
2019-09-26T10:26	71096	EC2 Nano for Wordpress	Performance	N/A	N/A	N/A	
2019-09-26T11:50	71097	How to redirect www.domain.com to domain.com	Redirections	N/A	N/A	N/A	
2019-09-26T12:43	71098	Unreachable website	Disk	N/A	N/A	N/A	
2019-09-26T12:51	71099	Multiple Wordpress Installations(Not Multisite) Dedicated Server Arc	WordPress	N/A	N/A	N/A	
2019-09-26T13:15	71100	Start services on reboot error	WordPress	N/A	N/A	N/A	
2019-09-26T14:06	71102	Run wordpress at root url	Application URL prefix	N/A	N/A	N/A	
2019-09-26T17:57	71104	Please how how do i remove previously installed ssl on my bitnami sta	Other SSL certificate	N/A	N/A	N/A	
2019-09-27T14:20	71112	Volume Keeps Growing In Size affecting Availability of my instance	Disk	N/A	N/A	N/A	
2019-09-27T21:31	71116	MultiSite Top Level SSL Certificate wrong certificate attached to new	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-27T22:23	71117	Error 400 when running bncert-tool	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-28T19:32	71122	Setup an additional domain with SSL	Let's Encrypt	Creation	No	N/A	(Duplicated #71129)
2019-09-28T19:55	71123	Varnish on Apache with SSL (HTTPS)	Miscellaneous	N/A	N/A	N/A	
2019-09-29T04:57	71126	Wordpress Multisite don't permit enable ssl for all domains	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-29T19:04	71129	Successfully requested certificate with LEGO - site still doesn't respon	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-09-29T19:33	71131	How to Create renew-certificate.sh	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-09-30T06:46	71133	MySQL with PARTITIONING PLUGIN	Database	N/A	N/A	N/A	
2019-09-30T14:02	71138	Can you bring down a current Wordpress site to work on locally?	Backup/restore/migrate	N/A	N/A	N/A	
2019-09-30T14:57	71139	All-in-one migration doesn't create all year/month folders in the uplo	Plug-ins	N/A	N/A	N/A	
2019-09-30T21:29	71144	Cannot use FTP with Bitnami user, must I login with the root in order	FTP/SFTP	N/A	N/A	N/A	
2019-09-30T23:58	71145	LetsEncrypt Certificate is not automatically renewing and won't perm	Let's Encrypt	Renewal	Yes	Improvement	Detect if the e-mail is registered
2019-10-01T08:41	71149	Renew-certificate.sh - Operation not permitted	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-01T13:25	71151	Generate-certificate 100% CPU	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-01T14:07	71152	Changes to php.ini are not reflected	PHP config/exts	N/A	N/A	N/A	
2019-10-01T15:27	71153	MySql : Forcing Close of thread 999 user:bn_wordpress	Database	N/A	N/A	N/A	
2019-10-02T02:07	71157	AWS EC2 - Bitnami Wordpress bncert-tool “resolves to different IP”	Let's Encrypt	Creation	Yes	Yes	None
2019-10-02T03:43	71158	Expired lets encrypt cert and tXT incorrect message	Let's Encrypt	Renewal	No	N/A	
2019-10-02T06:59	71160	I can't edit .htaccess file by using filezilla	Redirections Permissions Domains & DNS	N/A	N/A	N/A	
2019-10-02T09:42	71162	MySQL won’t start on WP AWS Installation	Database	N/A	N/A	N/A	
2019-10-02T11:31	71165	Error in creating the SSL Certificate for .ca and .com domain	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-10-02T12:35	71166	Hosting images on a subdomain	Apache configuration	N/A	N/A	N/A	
2019-10-02T13:00	71167	Apache2 config for framing ALLOW-FROM says unknown-parameter	Apache configuration	N/A	N/A	N/A	
2019-10-02T15:28	71170	Unable to install Apache as a service with name wordpressApache	Installer	N/A	N/A	N/A	
2019-10-02T15:39	71171	Application not found error while installing Bitnami for Wordpress in	Installer	N/A	N/A	N/A	
2019-10-02T23:27	71172	Cannot get cloudformation install of Wordpress to run successfully	Multi-tier	N/A	N/A	N/A	
2019-10-03T01:48	71173	ERR_TOO_MANY_REDIRECTS after following instructions to configur	Let's Encrypt	Creation	Yes	Bug	Don't supoport redirections for WordPress Multisite
2019-10-03T10:12	40053	Can’t restore Wordpress in new laptop running on Windows 10 from V	Backup/restore/migrate	N/A	N/A	N/A	
2019-10-03T15:09	71180	Bitnami Wordpress 4 Mac: Can't recover my password + generic user	Credentials	N/A	N/A	N/A	

2019-10-03T21:07	71183	CORS Issue - Wordpress on AWS - Coudfront offloaded media and asse	CORS Mixed content	N/A	N/A	N/A	
2019-10-04T00:11	71184	Let's encrypt certificate renewal	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-04T02:58	71185	Establishing Sub Domain	Let's Encrypt	Creation	Yes	Yes	None
2019-10-04T12:10	71186	SSL WWW not secure non-WWW is secure	Apache configuration	N/A	N/A	N/A	
2019-10-04T12:28	71188	Wp_options.ibd File is Growing Huge Everyday	Disk	N/A	N/A	N/A	
2019-10-04T20:45	71197	Htaccess webp wordpress multi-tier	Multi-tier Apache configuration	N/A	N/A	N/A	
2019-10-05T07:09	71201	Get Wooshark working on Google Cloud Platform	Plug-ins	N/A	N/A	N/A	
2019-10-05T10:40	71203	Unable to View mysql database in phpmyadmin due to enable require	phpMyAdmin	N/A	N/A	N/A	
2019-10-05T11:48	71204	Why is it very slow to have an initial connection?	Performance	N/A	N/A	N/A	
2019-10-05T15:11	71205	Redirection prevents logging in to WP Admin (site unavailable) after A	Redirections	N/A	N/A	N/A	
2019-10-05T15:15	71206	Redirect WWW to NON WWW With Bitnami AWS HTTPS Stack	Redirections	N/A	N/A	N/A	
2019-10-05T17:46	71207	How to reset local password / user on Localhost	Credentials Database	N/A	N/A	N/A	
2019-10-05T18:56	71208	Delete /Opt/ on Mac re-installing software and not working	Installer	N/A	N/A	N/A	
2019-10-06T02:50	71211	SSH tunnel for PHPMYADMIN access	SSH phpMyAdmin	N/A	N/A	N/A	
2019-10-06T16:12	71213	Help needed to go from local to online Wordpress	Backup/restore/migrate	N/A	N/A	N/A	
2019-10-06T21:46	71215	Set RDS as default	Database	N/A	N/A	N/A	
2019-10-06T22:55	71216	CORS header not working retrieving xml	CORS	N/A	N/A	N/A	
2019-10-07T06:17	71219	How to activate HTTPS in WordPress Multisite Certified by Bitnami ar	Redirections	N/A	N/A	N/A	
2019-10-07T06:31	71220	Rest API permission issues	Plug-ins	N/A	N/A	N/A	
2019-10-07T12:01	71225	I cannot enable HTTPS for website, when restarting apache, sslcertifi	Other SSL certificate	N/A	N/A	N/A	
2019-10-07T13:41	71227	Apache Web server can't start	Apache configuration	N/A	N/A	N/A	
2019-10-07T14:35	71229	I can't find my website	Installer	N/A	N/A	N/A	
2019-10-08T05:53	71233	Load Balancing with SSL and AWS Certificate Manager (Problem)	Load Balancer	N/A	N/A	N/A	
2019-10-08T09:53	71235	Multisite Google Config - New domains dashboard won't load	Domains & DNS	N/A	N/A	N/A	
2019-10-08T12:06	71236	Accidentally deleted/overwrote wp-config.php ... where do I find/res	Credentials	N/A	N/A	N/A	
2019-10-08T13:13	71237	Remove domain from Lets Encrypt certificate before renewal	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-08T15:11	71239	Downloading wordpress - stack wizard never comes up	Installer	N/A	N/A	N/A	
2019-10-08T21:46	71243	I bought the alidropship plugin recently and am having trouble install	Plug-ins	N/A	N/A	N/A	
2019-10-09T01:31	71244	Wp-admin URL not working after installing Varnish with SSL on Word	Miscellaneous	N/A	N/A	N/A	
2019-10-09T06:44	71246	Ssl- err_cert_common_name_invalid	Let's Encrypt	Creation	Unknown	N/A	(Not using Bncert?)
2019-10-09T07:58	71249	AWS product category	Miscellaneous	N/A	N/A	N/A	
2019-10-09T13:32	71253	DNS_PROBE_FINISHED_NXDOMAIN after disconnecting domain	Redirections	N/A	N/A	N/A	
2019-10-09T19:31	71256	Ubuntu 18.04 LTS Wordpress Stack?	Miscellaneous	N/A	N/A	N/A	
2019-10-10T04:21	71259	My website running so slow	Performance	N/A	N/A	N/A	
2019-10-10T04:25	71260	SSL redirect loop for /wp-admin page	Redirections	N/A	N/A	N/A	
2019-10-10T05:48	71262	Please see the error below, this was a workign website and now I am	Database	N/A	N/A	N/A	
2019-10-10T06:21	71263	Domain is running on HTTPS but its showing not secured	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-10-10T09:32	71267	The site is experiencing technical difficulties - AWS	Upgrades	N/A	N/A	N/A	
2019-10-10T14:36	71269	Error when trying to setup Auto Renew: Warning: Custom redirection	Let's Encrypt	Renewal	Yes	Yes	None
2019-10-10T15:40	71272	Windows 10 updates issue: MySQL Database and Apache Web Server	Miscellaneous	N/A	N/A	N/A	
2019-10-10T16:23	71273	Upgrading EC2 Instance Beyond t3.2xLarge	Resize instance	N/A	N/A	N/A	
2019-10-10T17:44	71274	How to redirect www.example.com to example.eom	Redirections	N/A	N/A	N/A	
2019-10-10T19:19	71275	Wp rocket is not working on my website	Plug-ins	N/A	N/A	N/A	
2019-10-10T19:31	71276	Unable to start apache. AH00072, AH00015 httpd could not be starte	Apache configuration	N/A	N/A	N/A	
2019-10-10T22:03	71278	How to remove 'wordpress' from site path	Application URL prefix	N/A	N/A	N/A	
2019-10-11T10:03	71286	Wordpress Multisite: Unable to update plugins in backend ... This is us	Permissions	N/A	N/A	N/A	
2019-10-11T10:29	71288	Wp-config.php cant connect to database	Database	N/A	N/A	N/A	
2019-10-11T13:26	71293	Can't get to renew the SSL certificate for the domain	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-11T14:58	71294	Migrating to newest Bitnami version from LAMP stack 5.6	Backup/restore/migrate	N/A	N/A	N/A	
2019-10-11T16:15	71295	Randomly deleted	Miscellaneous	N/A	N/A	N/A	
2019-10-11T18:25	71297	Can't Login through /wp-admin	Plug-ins	N/A	N/A	N/A	
2019-10-12T05:28	71300	Cant not write data to Addition Disks	Disk	N/A	N/A	N/A	
2019-10-12T11:20	71302	Unable to Install and delete plugins	Permissions Plug-ins	N/A	N/A	N/A	
2019-10-12T17:27	71304	Wordpress sites keeps crashing on Amazon EKS	Database	N/A	N/A	N/A	
2019-10-12T20:21	71305	Wordpress site stopped working after region change	Backup/restore/migrate	N/A	N/A	N/A	
2019-10-13T13:19	71308	BNCERT Tool Not Renewing Let's Encrypt SSL Certificate	Let's Encrypt	Renewal	Yes	Yes	None
2019-10-13T19:28	71311	Job for bitnami.service failed because the control process exited with	Disk	N/A	N/A	N/A	
2019-10-14T03:14	71312	My Bitnami Wordpress Instance on Google Cloud is taking to long to l	Performance	N/A	N/A	N/A	
2019-10-14T05:05	71314	Is it possible to install Mysql-ODBC connector on bitnami Mysql for wp	PHP config/exts	N/A	N/A	N/A	
2019-10-14T05:40	71315	Problems migrating to new AWS instance	Backup/restore/migrate	N/A	N/A	N/A	
2019-10-14T10:34	71317	Mysqld.bin CPU usage between 150% - 200% with Bitnami + Wordpre	Performance	N/A	N/A	N/A	
2019-10-14T11:28	71320	Receiving Error 524 on my Wordpress Site	Performance	N/A	N/A	N/A	
2019-10-14T14:42	71325	Wordpress site loading slow after migrating from one AWS EC2 instar	Performance Backup/restore/migrate Plug-ins	N/A	N/A	N/A	
2019-10-14T19:28	71331	Wordpress MULTI - TIER wp-config (http works fine but when i chang	Multi-tier WordPress	N/A	N/A	N/A	
2019-10-14T20:42	71332	Bncert-tool Not Auto Renewing	Let's Encrypt	Renewal	Yes	Yes	None
2019-10-15T12:15	71343	Wp_options table and Wp_options.ibd file too large!	WordPress	N/A	N/A	N/A	
2019-10-15T13:08	71344	CURL connection timeout	Network	N/A	N/A	N/A	
2019-10-15T17:07	71346	WordPress installed on AWS - This site can't be reached	Apache configuration	N/A	N/A	N/A	
2019-10-15T23:27	71350	Webpage not loading instead showing HTML 500 Error after updatin	Apache configuration	N/A	N/A	N/A	
2019-10-16T03:22	71351	How to completely disable secure connections?	Apache configuration	N/A	N/A	N/A	
2019-10-16T13:05	71358	Unable to do redirect from http://<mydomainname>.com to http://w	Redirections	N/A	N/A	N/A	
2019-10-16T15:36	71360	Error starting services No space left on device	Redirections	N/A	N/A	N/A	
2019-10-16T21:24	71363	CDN not working properly on a multisite	Load Balancer	N/A	N/A	N/A	
2019-10-16T21:31	71364	I am not able to see the Add New Plugin button even being an admin	Plug-ins	N/A	N/A	N/A	
2019-10-17T03:49	71368	I have a static IP, and can open an ssh tunnel, but I still cannot gain ac	phpMyAdmin	N/A	N/A	N/A	
2019-10-17T12:20	71377	After I attempted to install letscrypt ssl using the Alternative Approa	Let's Encrypt	Creation	No	N/A	(Not using Bncert)
2019-10-17T12:45	71378	ERR_CONNECTION_REFUSED issue	Let's Encrypt	Renewal	No	N/A	(Not using Bncert)
2019-10-17T13:23	71379	I have the index listing of my files	Miscellaneous	N/A	N/A	N/A	
2019-10-17T15:08	71381	SSL_PROTOCOL_ERROR on certain networks	Network	N/A	N/A	N/A	
2019-10-17T15:17	71382	How to keep Disk Full error from occurring?	Disk	N/A	N/A	N/A	
2019-10-17T18:02	71384	Security Guide for new install of Bitnami Wordpress Multisite on GCP	Security	N/A	N/A	N/A	
2019-10-17T21:17	71386	Can't Enable CORS	CORS Themes	N/A	N/A	N/A	
2019-10-17T23:56	71388	Infected HTTPD.bin file	Security	N/A	N/A	N/A	
2019-10-18T02:37	71389	How can I deploy WordPress with NGINX to Google Cloud Run	Containers	N/A	N/A	N/A	
2019-10-18T08:36	71392	Mysqli_real_connect(): (HY000/2002): No such file or directory	Disk	N/A	N/A	N/A	
2019-10-18T11:21	71395	Turn off SFTP Server	FTP/SFTP	N/A	N/A	N/A	
2019-10-18T11:38	71396	Cannot access the SQL database (application password not working a	Credentials Database	N/A	N/A	N/A	
2019-10-18T16:18	71398	Wordpress on EC2 micro instance randomly gives 502/504/ Cannot co	Performance	N/A	N/A	N/A	
2019-10-18T17:45	71399	Plugin menu missing	Plug-ins	N/A	N/A	N/A	
2019-10-19T13:47	71403	Permission Issues: AWS Bitnami WP AMI + Changing Root Directory F	Apache configuration	N/A	N/A	N/A	
2019-10-19T15:01	71406	Internal Server Error after migrating WP from PLESK to GCP	Backup/restore/migrate	N/A	N/A	N/A	

2019-10-19T18:15	71408	Tried to install Let's Encrypt on Lightsail. Cannot start Apache	Let's Encrypt Apache configuration	N/A	No	N/A	(Not using Bncert)
2019-10-19T18:17	71409	Accidentally deleted mysql.bin.log files	Database	N/A	N/A	N/A	
2019-10-19T23:21	71415	Bitnami Apache not automatically starting and serving my site after r	Miscellaneous	N/A	N/A	N/A	
2019-10-19T23:22	71416	Multiple domains with multi-apps	Let's Encrypt Apache configuration	Creation	Yes	Yes	None
2019-10-20T04:33	71417	Duplicate Certificate	Other SSL certificate	N/A	N/A	N/A	
2019-10-20T07:43	71419	Facing a CORS Issue when trying to serving assets from Cloudfront usi	CORS	N/A	N/A	N/A	
2019-10-20T22:25	71422	WordPress website keeps crashing with error establishing a database	Database	N/A	N/A	N/A	
2019-10-21T10:40	71429	Wordpress website loading too slow after migration	Performance Backup/restore/migrate	N/A	N/A	N/A	
2019-10-21T13:58	71432	Current bitnami LAMP stack still doesn't support libsodium	PHP config/exts	N/A	N/A	N/A	
2019-10-21T15:20	71434	Wordpress on Lightsail | Permission Error after Chmod wp-config	Permissions	N/A	N/A	N/A	
2019-10-21T19:45	71436	Granting developers/freelancers/partners access to an EC2 instance v	SSH	N/A	N/A	N/A	
2019-10-21T21:30	71438	Can establish first connection between Bitnami console and Oracle ac	Miscellaneous	N/A	N/A	N/A	
2019-10-22T02:01	71440	Not sure how to get the SSL cert on my deployment of WordPress and	Other SSL certificate	N/A	N/A	N/A	
2019-10-22T09:44	71441	Log out to see the Website as non-member/users	WordPress	N/A	N/A	N/A	
2019-10-22T12:34	71442	Wordpress MySQL crashes constantly with no error in log file	Performance Database	N/A	N/A	N/A	
2019-10-22T22:12	71446	Blank homepage and 500 server error when accessing websites	WordPress	N/A	N/A	N/A	
2019-10-23T01:41	71447	Getting https redirect error with bn-cert tool on multiste	Let's Encrypt	Renewal	Yes	Yes	None
2019-10-23T02:40	71448	Wordpress Letsencrypt SSL Renewal	Let's Encrypt	Renewal	Unknown	N/A	(Not using Bncert?)
2019-10-23T12:28	71458	Install multiple wordpress modules locally	Installer	N/A	N/A	N/A	
2019-10-23T15:25	71463	Form Validation Failure	WordPress	N/A	N/A	N/A	
2019-10-23T16:43	71464	An error occurred revoking certificates with Let's Encrypt:	Let's Encrypt	Renewal	Yes	Improvement	Detect if the e-mail is registered. Obtain the e-mail for the certificate to revoke.
2019-10-23T17:01	71465	As running bncert-tool for different domain, Error occurred: Error run	Let's Encrypt	Creation	Yes	Yes	None
2019-10-23T19:34	71468	Inconsistent behavior accessing 3 WordPress sites on single Lightsail i	Miscellaneous	N/A	N/A	N/A	
2019-10-24T01:53	71470	Acces the plugins directory	Plug-ins	N/A	N/A	N/A	
2019-10-24T04:44	71471	Offloading uploads to S3 / search and replace in database	Plug-ins	N/A	N/A	N/A	
2019-10-24T07:23	71472	I'm locked out from my Wp admin page. (AWS, Lightsail, wordpress)	Credentials	N/A	N/A	N/A	
2019-10-25T02:30	71481	I'm locked out from my Wp admin page	Credentials	N/A	N/A	N/A	
2019-10-25T10:03	71484	I need to switch my Lightsail instance to a Static IP, what should i do t	Plug-ins	N/A	N/A	N/A	
2019-10-25T10:09	71485	Multisite Module issue	Plug-ins	N/A	N/A	N/A	
2019-10-25T11:37	71486	MySQL could not be started. GCP+Apache+WordPress	Database	N/A	N/A	N/A	
2019-10-25T12:39	71487	Cannot restart Apache on my bitnami Instance	Apache configuration	N/A	N/A	N/A	
2019-10-25T13:38	71488	Cannot remove bitnami banner	Bitnami banner	N/A	N/A	N/A	
2019-10-25T16:16	71489	Wordpress Site Not Working	Apache configuration	N/A	N/A	N/A	
2019-10-25T18:26	71490	WordPress Multisite - subdomain_install set to false, but wp-admin ar	WordPress Apache configuration	N/A	N/A	N/A	
2019-10-26T03:02	71492	SSLCertificateFile: file '/opt/bitnami/apache2/conf/aknainmobiliaria.c	Let's Encrypt	Creation	No	N/A	
2019-10-26T10:26	71496	Connection to my website is not fully secured, How can I make it fully	Load Balancer	N/A	N/A	N/A	
2019-10-27T04:51	71500	Can't add new site or edit/add users inside Network Admin panel "Th	WordPress	N/A	N/A	N/A	
2019-10-27T07:18	71502	My SSL certificate has expired and i am not able to renew it because	Let's Encrypt	Renewal	Unknown	N/A	
2019-10-27T08:07	71503	Unable to Access phpmyadmin : Bad Request / This site can't be reac	phpMyAdmin Redirections	N/A	N/A	N/A	
2019-10-27T08:41	71504	Wordpress on NGINX + SSL: Server Terminate during product upload	PHP config/exts	N/A	N/A	N/A	
2019-10-27T18:09	71507	What to use for automatic git deployment to a bitnami wordpress sta	Miscellaneous	N/A	N/A	N/A	
2019-10-28T14:54	71510	Db_password not right	Credentials Database	N/A	N/A	N/A	
2019-10-28T15:00	71511	Could not open configuration file /opt/bitnami/apache2/conf/bitnam	Apache configuration	N/A	N/A	N/A	
2019-10-28T18:11	71515	With SSL setup everything works except when I type http://domain.c	Domains & DNS	N/A	N/A	N/A	
2019-10-28T22:30	71517	Error with connection82bc3be8-39eb-5239-6df3-e5dc222b1e4d	Plug-ins	N/A	N/A	N/A	
2019-10-29T00:27	71518	Production-Ready Wordpress on AWS fails to create Wordpress Stack	Multi-tier	N/A	N/A	N/A	
2019-10-29T07:56	71520	Sir I Installed Bitnami wordpress from aws market place and i am stu	SSH	N/A	N/A	N/A	
2019-10-30T11:26	71532	How to change the domain of WordPress website on Amazon web se	Domains & DNS	N/A	N/A	N/A	
2019-10-30T12:28	71533	MySQL Data abnormally growing for unknown reason	Database	N/A	N/A	N/A	
2019-10-30T21:53	71535	When Bitnami Boots in Lightsail its loading the private ip in the conso	SSH	N/A	N/A	N/A	

Apéndice C
Generación y configuración de certificados HTTPS

C.1 Generación de un certificado HTTPS

C.1.1 Generación con OpenSSL

Para la creación de un certificado, primero es necesario generar la clave privada. Esto es muy sencillo con programas como `openssl`.

Código C.1 Creación de una clave privada con OpenSSL de 2048 bits.

```
$ sudo openssl genrsa -out server.key 512
Generating RSA private key, 512 bit long modulus
.......++++++++++++
.........++++++++++++
e is 65537 (0x10001)
```

Código C.2 La privada obtenida en el ejemplo anterior.

```
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMwrya7BDY3qfLzptJ7c3pjLfOYuBpzcKR6tz4KjzUJ1yETyj8t7
aRDt4+9CKCccl815tyJT9T20geTWNHerItUCAwEAAQJBAIj3cxQt5GbpAIdHDOlp
6FZ+ZCqSg9MlCtzO4x+TvXYwFD9BOJpo8gNLtCcrm9G9JDVUacFSgaSAUW02lgYc
/MECIQDywwbcqNkn2320G1bnBjrG+Df3SV+1YhDb/+HLHGo1pQIhANdOB+gCMpIZ
DbznVuUewcpj6AT0RHP9VI0k8QnsG5FxAiBIjsoKQd1F8HCN2G4M9uuydJYlrySQ
DhOD7eMK1h9YkQIhAI7Dbvqoel/lvPZFb5j9jAJnvLGMRteiYy40EKBDrwQBAiEA
v0wWBq7nCgHHli9EX95KiK+T67REmVIpmnGJRsjnohE=
-----END RSA PRIVATE KEY-----
```

A continuación, es necesario crear una solicitud de firma de certificado o CSR, que será necesario enviar a una autoridad de certificación, con la que permitirá generar un certificado.

El certificado estará asociado a un dueño y a un dominio específico, que se definen durante la creación de solicitud de firma de certificado, como se observa a continuación.

Código C.3 Creación de la solicitud de firma de certificado con OpenSSL.

```
$ openssl req -new -key server.key -out cert.csr
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:ES
State or Province Name (full name) []:Sevilla
Locality Name (eg, city) []:Sevilla
Organization Name (eg, company) []:Universidad de Sevilla
Organizational Unit Name (eg, section) []:Dpto. Telemática
Common Name (eg, fully qualified host name) []:example.com
Email Address []:marcos@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

Código C.4 La solicitud de firma de certificado obtenida en el ejemplo anterior.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZTCCAQ8CAQAwgakxCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdTZXZpbGxhMRAw
DgYDVQQHDAdTZXZpbGxhMR8wHQYDVQQKDBZVbml2ZXJzaWRhZCBkZSBTZXZpbGxh
MRwwGgYDVQQLDBNEcHRvLiBUZWxlbcODwqF0aWNhMRQwEgYDVQQDDAtleGFtcGxl
LmNvbTEhMB8GCSqGSIb3DQEJARYSbWFyY29zQGV4YW1wbGUuY29tMFwwDQYJKoZI
hvcNAQEBBQADSwAwSAJBAMwrya7BDY3qfLzptJ7c3pjLfOYuBpzcKR6tz4KjzUJ1
yETyj8t7aRDt4+9CKCccl815tyJT9T2OgeTWNHerItUCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA0EAx2LhhR7pDIBN7LPcki4jJYH1SRkzi8GGP5UZSWbQQhDXpalnWqwA
pRR6rKVmAKHoyB0FDXwdF1RlWPqpCVGlfw==
-----END CERTIFICATE REQUEST-----
```

La certificación habitualmente tiene un coste monetario, y requiere un proceso de verificación para confirmar la validez de los datos provistos en la solicitud de firma del certificado. Este proceso culmina con la obtención de un certificado asociado a la clave privada original, que normalmente sería reconocido como válido en los navegadores Web más populares si es usado en el dominio configurado (en el ejemplo anterior, para `example.com`).

Es posible, aunque habitualmente no recomendable, la creación de un certificado autofirmado por el propio equipo, como se realiza a continuación. Este certificado no sería reconocido como válido por un cliente Web.

Código C.5 Creación de un certificado autofirmado con la propia clave privada mediante OpenSSL.

```
$ openssl x509 -in cert.csr -out server.crt -req -signkey server.key -days 365
Signature ok
subject=/C=ES/ST=Sevilla/L=Sevilla/O=Universidad de Sevilla/OU=Dpto. Telem\xC3\
    x83\xC2\xA1tica/CN=example.com/emailAddress=marcos@example.com
Getting Private key
```

Código C.6 El certificado autofirmado obtenido en el ejemplo anterior.

```
-----BEGIN CERTIFICATE-----
MIICRjCCAfACCQCc+6szHGUZzTANBgkqhkiG9w0BAQUFADCBqTELMAkGA1UEBhMC
```

```
RVMxEDAOBgNVBAgMB1NldmlsbGExEDAOBgNVBAcMB1NldmlsbGExHzAdBgNVBAoM
FlVuaXZlcnNpZGFkIGRlIFNldmlsbGExHDAaBgNVBAsME0RwdG8uIFRlbGVtw4PC
oXRpY2ExFDASBgNVBAMMC2V4YW1wbGUuY29tMSEwHwYJKoZIhvcNAQkBFhJtYXJj
b3NAZXhhbXBsZS5jb20wHhcNMTkxMjAzMjExNTAzWhcNMjAxMjAyMjExNTAzWjCB
qTELMAkGA1UEBhMCRVMxEDAOBgNVBAgMB1NldmlsbGExEDAOBgNVBAcMB1Nldmls
bGExHzAdBgNVBAoMFlVuaXZlcnNpZGFkIGRlIFNldmlsbGExHDAaBgNVBAsME0Rw
dG8uIFRlbGVtw4PCoXRpY2ExFDASBgNVBAMMC2V4YW1wbGUuY29tMSEwHwYJKoZI
hvcNAQkBFhJtYXJjb3NAZXhhbXBsZS5jb20wXDANBgkqhkiG9w0BAQEFAANLADBI
AkEAzCvJrsENjep8vOm0ntzemMt85i4GnNwpHq3PgqPNQnXIRPKPy3tpEO3j70Io
JxyXzXm3IlP1PbSB5NY0d6si1QIDAQABMA0GCSqGSIb3DQEBBQUAA0EAf2bCCKHg
J8sgMsMdql/jXTi2ZMB6VPo8BstqAT34CZFjXRF/5biuNEckE3rn0f/cpK2wfAXi
6hHtk7Za6oqErA==
-----END CERTIFICATE-----
```

C.1.2 Generación con Let's Encrypt

Let's Encrypt permitirá generar tanto una clave privada como un certificado firmado, válido para todos los navegadores Web. Para ello, se habrá de usar uno de los clientes soportados [48]. En este caso, haremos uso de LEGO por la facilidad de instalación [55].

El primer paso consistirá en descargar la herramienta desde la página de descarga[1]. El uso de la herramienta está documentado en la página oficial [59], pero los comandos más comunes son los siguientes[2]:

- `lego run`: Generar un certificado nuevo, para una cuenta específica de Let's Encrypt.
- `lego revoke`: Revocar un certificado existente de una cuenta específica de Let's Encrypt.
- `lego renew`: Revocar un certificado existente de una cuenta específica de Let's Encrypt.

Por ejemplo, para generar un certificado nuevo, usando el reto TLS [47], podremos ejecutar este comando:

Código C.7 Ejemplo de generación de un certificado HTTPS vía LEGO.

```
$ lego --tls --email user@example.com --domains mydomain.com --accept-tos --
    path ~ run
```

Una vez generado, se podrán encontrar los certificados en la carpeta `/.lego` dentro del servidor donde se ha ejecutado el comando.

C.2 Configuración del servidor Web para el uso de certificados

Para configurar el servidor Web, es necesario que las respuestas al puerto HTTPS (por defecto 443) respondan con el certificado adecuado. Para ello, hay que seguir las siguientes instrucciones según el servidor Web utilizado:

- Apache: En el virtual host de HTTPS, configurar las opciones `SSLCertificateKeyFile` y `SSLCertificateFile` con la ubicación dentro del sistema de ficheros de la clave privada y el certificado HTTPS, respectivamente. Posteriormente, reiniciar el servidor.
- NGINX: En el server block de HTTPS, configurar las opciones `ssl_certificate_key` y `ssl_certificate` con la ubicación dentro del sistema de ficheros de la clave privada y el certificado HTTPS, respectivamente. Posteriormente, reiniciar el servidor.

En el caso de que interese activar la renovación automatizada, será necesario utilizar un reto tipo DNS si se dispone de acceso a la configuración del dominio. Si no, la forma más sencilla será con un reto HTTP, requiriendo configuración adicional. Esto se debe a que, en el tipo de retos HTTP, se intentará crear un fichero

[1] Página con enlaces de descarga de la herramienta Lego: https://github.com/go-acme/lego/releases
[2] Se recomienda ejecutar el comando `lego help` para visualizar las opciones de configuración soportadas para cada comando.

con un contenido aleatorio que será verificado con el servicio de Let's Encrypt, para asegurar que se tiene control de los ficheros pertenecientes al dominio.

En el caso de Apache, esa configuración podría tener esta forma dentro del virtual host de HTTPS:

Código C.8 Ejemplo de configuración de Apache para renovación automatizada de certificados utilizando reto HTTP.

```
Alias /.well-known /etc/lego
<Directory /etc/lego>
  Require all granted
</Directory/
```

De forma adicional, para que la renovación automatizada funcione, será necesario añadir una tarea programada cada cierto tiempo. Por ejemplo, utilizando Cron, se puede activar añadiendo la siguiente línea a `/etc/crontab`:

Código C.9 Ejemplo de renovación automatizada de certificados utilizando reto HTTP vía Cron.

```
0 0 1 * * sudo lego --path /etc/lego --email user@example.com --http --http-
    timeout 30 --http.webroot /etc/lego --domains example.com renew
```

C.2.1 Comprobación

Para comprobar de manera sencilla que se ha configurado correctamente el certificado en el servidor Web, se puede usar un programa equivalente a `telnet` para comunicaciones cifradas vía TLS, `openssl s_client`.

Por ejemplo, para conectarnos con https://example.com ejecutaremos el siguiente comando, que inmediatamente nos mostrará información sobre su certificado:

Código C.10 Ejemplo de cliente HTTPS vía OpenSSL https://example.com.

```
$ openssl s_client -connect example.com:443
CONNECTED(00000005)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global
    Root CA
verify return:1
depth=1 C = US, O = DigiCert Inc, CN = DigiCert SHA2 Secure Server CA
verify return:1
depth=0 C = US, ST = California, L = Los Angeles, O = Internet Corporation for
    Assigned Names and Numbers, OU = Technology, CN = www.example.org
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=Los Angeles/O=Internet Corporation for Assigned
     Names and Numbers/OU=Technology/CN=www.example.org
   i:/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIHQDCCBiigAwIBAgIQD9B43Ujxor1NDyupa2A4/jANBgkqhkiG9w0BAQsFADBN
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5E
aWdpQ2VydCBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMTgxMTI4MDAwMDAwWhcN
MjAxMjAyMTIwMDAwWjCBpTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
```

```
aWExFDASBgNVBAcTC0xvcyBBbmdlbGVzMTwwOgYDVQQKEzNJbnRlcm5ldCBDb3Jw
b3JhdGlvbiBmb3IgQXNzaWduZWQgTmFtZXMgYW5kIE51bWJlcnMxEzARBgNVBAsT
ClRlY2hub2xvZ3kxGDAWBgNVBAMTD3d3dy5leGFtcGxlLm9yZzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANDwEnSgliByCGUZElpdStA6jGaPoCkrp9vV
rAzPpXGSFUIVsAeSdjF11yeOTVBqddF7U14nqu3rpGA68o5FGGtFM1yFEaogEv5g
rJ1MRY/d0w4+dw8JwoVlNMci+3QTuUKf9yH28JxEdG3J37Mfj2C3cREGkGNBnY80
eyRJRqzy8I0LSPTTkhr3okXuzOXXg38ugr1x3SgZWDNuEaE6oGpyYJIBWZ9jF3pJ
QnucP9vTBejMh374qvyd0QVQq3WxHrogy4nUbWw3gihMxT98wRD1oKVma1NTydvt
hcNtBfhkp8kO64/hxLHrLWgOFT/l4tz8IWQt7mkrBHjbd2XLVPkCAwEAAaOCA8Ew
ggO9MB8GA1UdIwQYMBaAFA+AYRyCMWHVLyjnjUY4tCzhxtniMB0GA1UdDgQWBBRm
mGIC4AmRp9njNvt2xrC/oW2nvjCBgQYDVR0RBHoweIIPd3d3LmV4YW1wbGUub3Jn
ggtleGFtcGxlLmNvbYILZXhhbXBsZS5lZHWCC2V4YW1wbGUubmV0ggtleGFtcGxl
Lm9yZ4IPd3d3LmV4YW1wbGUuY29tgg93d3cuZXhhbXBsZS5lZHWCD3d3dy5leGFt
cGxlLm5ldDAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMGsGA1UdHwRkMGIwL6AtoCuGKWh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNv
bS9zc2NhLXNoYTItZzYuY3JsMC+gLaArhilodHRwOi8vY3JsNC5kaWdpY2VydC5j
b20vc3NjYS1zaGEyLWc2LmNybDBMBgNVHSAERTBDMDcGCWCGSAGG/WwBATAqMCgG
CCsGAQUFBwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAgGBmeBDAEC
AjB8BggrBgEFBQcBAQRwMG4wJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2lj
ZXJ0LmNvbTBGBggrBgEFBQcwAoY6aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0U0hBMlNlY3VyZVNlcnZlckNBLmNydDAMBgNVHRMBAf8EAjAAMIIB
fwYKKwYBBAHWeQIEAgSCAW8EggFrAWkAdwCkuQmQtBhYFIe7E6LMZ3AKPDWYBPkb
37jjd80OyA3cEAAAAWdcMZVGAAAEAwBIMEYCIQCEZIG3IR36Gkj1dq5L6EaGVycX
sHvpO7dKV0JsooTEbAIhALuTtf4wxGTkFkx8blhTV+7sf6pFT78ORo7+cP39jkJC
AHYAh3W/51l8+IxDmV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFnXDGWFQAABAMA
RzBFAiBvqnfSHKeUwGMtLrOG3UGLQIoaL3+uZsGTX3MfSJNQEQIhANL5nUiGBR6g
l0QlCzzqzvorGXyB/yd7nttYttzo8EpOAHYAb1N2rDHwMRnYmQCkURX/dxUcEdkC
wQApBo2yCJo32RMAAAFnXDGWnAAABAMARzBFAiEA5Hn7Q4SOyqHkT+kDsHq7ku7z
RDuM7P4UDX2ft2Mpny0CIE13WtxJAUr0aASFYZ/XjSAMMfrB0/RxClvWVss9LHKM
MA0GCSqGSIb3DQEBCwUAA4IBAQBzcIXvQEGnakPVeJx7VUjmvGuZhrr7DQOLeP4R
8CmgDM1pFAvGBHiyzvCH1QGdxFl6cf7wbp7BoLCRLR/qPVXFMwUMzcE1GLBqaGZM
v1Yh2lvZSLmMNSGRXdx113pGLCInpm/TOhfrvr0TxRImc8BdozWJavsn1N2qdHQu
N+UBO6bQMLCD0KHEdSGFsuX6ZwAworxTg02/1qiDu7zW7RyzHvFYA4IAjpzvkPIa
X6KjBtpdvp/aXabmL95YgBjT8WJ7pqOfrqhpcmOBZa6Cg6O1l4qbIFH/Gj9hQB5I
0Gs4+eH6F9h3SojmPTYkT+8KuZ9w84Mn+M8qBXUQoYoKgIjN
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Los Angeles/O=Internet Corporation for Assigned
    Names and Numbers/OU=Technology/CN=www.example.org
issuer=/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA
---
No client certificate CA names sent
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 4643 bytes and written 322 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
   Protocol : TLSv1.2
   Cipher   : ECDHE-RSA-AES128-GCM-SHA256
   Session-ID: 8
       E8904F449263973B4D6133CFF421091CA50C60A8AC35A2E37405C9BDF9954B6
   Session-ID-ctx:
```

```
    Master-Key: 92
        CD31CE0C83611CA8A5D7452C6EB51FF57C9CB6C8FEBDEC1DE12E8057AFC20CD9C9C6DA30B9FE07E8FDA875

    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 64 c1 52 7f ea 00 09 f1-ad 85 6e 60 2c 35 39 e6 d.R.......n`,59.
    0010 - 3b df 0e c0 20 fd 4e 29-c4 dc 7a 5e 78 83 3b b9 ;... .N)..z^x.;.
    0020 - b3 ff 81 77 aa f0 bc d3-80 82 dd da 38 5d 98 8d ...w........8]..
    0030 - 5b e0 75 49 a9 61 9e 68-d7 1f 45 51 19 52 2a 6b [.uI.a.h..EQ.R*k
    0040 - 93 d7 2b 12 25 49 74 da-bc 9b 31 6c 61 81 38 c5 ..+.%It...1la.8.
    0050 - 48 dc 1b bc dd 2f 50 2a-85 fb d1 03 63 d4 cb 79 H..../P*....c..y
    0060 - 5a 44 a3 a9 d2 ea b7 2f-41 02 96 7d 96 67 2c 97 ZD...../A..}.g,.
    0070 - fc 3e 91 37 a7 b8 f4 94-6c 01 13 2e 48 70 9f 85 .>.7....l...Hp..
    0080 - 08 f3 50 d0 90 6e 9d 5d-4a 2f ea f6 40 21 3e 0e ..P..n.]J/..@!>.
    0090 - 34 3e 94 69 76 80 dc d2-6e b4 3a 31 f6 48 f4 6a 4>.iv...n.:1.H.j

    Start Time: 1574188578
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

Con esta información tenemos información útil como la siguiente:

- El servidor HTTPS de https://example.com utiliza un certificado provisto por la autoridad de certificación DigiCert.
- La organización detrás de https://example.com es la IANA.
- La clave pública tiene un tamaño de 2048 bits.
- El protocolo utilizado en esta comunicación es TLSv1.2.
- El conjunto de cifrado de la comunicación es ECDHE-RSA-AES128-GCM-SHA256: El algoritmo de intercambio de claves está basado en Diffie-Hellman (ECDHE), el algoritmo de autenticación es RSA, el algoritmo de cifrado está basado en AES y el algoritmo de autenticación de mensajes es SHA256.

Es en este momento cuando se debe introducir la petición en consola, que se observa que es idéntica al a utilizada anteriormente. Para indicar que hemos terminado utilizamos el salto de línea doble. Por ejemplo:

Código C.11 Ejemplo de petición HTTPS vía cliente de OpenSSL para obtener https://example.com.

```
GET / HTTP/1.1
Host: example.com
Accept: */*
```

Al introducirlo, obtendremos la respuesta:

Código C.12 Ejemplo de respuesta HTTPS vía cliente de OpenSSL para obtener https://example.com.

```
HTTP/1.1 200 OK
Age: 557211
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Thu, 05 May 2022 21:53:14 GMT
Etag: "3147526947+ident"
Expires: Thu, 12 May 2022 21:53:14 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (dcb/7F3B)
```

```
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256

<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "
            Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may
        use this
    domain in literature without prior coordination or asking for permission.</
        p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></
        p>
</div>
</body>
</html>
```

Apéndice D
Código fuente

El código fuente de la herramienta de configuración de HTTPS de Bitnami, de la versión que fue desarrollada como parte de esta memoria en su versión `0.1.0`, se ha publicado de forma abierta en GitHub en el siguiente enlace:

https://github.com/marcosbc/https-configuration-tool

No obstante, las nuevas versiones basadas en esa versión, no son de código abierto y no existe forma de obtener el código fuente, actualmente. La última versión disponible, a fecha de 19/07/2022, es de `1.0.0`.

D.1 Requisitos

Es necesario disponer de los siguientes programas en la máquina donde se desee construir la herramienta:

- Bash [60]: Intérprete de línea comandos del proyecto GNU. Está disponible en la práctica mayoría de sistemas operativos con el kernel Linux, y la mayoría de sistemas operativos basados en UNIX.
- VMware InstallBuilder [6]: Solución de construcción de instaladores de la empresa VMware.

D.2 Estructura

El proyecto se compone en los siguientes ficheros:

- Ficheros asociados al repositorio Git: Estos ficheros son necesarios para hospedar el proyecto en GitHub y para poder gestionar el proyecto con Git. Se corresponden a los ficheros de licencia `LICENSE`, el fichero de descripción `README.md`, y el fichero `.gitignore`.
- Ficheros de construcción: Ficheros necesarios para poder construir la herramienta desde la línea de comandos. Corresponde al fichero `build.sh`.
- Sistema de pruebas automatizado: Todos los ficheros dentro de la carpeta `tests`.
- Ficheros del instalador: Todos los demás ficheros. Corresponde a los ficheros con extensión XML, LNG, INI y ficheros de imágenes.

D.2.1 Ficheros del instalador

Fichero de proyecto principal

El instalador contiene un fichero principal, también denominado fichero de proyecto, con el nombre de `bncert.xml`. Realiza las siguientes funciones:

- Configurar todas las propiedades de configuración del instalador, como el nombre del fichero, ficheros de idioma soportados, imágenes asociadas, etc.
- Define todas las páginas del instalador, junto con todos los parámetros asociados y su configuración, y ejecuta las funciones asociadas a cada uno de ellos.

- Contiene la lista de acciones a realizar en el ciclo de vida del instalador, como por ejemplo durante la inicialización o la cancelación de una ejecución.
- Incluye los distintos componentes de InstallBuilder (alojados en un fichero diferente).

Fichero de proyecto del auto-actualizador

Para soportar la actualización, es necesario la construcción del auto-actualizador, que se incluye en la herramienta. El fichero de proyecto del auto-actualizador es `bncert-auto-updater.xml` y define los pasos para obtener la última versión del programa, y descargarla si el usuario acepta la actualización.

Nótese que se emplea el fichero `bncert-update.xml` para obtener la última versión de la herramienta, y comprobar si es necesario actualizar en caso de que la versión local sea menor. Se obtiene de la siguiente ubicación:

https://downloads.bitnami.com/files/bncert/latest/bncert-update.xml

Componentes

Los diferentes componentes soportados están alojados en ficheros distintos. Actualmente están los siguientes:

- `bncert-auto-update.xml`: El componente asociado al auto-actualizador, que lo empaqueta dentro de Bncert.
- `bncert-base-functions.xml` y `bncert-functions.xml`: Funciones comunes de la herramienta. Por ejemplo, para verificar si una instalación existente es apta para su configuración.
- `bncert-webserver-functions.xml` y `bncert-webserver-apache-functions.xml`: Funciones asociadas a la configuración del servidor Web empleado. Actualmente, solo se soporta el servidor Web Apache, pero se ha diseñado de manera modular, de forma que añadir otro servidor como NGINX sea sencillo.
- `bncert-letsencrypt-mode.xml`: Acciones, páginas de instalador y parámetros usados en caso de que el usuario necesite realizar acciones asociadas a certificados HTTPS de Let's Encrypt.
- `bncert-letsencrypt-functions.xml`: Funciones asociadas a certificados HTTPS de Let's Encrypt, como por ejemplo la renovación de un certificado existente.

D.3 Construcción

Para poder construir la herramienta, basta con ejecutar el siguiente comando en la línea de comandos:

Código D.1 Construcción de Bncert en local.

```
$ ./build.sh
Autoupdater successfully created. You can find it at

 /Applications/VMware InstallBuilder for Qt Enterprise 21.6.0/autoupdate/output
     /autoupdate-linux-x64.run
 Building HTTPS Configuration Tool linux-x64
 0% _____________ 50% _____________ 100%
 ########################################
```

Esto resultará en la generación del fichero `bncert-0.1.0-linux-x64.run` en la carpeta desde la que se ejecutó el comando anterior.

D.4 Pruebas

D.4.1 Estructura

Las pruebas se localizan dentro de la carpeta `tests` del repositorio mencionado anteriormente. Esta carpeta tiene la siguiente estructura de directorios:

- Carpeta `bin`: Contiene el binario de la herramienta `tclkit`, dependencia del sistema de pruebas automatizado.
- Carpeta `src`: Scripts necesarios para poder construir el binario `tclkit` del punto anterior.
- Carpeta `lib`: Contiene ficheros con funciones comunes del sistema de pruebas automatizado.
- Carpeta `tests`: Ubicación donde se localizan los ficheros de pruebas funcionales, de integración y unitarias, en las sub-carpetas `functional`, `integration` y `unit`, respectivamente.
- Fichero `env.tcl`: Fichero de configuración del sistema de pruebas.

D.4.2 Configuración

Para poder usar el sistema de pruebas, es necesario configurar los siguientes parámetros ubicados en el fichero `env.tcl`:

- Variable `resolvable_domain_with_www`: Dominio que apunte a la instancia desde la que se ejecutan las pruebas, que también cuenta con un subdominio `www` apuntando a ella.
- Variable `resolvable_domain_without_www`: Dominio que apunte a la instancia desde la que se ejecutan las pruebas, que no soporta un subdominio `www`.
- Variable `valid_email`: Dirección de correo electrónico válida, que se asociará a los certificados de prueba creados.

Los valores por defecto de las anteriores variables se corresponden a las que se utilizan en Bitnami.

Además, es necesario ubicar el fichero de la herramienta, `bncert-0.1.0-linux-x64.run`, en la carpeta `inputs_for_tests`.

D.4.3 Ejecución

Para ejecutar las pruebas, basta con ejecutar todos y cada uno de los ficheros pruebas con la herramienta `tclkit`.

Código D.2 Ejecución del sistema de pruebas automatizado para la herramienta Bncert.

```
$ bin/tclkit tests/unit/unattended.tcl
Launching unattended mode requires --installdir
spawn sudo /home/bitnami/projects/https-configuration-tool/tests/
    inputs_for_tests/bncert-0.2.0-linux-x64.run --dry_run 1 --mode unattended
There has been an error.
The following options were not specified and are required:
--installdir

[OK] Unattended mode requires --installdir


[OK] Process exited

Launching as unattended mode is not allowed
spawn sudo /home/bitnami/projects/https-configuration-tool/tests/
    inputs_for_tests/bncert-0.2.0-linux-x64.run --dry_run 1 --installdir /path/
    to/something --mode unattended
Unattended mode is not supported yet. Please use --mode text or --mode gui
    instead.

[OK] Unattended mode is not supported


[OK] Process exited
```

Índice de Figuras

Índice de Tablas

Índice de Códigos

Bibliografía

[1] Google. HTTPS as a ranking signal, 2014. https://developers.google.com/search/blog/2014/08/https-as-ranking-signal. Último acceso: 19/07/2022.

[2] Let's Encrypt. Let's Encrypt: Delivering SSL/TLS Everywhere, 2014. https://letsencrypt.org/2014/11/18/announcing-lets-encrypt.html. Último acceso: 19/07/2022.

[3] Navegador Web Mozilla Firefox. https://www.mozilla.org/es-ES/firefox/. Último acceso: 23/07/2022.

[4] Editor de texto Vim. https://www.vim.org/. Último acceso: 23/07/2022.

[5] Software de control de versiones distribuido Git. https://git-scm.com/. Último acceso: 23/07/2022.

[6] Herramienta VMware InstallBuilder. https://installbuilder.com/. Último acceso: 23/07/2022.

[7] Herramienta Tclkit. https://wiki.tcl-lang.org/page/Tclkit. Último acceso: 23/07/2022.

[8] Herramienta Expect. https://core.tcl-lang.org/expect/index. Último acceso: 23/07/2022.

[9] Software de hojas de cálculo Microsoft Excel. https://www.microsoft.com/en-us/microsoft-365/excel/. Último acceso: 23/07/2022.

[10] Sistema de preparación de documentos LaTeX. https://www.latex-project.org/. Último acceso: 23/07/2022.

[11] MockFlow. https://mockflow.com/. Último acceso: 23/07/2022.

[12] diagrams.net. https://diagrams.net/. Último acceso: 23/07/2022.

[13] Amazon Web Services (AWS). https://aws.amazon.com/. Último acceso: 23/07/2022.

[14] Amazon EC2. https://aws.amazon.com/ec2/. Último acceso: 23/07/2022.

[15] Amazon Route 53. https://aws.amazon.com/route53/. Último acceso: 23/07/2022.

[16] GitHub: Servicio de hospedaje de repositorios Git. https://github.com/. Último acceso: 23/07/2022.

[17] ITU. Individuals using the Internet. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Último acceso: 19/07/2022.

[18] Oliver Burkeman (The Guardian). Forty years of the internet: how the world changed for ever, 2009. https://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpanet. Último acceso: 24/07/2022.

[19] APNIC. IPv4 exhaustion. https://www.apnic.net/manage-ip/ipv4-exhaustion/. Último acceso: 19/07/2022.

[20] APNIC. Addressing 2019 (IP Addresses, IPv6), 2020. https://labs.apnic.net/?p=1288. Último acceso: 23/07/2022.

[21] RIPE. IPv6 Enabled Networks. http://v6asns.ripe.net/v/6?s=_ALL. Último acceso: 19/07/2022.

[22] Google. IPv6 Adoption. https://www.google.com/intl/en/ipv6/statistics.html. Último acceso: 19/07/2022.

[23] IETF. RFC 1034 - Domain names - Concepts and facilities, 1987. https://www.ietf.org/rfc/rfc1034.txt. Último acceso: 19/07/2022.

[24] IETF. RFC 7766 - DNS Transport over TCP - Implementation Requirements, 2016. https://datatracker.ietf.org/doc/html/rfc7766. Último acceso: 19/07/2022.

[25] CloudFlare. What are the different types of DNS server? https://www.cloudflare.com/learning/dns/dns-server-types/. Último acceso: 19/07/2022.

[26] Root Server Technical Operations Association. DNS Root Servers. https://root-servers.org/. Último acceso: 23/07/2022.

[27] CloudFlare. What is a DNS record? https://www.cloudflare.com/learning/dns/dns-records/. Último acceso: 19/07/2022.

[28] Mozilla Developer Network (MDN). Visión General Cliente-Servidor (HTTP). https://developer.mozilla.org/es/docs/Learn/Server-side/First_steps/Client-Server_overview. Último acceso: 19/07/2022.

[29] Mozilla Developer Network (MDN). Códigos de estado de respuesta HTTP. https://developer.mozilla.org/es/docs/Web/HTTP/Status. Último acceso: 19/07/2022.

[30] IANA. IANA-managed Reserved Domains. https://www.iana.org/domains/reserved. Último acceso: 19/07/2022.

[31] Wikipedia. Usage share of web browsers. https://en.wikipedia.org/wiki/Usage_share_of_web_browsers. Último acceso: 19/07/2022.

[32] Mozilla Developer Network (MDN). Blink browser layout engine. https://developer.mozilla.org/en-US/docs/Glossary/Blink. Último acceso: 19/07/2022.

[33] BBC. Microsoft's Internet Explorer losing browser share, 2010. https://www.bbc.com/news/10095730. Último acceso: 19/07/2022.

[34] StatCounter. Browser Market Share Worldwide. https://gs.statcounter.com/browser-market-share. Último acceso: 23/07/2022.

[35] StatCounter. Desktop vs Mobile vs Tablet Market Share Worldwide. https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet. Último acceso: 23/07/2022.

[36] CERN. A short history of the Web. https://home.cern/science/computing/birth-web/short-history-web. Último acceso: 19/07/2022.

[37] Wikipedia. Web server. https://en.wikipedia.org/wiki/Web_server. Último acceso: 19/07/2022.

[38] Netcraft. June 2022 Web Server Survey, 2022. https://news.netcraft.com/archives/2022/06/30/june-2022-web-server-survey.html. Último acceso: 23/07/2022.

[39] Wikipedia. Criptografía. https://en.wikipedia.org/wiki/Cryptography. Último acceso: 19/07/2022.

[40] CloudFlare. What happens in a TLS handshake? https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/. Último acceso: 19/07/2022.

[41] Wikipedia. Diffie-Hellman. https://es.wikipedia.org/wiki/Diffie-Hellman. Último acceso: 19/07/2022.

[42] Wikipedia. CA/Browser Forum. https://en.wikipedia.org/wiki/CA/Browser_Forum. Último acceso: 19/07/2022.

[43] Jari Turkia. Goodbye CAcert.org - Welcome Let's Encrypt!, 2018. https://blog.hqcodeshop.fi/archives/391-Goodbye-CAcert.org-Welcome-Lets-Encrypt!.html. Último acceso: 19/07/2022.

[44] W3Techs. Usage statistics of SSL certificate authorities for websites. https://w3techs.com/technologies/overview/ssl_certificate. Último acceso: 19/07/2022.

[45] EFF. Is Let's Encrypt the Largest Certificate Authority on the Web? https://www.eff.org/deeplinks/2016/10/lets-encrypt-largest-certificate-authority-web. Último acceso: 19/07/2022.

[46] Let's Encrypt. Rate Limits. https://letsencrypt.org/docs/rate-limits/. Último acceso: 19/07/2022.

[47] Let's Encrypt. Challenge Types. https://letsencrypt.org/docs/challenge-types/. Último acceso: 19/07/2022.

[48] Let's Encrypt. ACME Client Implementations. https://letsencrypt.org/docs/client-options/. Último acceso: 19/07/2022.

[49] Google. A secure web is here to stay, 2018. https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html. Último acceso: 19/07/2022.

[50] Let's Encrypt. Why ninety-day lifetimes for certificates?, 2015. https://letsencrypt.org/2015/11/09/why-90-days.html. Último acceso: 19/07/2022.

[51] Servidor Web Caddy. https://caddyserver.com/. Último acceso: 23/07/2022.

[52] Servidor Web Traefik. https://traefik.io/. Último acceso: 24/07/2022.

[53] Kubernetes cert-manager. https://cert-manager.io/. Último acceso: 23/07/2022.

[54] Herramienta CertBot. https://certbot.eff.org/. Último acceso: 23/07/2022.

[55] Go ACME. LEGO - Let's Encrypt client and ACME library written in Go. https://go-acme.github.io/lego/. Último acceso: 19/07/2022.

[56] Let's Encrypt. Let's Encrypt Stats. https://letsencrypt.org/stats/. Último acceso: 23/07/2022.

[57] Jacob Hoffman-Andrews (Let's Encrypt). go-acme/lego #1656: small random sleep at renewal to avoid load spikes (GitHub), 2022. https://github.com/go-acme/lego/issues/1656. Último acceso: 23/07/2022.

[58] Matthew McPherrin (Let's Encrypt). bitnami/vms #43: All bitnami instances renew certificates at the same time, causing errors (GitHub), 2022. https://github.com/bitnami/vms/issues/43. Último acceso: 23/07/2022.

[59] Go ACME. LEGO - CLI. https://go-acme.github.io/lego/usage/cli/. Último acceso: 19/07/2022.

[60] Herramienta GNU Bash. https://www.gnu.org/software/bash/. Último acceso: 23/07/2022.