Propuesta de una infraestructura segura para el monitoreo de eventos en Eduroam Latinoamérica

Javier Richard Quinto Ancieta, Andres Mijail Leiva Cochachin, José Luis Quiroz Arroyo

INICTEL-UNI, San Borja - Lima 41 – Perú

Resumen.- La gestión de cuentas de usuarios en las redes inalámbricas era un problema tanto para administradores de redes como para los usuarios en itinerancia ya que se tenía que realizar trámites previos para acceder inalámbricamente a los servicios de red de una institución en particular. Asimismo, no se garantizaba la seguridad en la confidencialidad de la información debido a que se utilizaban algoritmos de cifrado inseguros y fácilmente vulnerados como RC4 en WEP. En la actualidad existen protocolos más robustos en cuanto a la autenticación y confidencialidad de la información como 802.1X implementado en los servidores RADIUS. Actualmente existe un servicio de movilidad segura para redes académicas y de investigación llamado eduroam, el cual permite que estudiantes e investigadores de distintas instituciones puedan acceder a las redes avanzadas desde cualquier institución asociada utilizando únicamente cuentas de correo electrónico de su universidad de origen. El servicio de eduroam internacional forma parte del grupo de trabajo GEANT3 operada por TERENA. Actualmente, muchas organizaciones con eduroam utilizan servidores RADIUS que implementan 802.1X para brindar seguridad en la autenticación de sus usuarios locales e itinerantes. Para toda institución de una red académica es importante realizar el monitoreo de eventos de las autenticaciones de sus usuarios, debido a que permite tener un registro de información tales como la cantidad de accesos aceptados o rechazados de usuarios locales o itinerantes en dicha institución. Sin embargo, eduroam Latinoamérica no cuenta con un sistema de monitoreo centralizado que registre los eventos de cada institución asociada a eduroam. En este artículo se presenta un escenario compuesto por 2 servidores RADIUS que representan a 2 instituciones, 2 servidores RADIUS federados que representan a 2 países y un servidor RADIUS confederado. Cada uno de los servidores federados envían sus logs hacia a un servidor rsyslog central el cual, se encarga de realizar un análisis sintáctico de los archivos de logs de cada servidor. La infraestructura propuesta es eficiente y rentable debido a que utiliza freeradius, que es software libre, y además segura ya que utiliza el protocolo TLS para el proceso de envío de logs. Asimismo es escalable porque permite incorporar fácilmente más servidores RADIUS según el número de países y de instituciones. Existe un sistema de reportes de eventos de autenticación para Eduroam Europa llamado F-Ticks cuyo funcionamiento se basa en el monitoreo de eventos mediante logs que son enviados hacia un servidor syslog central en el cual se genera reportes estadísticos. A diferencia de F-Ticks, nuestro sistema de monitoreo utiliza rsyslog sobre TLS garantizando la seguridad de los registros enviados al servidor rsyslog central. Asimismo, nuestro sistema genera estadísticas diarias que muestran las cantidades de accesos aceptados y fallidos en gráficos de series de tiempo. Igualmente, muestra la procedencia de las consultas según el país y la institución que autoriza el acceso, a su vez genera un reporte con los nombres de usuarios tanto aceptados como fallidos en cada servidor RADIUS.

1. Introducción

El objetivo de nuestro trabajo es dar una propuesta de una infraestructura segura de monitoreo de eventos para eduroam Latinoamérica. Por default, el protocolo de autenticación y autorización que permite a los usuarios acceder a una red inalámbrica de manera segura es RADIUS y eduroam depende de éste protocolo para el roaming de los usuarios académicos hacia redes avanzadas. Los reportes del monitoreo actual en eduroam Latinoamérica no permite tener una gestión segura de cuantos usuarios se autentican hacia las redes académicas en un periodo de tiempo determinado.

Debido a los problemas de los reportes de monitoreo de estadísticas usando el servidor virtual status y al formato común de los logs, los reportes de monitoreo de eventos son complicados de determinar. Si usamos los reportes de estadísticas del paquete freeradius, tenemos el problema de desaparición del reporte de eventos cada vez que reiniciamos el demonio del servidor RADIUS, y si usamos los logs del paquete freeradius, la información que nos brinda por cada evento de autenticación no es suficiente para poder determinar el tipo de conexión, institución visitada, país visitado y el nombre del usuario que accede al sistema de eduroam-la.

Freeradius es un software altamente configurable y de alto rendimiento, soporta muchos lenguajes de programación como Perl, Python, etc. Éste paquete está construida sobre módulos externos, estos módulos son totalmente configurables. Sin embargo la programación de dichos módulos no son muy fáciles de manejar y desplegar en las federaciones de eduroam-la.

Por otro lado, el uso de un servidor syslog centralizado permite obtener, en un reporte, los eventos de autenticación a eduroam. Syslog cuenta con parámetros que permiten obtener información por separado, a éstos se conocen como facility y priority, ellos permiten hacer reportes de los logs de manera ordenada. Sin embargo, los reportes de los logs del Syslog viajan en texto claro, éstos logs pueden ser fácilmente obtenidos usando sensores de monitoreo, como wireshark. En la figura 1 se puede observar un ejemplo de la captura de un paquete syslog en texto claro.

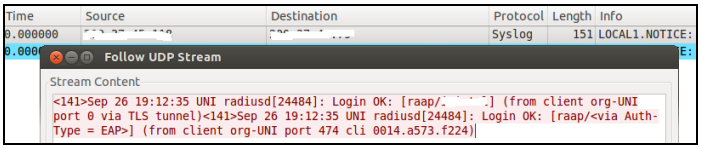


Figura 1. Captura de un paquete syslog en claro

En el presente artículo, se presenta una propuesta de implementación de un sistema de reportes de monitoreo para eduroam-la usando los atributos del paquete freeradius y el módulo linelog del mismo.

2. RADIUS y sistema de gestión de acceso usando AAA

Proceso AAA usando paquetes RADIUS

El modelo AAA fue desarrollado después de la creación del RADIUS con la finalidad de crear un estándar en los métodos de autenticación y autorización para la validación de los usuarios a la red. Los servidores RADIUS utilizan el modelo AAA como framework, existiendo otros protocolos que usan este modelo, por ejemplo Tacacs de Cisco.

El uso más general del AAA es en escenarios de autenticación en donde es necesario centralizar las consultas de acceso y llevar la cuenta de los eventos en un solo servidor y poder ser administrado por éste.

El modelo AAA se basa en 3 aspectos fundamentales: autenticación, autorización y contabilidad. La autenticación es el

proceso en donde el usuario envía sus credenciales a un cliente RADIUS para su posterior acceso a la red. Dichas credenciales podrían ser de diversos tipos (usuario y clave, certificados digitales) usando algoritmos de cifrado (PAP, CHAP) o un protocolo extensible de autenticación (EAP). También indica el protocolo a usar. La autorización define el tipo de acceso a la red a la cual el usuario debe conectarse, para ello se definen una serie de políticas para los usuarios. La contabilidad es más que tener un estado de cuentas de cada usuario, existe una variedad de aplicaciones que también lo definen como por ejemplo: auditoria, asignación de costos y los análisis de tendencias. En la figura 2 se observa un diagrama de red inalámbrica con soporte 802.1X y AAA.

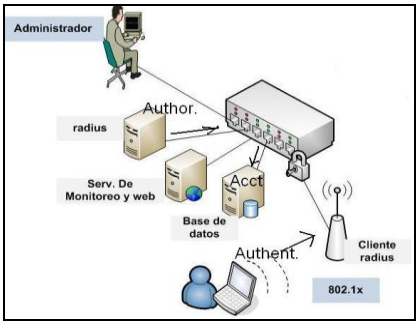


Figura 2. Escenario 802.1X y AAA

Los tipos de paquetes enviados en un proceso AAA utilizando RADIUS contienen valores predefinidos para diversos eventos de autenticación y contabilidad. Cada valor predefinido contiene una serie de atributos en un par Valor-Atributo (AVPs) desde un cliente a un servidor RADIUS. Los atributos limitan que tipo de paquete debe ser enviado en el proceso de autenticación y contabilidad.

En el proceso de autenticación, existen 10 tipos de paquetes RADIUS que son fundamentales (RFC 2865) entre los más usados son Access-request, Access-challenge, Access-accept, Access-reject. Para el proceso de contabilidad existen solo 7 tipos de paquetes RADIUS que son fundamentales (RFC 2866) entre los más usados son Accounting-request, Accounting-response, estos 17 tipos de paquetes se diferencian por un código en el formato del paquete RADIUS.

La RFC 1865 muestra una tabla del total de atributos para el proceso de autenticación y un valor aleatorio de 1 byte en el campo identificador por cada tipo de paquete, éste último otorga seguridad a un paquete RADIUS dificultando algún tipo de ataque por clonación de paquetes. Para esto existe dos tipos de paquete llamado Auth-Duplicate-Requests y Acct-Duplicate-Requests que detecta cualquier intento de duplicidad de paquete mandando mensajes de alerta al RADIUS usando un puerto definido por el administrador, también existen los paquetes RADIUS mal formados que se originan debido a un incorrecto shared-secret, así también existen los paquetes inválidos y los paquetes rechazados tanto para la autenticación y contabilidad en un proceso AAA.

Para mejorar la seguridad, el atributo User-Password solo es enviado en el tipo de paquete Access-request y su valor es cifrado durante la autenticación usando Hash MD5 [11], su longitud está en el rango de 18 a 130 bytes del tipo String (cadena de texto).

Otra medida de seguridad es el máximo número de atributos permitidos en un paquete RADIUS, si éste valor es muy pequeño entonces los paquetes RADIUS no serán aceptados, si éste valor es muy grande entonces facilita al atacante para poder enviar más atributos de lo permitido siendo esto una vulnerabilidad en el paquete RADIUS. El valor máximo de atributos permitido en un paquete RADIUS es 200. Otro problema de seguridad es el valor reject_delay, lo que significa un retardo en los paquetes rechazados, si éste valor es 0, entonces es vulnerable a ataques de denegación de servicio o ataques de fuerza bruta, ya que estos pueden enviar varios paquetes de tipo reject sobre cargando al servidor RADIUS, para un valor reject_delay muy grande, entonces el servidor RADIUS procesaría más tiempo dicha consulta no siendo eficaz para la seguridad en el servidor.

3. Atributos

Los atributos forman parte del formato de un paquete RADIUS y su función es llevar información específica del proceso de autenticación en un sistema 802.1X. Los atributos pueden aparecer en cada tipo de paquete RADIUS, dentro de un campo de longitud mínima igual a dos bytes.

En el presente trabajo, se ha realizado un estudio de los atributos usados por un paquete RADIUS cada vez que existe una autenticación hacia una red inalámbrica con eduroam. Éste estudio consiste en la extracción de ciertos atributos definidos en un archivo de texto y procesados en lenguaje perl, el resultado final es reportado en un sistema web para el monitoreo global del sistema de eduroam para Latinoamérica.

A continuación se define los atributos en tres tipos según la ubicación en donde el usuario se encuentre.

Roaming local:

La tabla roaming local muestran los atributos más resaltantes en cuanto a la autenticación de un usuario conectado a la red inalámbrica de su propia institución. Estos atributos se definen como variables del sistema y son de dos tipos: variable y constante.

Entre los atributos “variables” tenemos al “REALM” que define al dominio de la institución proveedora del servicio (SP), “User-eduroam” que define al nombre del usuario que se encuentra actualmente asociado a la red inalámbrica, “VISINST” que define el nombre de la institución visitada y el “CSI” que define la mac-adreess del usuario móvil. En cuanto a los atributos “constante” tenemos al “VISCOUNTRY” que define el dominio país del usuario asociado y al atributo “RESULT” que define el resultado del acceso a la red WIFI.

ATRIBUTOS	DEFINICION	TIPO	SIGNIFICADO
REALM	%{Realm}	Variable	Dominio
User-eduroam	%{User-Name}	Variable	Nombre de usuario
VISINST	%{Client-Shortname}	Variable	Institución visitada
VISCOUNTRY	PE	Constante	País visitado
CSI	%{Calling-Station-Id}	Variable	Dirección MAC
RESULT	OK	Constante	Resultado

Tabla1. Roaming local

Roaming nacional:

La tabla roaming nacional muestran los atributos más resaltantes en cuanto a la itinerancia de un usuario cuando éste visita otra institución dentro de su propio país.

ATRIBUTOS	DEFINICION	TIPO	SIGNIFICADO
REALM	%{Realm}	Variable	Dominio
User-eduroam	%{User-Name}	Variable	Nombre de usuario
VISINST	%{Client-Shortname}	Variable	Institución visitada
VISCOUNTRY	PE	Constante	País visitado
CSI	%{Calling-Station-Id}	Variable	Dirección MAC
RESULT	OK	Constante	Resultado

Tabla2. Roaming nacional

Estos atributos son los mismos de la tabla anterior, pero la diferencia está en el resultado que muestra cada uno de los atributos.

Roaming internacional:

La tabla roaming internacional muestran los atributos más resaltantes en cuanto a la itinerancia de un usuario de una institución cuando éste visita otras instituciones fuera de su país de origen.

ATRIBUTOS	DEFINICION	TIPO	SIGNIFICADO
REALM	%{Realm}	Variable	Dominio
VISCOUNTRY	%{Client-Shortname}	Variable	País visitado
CSI	%{Calling-Station-Id}	Variable	Dirección MAC
RESULT	OK	Constante	Resultado

Tabla3. Roaming internacional

4. Esquema del mecanismo de monitoreo

En la figura 3 se muestra el esquema de mecanismo de monitoreo propuesto en el artículo. En éste esquema se observa que después que un servidor de logs central reciba los eventos de autenticación, éste procesa los logs para su filtrado y extracción de atributos, luego es almacenado en una base de datos MySQL y mostrados en un sistema Web para los reportes del monitoreo.

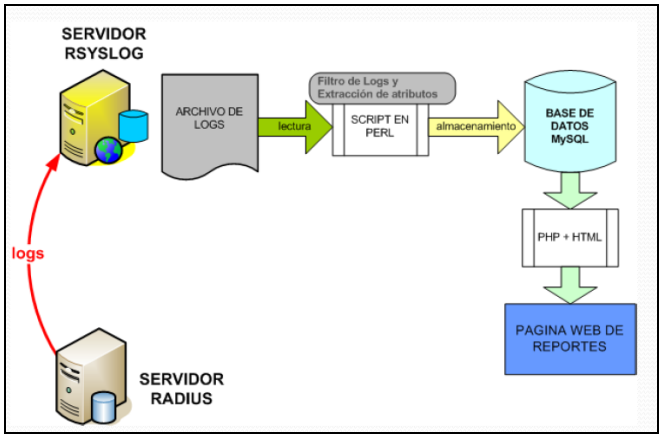


Figura 3. Mecanismo de monitoreo para eduroam-la

5. Monitoreo de la base de datos

Para el monitoreo de eduroam en una base de datos se han agrupado de manera gráfica dos regiones para identificar las entidades generales y entidades de monitoreo la cual se visualizará en la figura 4. Así la región de identidades generales mostrará de manera gráfica que por cada federación conectada a eduroam se tendrán muchas instituciones que dependen de ella y cada institución tendrá muchos servicios y usuarios a su cargo. Las entidades de monitoreo registrarán los eventos de los usuarios en el uso de la red eduroam, éste modelo de datos fue diseñado con una herramienta llamado DBDesigner4 usando software libre.

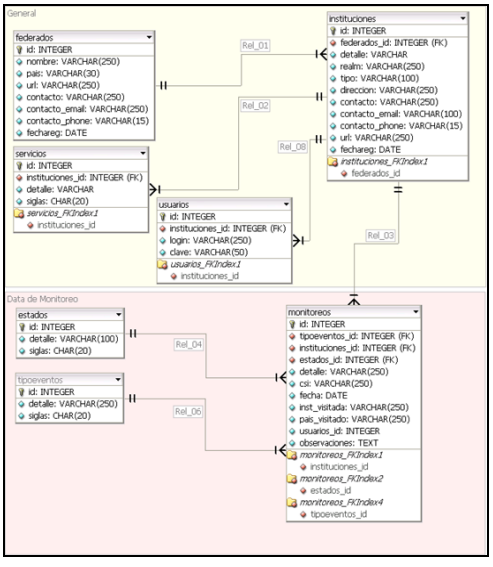


Figura 4. Modelamiento de la base de datos

6. Almacenamiento en la base de datos

En la figura 5 se observa la propuesta de un esquema de servidores de logs distribuidos en dos niveles.

El primer nivel es el federado, en el que cada NREN almacenará los eventos de autenticación local de cada institución que las pertenece, estos datos son guardados en un archivo de nombre radius-locales-logsec.log, luego son procesados por un script en perl resultando el archivo script-eduroam-locales.pl, éste nivel también almacena los logs de roaming de los usuarios visitantes, estos datos son guardados en el archivo radius-federado-logsec.log, luego son procesados por el script script-eduroam-nac.pl, éste último script es enviado al servidor de log central latinoamericano.

El segundo nivel es el confederado, este servidor de logs solamente recibirá los logs de las autenticaciones realizadas por los usuarios que visitan otras federaciones y requieran acceder a eduroam. Todos estos datos serán procesados por un script en perl de nombre script-eduroam-int.pl para luego ser almacenados en una página web con APACHE/PHP.

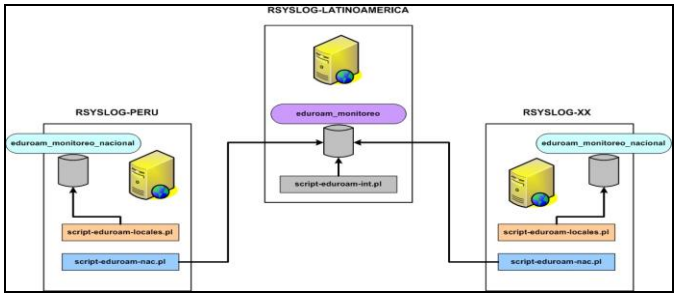


Figura 5. Esquema de almacenamiento de datos

7. Mecanismo de monitoreo usando el módulo linelog

El paquete freeradius cuenta con distintos módulos de programación, estos módulos del sistema realizan instrucciones externas al servidor para la ejecución de una determinada tarea. Existe un módulo especial llamado "linelog", éste módulo logeará, por cada autenticación de un usuario, una línea de texto a un archivo determinado. Estas líneas de respuesta pueden ser dinámicamente expandidas. La propuesta de éste artículo es usar un servidor syslog centralizado que almacene, en un archivo determinado, los mensajes de autenticación de los usuarios de eduroam-la.

En el cuadro siguiente se observa la configuración del módulo linelog propuesto.

```
linelog Logsec {
filename = syslog
format = ""
reference = "Logsec.%{%{reply:Packet-Type}:-format}"
Logsec {
Access-Accept = "LOGSEC/eduroam-la/1.0#REALM=%{Realm}#User-
eduroam=%{Stripped-User-Name}#VISINST=%{Client-
Shortname}#VISCOUNTRY=PE#CSI=%{Calling-Station-Id}#RESULT=OK"

Access-Reject = "LOGSEC/eduroam-la/1.0#REALM=%{Realm}#User-
eduroam=%{Stripped-User-Name}#VISINST=%{Client-
Shortname}#VISCOUNTRY=PE#CSI=%{Calling-Station-Id}#RESULT=FAIL"
}
}
```

Para lograr esto, es necesario configurar al servidor freeradius de un modo determinado, lo cual permita enviar los logs de autenticación a un servidor rsyslog determinado. En los parámetros de configuración se debe configurar el número IP y el puerto TCP con el cual los logs serán enviados desde el servidor RADIUS al servidor de Logs central. En nuestro caso usaremos el puerto 10514 TCP y usando la facility "**local1**" y priority **info.**

En la figura 6 se observa un escenario de dos servidores RADIUS. Estos servidores envían sus logs a un servidor Rsyslog centralizado.

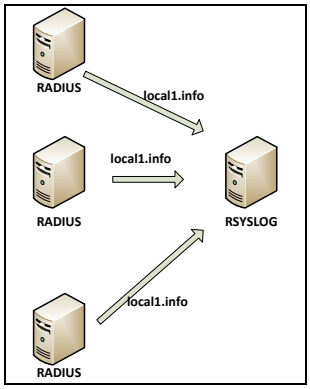


Figura 6. Jerarquía de servidores Rsyslog

En el cuadro debajo se observa las líneas de configuración que tendrá cada servidor RADIUS para activar su sistema de monitoreo.

```
log {
      destination = syslog
      file = ${logdir}/radius.log
      syslog_facility = local1
      stripped_names = yes
      auth = yes
      auth_badpass = yes
      auth_goodpass = yes
      msg_goodpass = "Usuario aceptado:  %{User-Name}"
      msg_badpass = "Usuario rechazado: %{User-Name}"
}
```

8. Mecanismo de seguridad usando el servidor Rsyslog

Ante la necesidad de tener un servidor de logs centralizado y seguro, se ha optado por cifrar los mensajes de los logs en la red, logrando así la confidencialidad de la información mediante el uso del protocolo de seguridad de la capa de transporte (TLS).

Los servidores de logs usados actualmente no cuentan con un mecanismo de seguridad que nos permitan cifrar las informaciones de logs, estos con lleva a los administradores de redes usar otros mecanismos que permitan proteger dicha información, una solución ante estos problemas es el uso de "**stunnel**", sin embargo esta solución carece de ciertas perdidas de mensajes de logs en su transmisión y la falta de fiabilidad en las transmisiónes TCP.

Para lograr establecer un cifrado en los logs, es necesario usar una transmisión confiable como TCP y el uso de controladores como NetStream tanto para el cliente como para el servidor Rsyslog y el controlador GTLS para usarlo con el paquete GNUTLS. Por lo tanto, en cada servidor RADIUS es necesario la instalación de los paquetes **rsyslog-gnutls** y **gnutls-bin**.

Para lograr una mejor confidencialidad de la información, es necesario la creación de una autoridad certificadora X509 usando los controladores GTLS, luego éste servidor garantizará a los servidores RADIUS que la información de sus reportes viajaran de modo seguro. En la figura 7 se observa un esquema de llaves digitales que permitirán enviar nuestro logs de forma segura a un servidor centralizado.

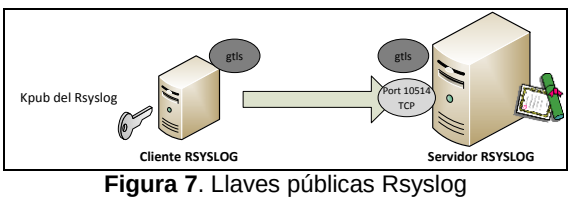


Figura 7. Llaves públicas Rsyslog

Luego, para usar los controladores gtls y tcp, necesitamos agregar los módulos respectivos en el archivo de configuración principal del RSYSLOG y por último, dar la ruta exacta de los certificados alojados en el servidor. En el cuadro siguiente se observa el archivo de configuración (/etc/rsyslog.conf).

```
$ModLoad imuxsock
$ModLoad imklog
# Modulo GTLS
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /llaves/ca.pem
$DefaultNetstreamDriverCertFile /llaves/rsyslog.inictel-uni.edu.pe.crt.pem
$DefaultNetstreamDriverKeyFile /llaves/rsyslog.pem
$ModLoad imtcp
$InputTCPServerStreamDriverMode 1
$InputTCPServerStreamDriverAuthMode anon
$InputTCPServerRun 10514
```

9. RESULTADOS Y DISCUSIÓN

Las pruebas de laboratorio se realizó en el Area de Conmutación y Transmisión del INICTEL-UNI, se usó máquinas virtuales en debían y la infraestructura de red está directamente conectada a la Red Académica Peruana (RAAP) y a CLARA. Los resultados de las pruebas en el monitoreo de los servidores radius en eduroam fueron los siguientes:

- Para las autenticaciones locales con éxito:

```
LOGSEC/eduroam-la/1.0#REALM=inictel-uni.edu.pe#User-eduroam=jquinto#VISINST=ap-INICTEL-UNI#VISCOUNTRY=PE#CSI=E0-B9-A5-97-A4-64#RESULT=OK
```

- Para las autenticaciones locales fallidas:

```
LOGSEC/eduroam-la/1.0#REALM=inictel-uni.edu.pe#User-eduroam=jquispe#VISINST=ap-INICTEL-UNI#VISCOUNTRY=PE#CSI=00-14-A5-65-F2-24#RESULT=FAIL
```

En la figura 8 se observa el escenario de monitoreo real en el cual el servidor radius del INICTEL-UNI enviará sus logs al servidor de logs RSYSLOG-Perú oficial de la RAAP mediante una conexión cifrada usando TLS.

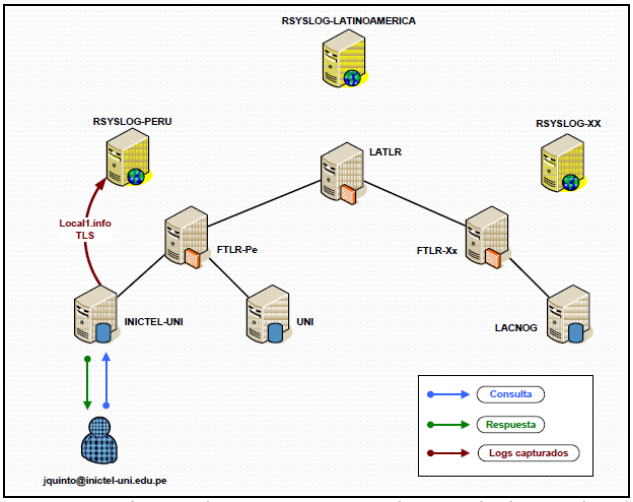


Figura 8. Monitoreo de eventos para eduroam-la (Autenticación Local)

En la figura 9 se observa los reportes de monitoreo del servidor radius institucional del INICTEL-UNI.

CONFIGURACION DEL REPORTE

Ingresar Fecha:	Mes: Sep Dia: 26
Ingresar atributo:	todo
Ingresar Tipo de Servidor:	INICTEL-UNI (INICTEL-UNI, UNI)

Generar Reporte

REPORTE INICTEL-UNI

Fecha: Sep 26

TOTAL ACEPTADOS:	90
TOTAL FALLIDOS:	0

REPORTE DE REALMS

ACEPTADOS	**Cantidad**
inictel-uni.edu.pe	90

RECHAZADOS	**Cantidad**
Ninguno	0

REPORTE DE USUARIOS

ACEPTADOS	**Cantidad**
raap	79
aleiva	9
ddiaz	1
jquinto	1

RECHAZADOS	**Cantidad**
Ninguno	0

REPORTE DE CSI

ACEPTADOS	**Cantidad**
66-66-77-77-88-88	67
380a.9426.49c3	8
78d6.f064.79d4	8
78-D6-F0-64-79-D4	4
0014.a573.f224	1
0022.fae3.3dfe	1
38-0A-94-26-49-C3	1

RECHAZADOS	**Cantidad**
Ninguno	0

Figura 9. Reportes de monitoreo del servidor radius del INICTEL-UNI

En la figura 10 se observa el escenario de monitoreo real en el cual el servidor federado de la RAAP enviará sus logs al servidor de logs RSYSLOG-Perú oficial de la RAAP mediante una conexión cifrada usando TLS.

- Para las autenticaciones remotas con éxito

LOGSEC/eduroam-la/1.0#REALM=**lacnog.edu.xx**#User-eduroam=**raap@uni.edu.pe**#VISINST=**org-INICTEL-UNI**#VISCOUNTRY=**PE**#CSI=**0014.a573.f224**#RESULT=**OK**

- Para las autenticaciones remotas fallidas

LOGSEC/eduroam-la/1.0 #REALM=**lacnog.edu.xx**#User-eduroam=**raap@uni.edu.pe**#VISINST=**org-INICTEL-UNI**#VISCOUNTRY=**PE**#CSI=**0014.a573.f224**#RESULT=**FAIL**

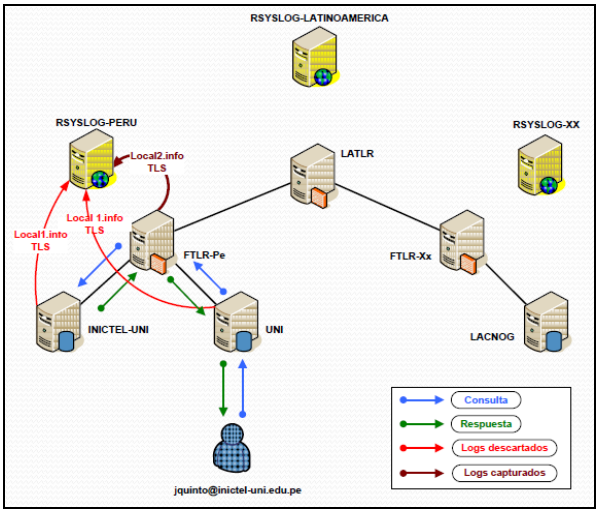


Figura 10. Monitoreo de eventos para eduroam-la (Roaming nacional)

En la figura 11 se observa los reportes de monitoreo del servidor federado de la Red Académica Peruana (RAAP)

CONFIGURACION DEL REPORTE

Ingresar Fecha:	Mes: Sep Dia: 26
Ingresar atributo:	todo
Ingresar Tipo de Servidor:	INICTEL-UNI (INICTEL-UNI, UNI)

Generar Reporte

REPORTE DE ROAMING NACIONAL EN INICTEL-UNI

Fecha: Sep 26

TOTAL ACEPTADOS:	0
TOTAL FALLIDOS:	8

REPORTE DE REALMS VISITANTES A INICTEL-UNI

ACEPTADOS	**Cantidad**
Ninguno	0

RECHAZADOS	**Cantidad**
uni.edu.pe	8

REPORTE DE USUARIOS VISITANTES EN INICTEL-UNI

ACEPTADOS	**Cantidad**
Ninguno	0

RECHAZADOS	**Cantidad**
raap@uni.edu.pe	5
jquinto@uni.edu.pe	3

REPORTE DE CSI

ACEPTADOS	**Cantidad**
Ninguno	0

RECHAZADOS	**Cantidad**
	8

Figura 11. Reportes de monitoreo del servidor federado de la RAAP

En la figura 12 se observa el escenario de monitoreo real en el cual el servidor federado de la RAAP enviará sus logs al servidor de logs RSYSLOG propuesto para CLARA mediante una conexión cifrada usando TLS.

- Para las autenticaciones remotas con éxito en el confederado.

LOGSEC/eduroam-la/1.0 #REALM=**lacnog.edu.xx**#VISCOUNTRY=**org-FTLR-Pe**#CSI=**00-14-A5-73-F2-24**#RESULT=**OK**

- Para las autenticaciones remotas fallidas en el confederado.

LOGSEC/eduroam-la/1.0 #REALM=**lacnog.edu.xx**#VISCOUNTRY=**org-FTLR-Pe**#CSI=**00-14-A5-73-F2-24**#RESULT=**FAIL**

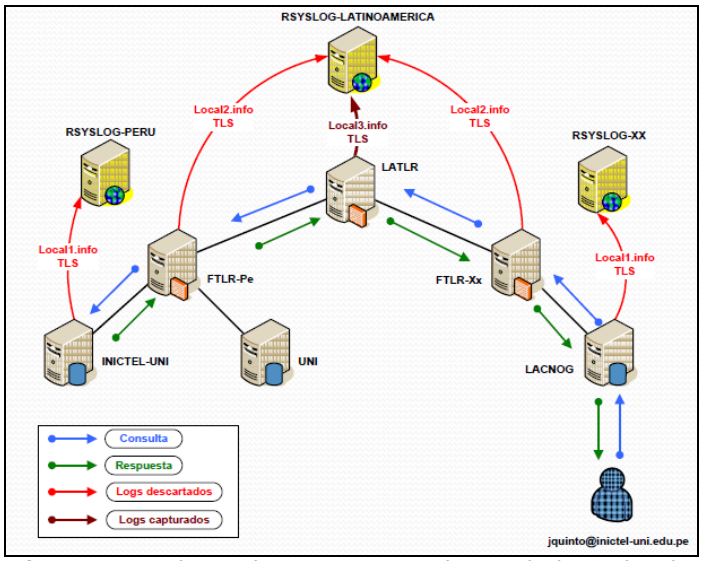
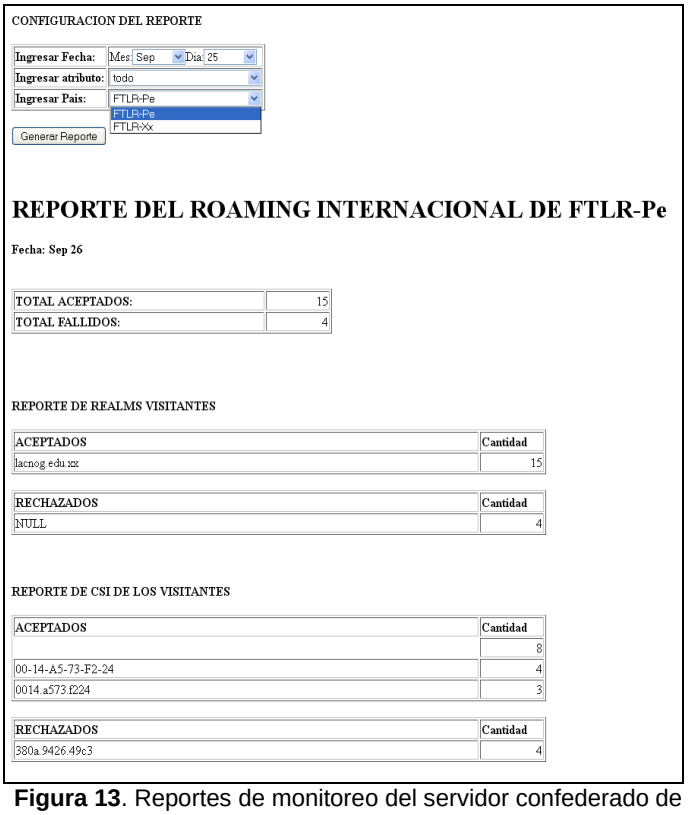


Figura 12. Monitoreo de eventos para eduroam-la (Roaming de federaciones)

En la figura 13 se observa los reportes de monitoreo del servidor radius institucional del INICTEL-UNI



CONFIGURACION DEL REPORTE

Ingresar Fecha: Mes: Sep Dia: 25
Ingresar atributo: todo
Ingresar Pais: FTLR-Pe
FTLR-Pe
FTLR-Xx
Generar Reporte

REPORTE DEL ROAMING INTERNACIONAL DE FTLR-Pe

Fecha: Sep 26

TOTAL ACEPTADOS:	15
TOTAL FALLIDOS:	4

REPORTE DE REALMS VISITANTES

ACEPTADOS	Cantidad
lacnog.edu.xx	15

RECHAZADOS	Cantidad
NULL	4

REPORTE DE CSI DE LOS VISITANTES

ACEPTADOS	Cantidad
	8
00-14-A5-73-F2-24	4
0014.a573.f224	3

RECHAZADOS	Cantidad
380a.9426.49c3	4

Figura 13. Reportes de monitoreo del servidor confederado de CLARA

10. CONCLUSIONES

En este artículo, se presenta el análisis de los atributos usados por los usuarios al momento de autenticarse a una red con eduroam y la protección de estos atributos mediante una conexión cifrada usando TLS. Se estudió la situación actual del monitoreo de eduroam en Latinoamérica y los problemas que ocurrían cuando se usaban otros mecanismos de logs como stunnel y openvpn. También se analizó sobre la seguridad de los logs al ser trasportados a un servidor de Rsyslog centralizado. Por último, se analizan y exploran las características de los atributos usados en el paquete RADIUS, su procesamiento y filtrado de los atributos más importantes y su almacenamiento en una base de datos MySQL, este resultado es mostrado en un sistema Web para su posterior monitoreo y control de la cantidad de usuarios que se autentican a eduroam por un periodo de tiempo.