

Configuración de ThreatGrid RADIUS sobre autenticación DTLS para la consola y el portal OAdmin

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe la función de autenticación RADIUS (servicio de usuario de acceso telefónico de autenticación remota) introducida en la versión 2.10 de ThreatGrid (TG). Permite a los usuarios iniciar sesión en el portal de administración, así como en el portal de consola con las credenciales almacenadas en el servidor de autenticación, autorización y contabilidad (AAA).

En este documento encontrará los pasos necesarios para configurar la función.

Prerequisites

Requirements

- ThreatGrid versión 2.10 o superior
- Servidor AAA que admite la autenticación RADIUS sobre DTLS (draft-ietf-radext-dtls-04)

Componentes Utilizados

- Appliance ThreatGrid 2.10
- Identity Services Engine (ISE) 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

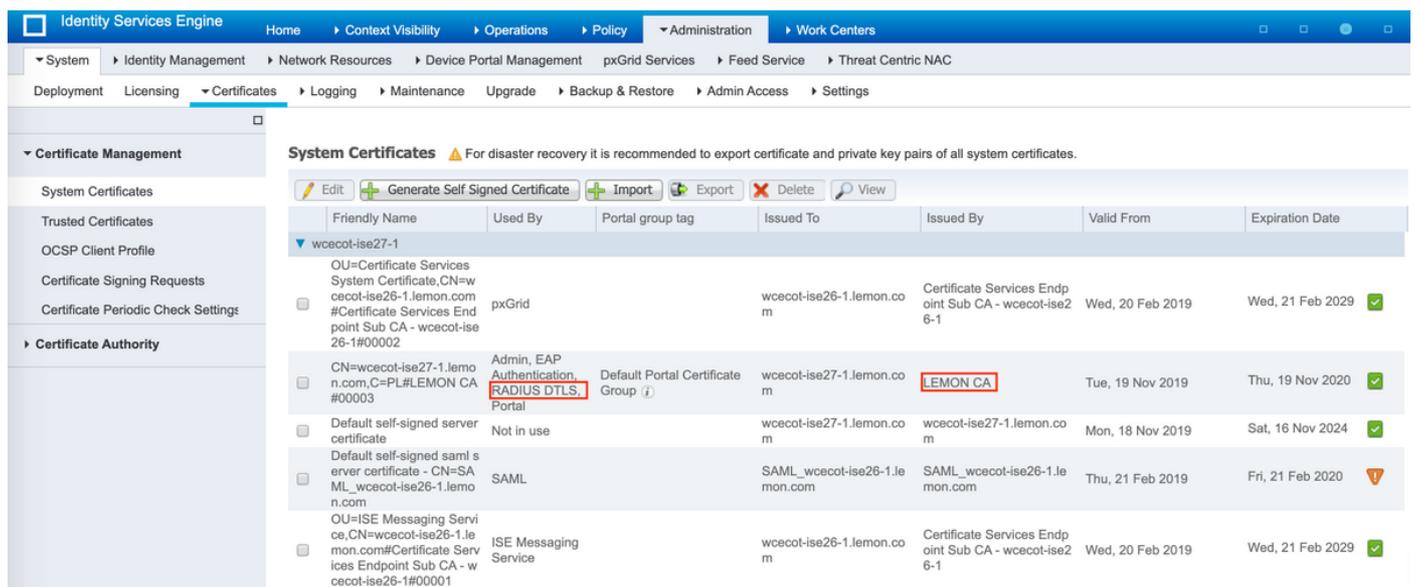
Esta sección proporciona instrucciones detalladas sobre cómo configurar ThreatGrid Appliance e ISE para la función de autenticación RADIUS.

Nota: Para configurar la autenticación, asegúrese de que se permite la comunicación en el puerto UDP 2083 entre la interfaz ThreatGrid Clean y el nodo de servicio de políticas de ISE (PSN).

Configuración

Paso 1. Preparar el certificado de ThreatGrid para la autenticación.

RADIUS sobre DTLS utiliza la autenticación de certificados mutua, lo que significa que se necesita el certificado de Autoridad de Certificación (CA) de ISE. Primero verifique qué certificado DTLS RADIUS firmado por CA:



Identity Services Engine Administration > System > Certificates > System Certificates

System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
wcecot-ise27-1						
OU=Certificate Services System Certificate,CN=wcecot-ise26-1.lemmon.com#Certificate Services Endpoint Sub CA - wcecot-ise26-1#00002	pxGrid		wcecot-ise26-1.lemmon.com	Certificate Services Endpoint Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029
CN=wcecot-ise27-1.lemmon.com,C=PL#LEMON CA#00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wcecot-ise27-1.lemmon.com	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 2020
Default self-signed server certificate	Not in use		wcecot-ise27-1.lemmon.com	wcecot-ise27-1.lemmon.com	Mon, 18 Nov 2019	Sat, 16 Nov 2024
Default self-signed saml server certificate - CN=SAML_wcecot-ise26-1.lemmon.com	SAML		SAML_wcecot-ise26-1.lemmon.com	SAML_wcecot-ise26-1.lemmon.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020
OU=ISE Messaging Service,CN=wcecot-ise26-1.lemmon.com#Certificate Services Endpoint Sub CA - wcecot-ise26-1#00001	ISE Messaging Service		wcecot-ise26-1.lemmon.com	Certificate Services Endpoint Sub CA - wcecot-ise26-1	Wed, 20 Feb 2019	Wed, 21 Feb 2029

Paso 2. Exportar el certificado de CA de ISE.

Vaya a **Administration > System > Certificates > Certificate Management > Trusted Certificates**, localice la CA, seleccione **Export** como se muestra en la imagen y guarde el certificado en el disco para más adelante:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Trusted Certificates

Edt Import Export Delete View Show All

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Tue, 13 May 20...
Cisco CA Manufacturing	Disabled	Endpoints Infrastructure AdminAuth	6A 69 67 83 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May 20...
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2025
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20...
Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco Root CA 2048	Disabled	Endpoints Infrastructure AdminAuth	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 20...
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Mon, 10 Aug 20...
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...
Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20...
Cisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXIC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2023
Default self-signed server certificate	Enabled	Endpoints Infrastructure AdminAuth	5C 6E B6 16 00 00 ...	wccot-ise26-1.lemo...	wccot-ise26-1.lemo...	Thu, 21 Feb 2019	Fri, 21 Feb 20...
DigiCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert root CA	Enabled	Endpoints Infrastructure AdminAuth	02 AC 5C 26 6A 0B...	DigiCert High Assurance...	DigiCert High Assurance...	Fri, 10 Nov 2006	Mon, 10 Nov 20...
DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure AdminAuth	04 E1 E7 A4 DC 5C...	DigiCert SHA2 High Ass...	DigiCert High Assurance...	Tue, 22 Oct 2013	Sun, 22 Oct 20...
DoflamingoCA_ec.crt	Enabled	Endpoints Infrastructure AdminAuth	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20...
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF 80 80 D6 A3...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 20...
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 20...
LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 20...

Paso 3. Agregue ThreatGrid como dispositivo de acceso a la red.

Vaya a **Administration > Network Resources > Network Devices > Add** para crear una nueva entrada para TG e introduzca el **Name**, la **dirección IP** de la interfaz Clean y seleccione **DTLS Required** como se muestra en la imagen. Haga clic en **Guardar** en la parte inferior:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > ksec-threatgrid02-clean

Network Devices

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

DNS Name

General Settings

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

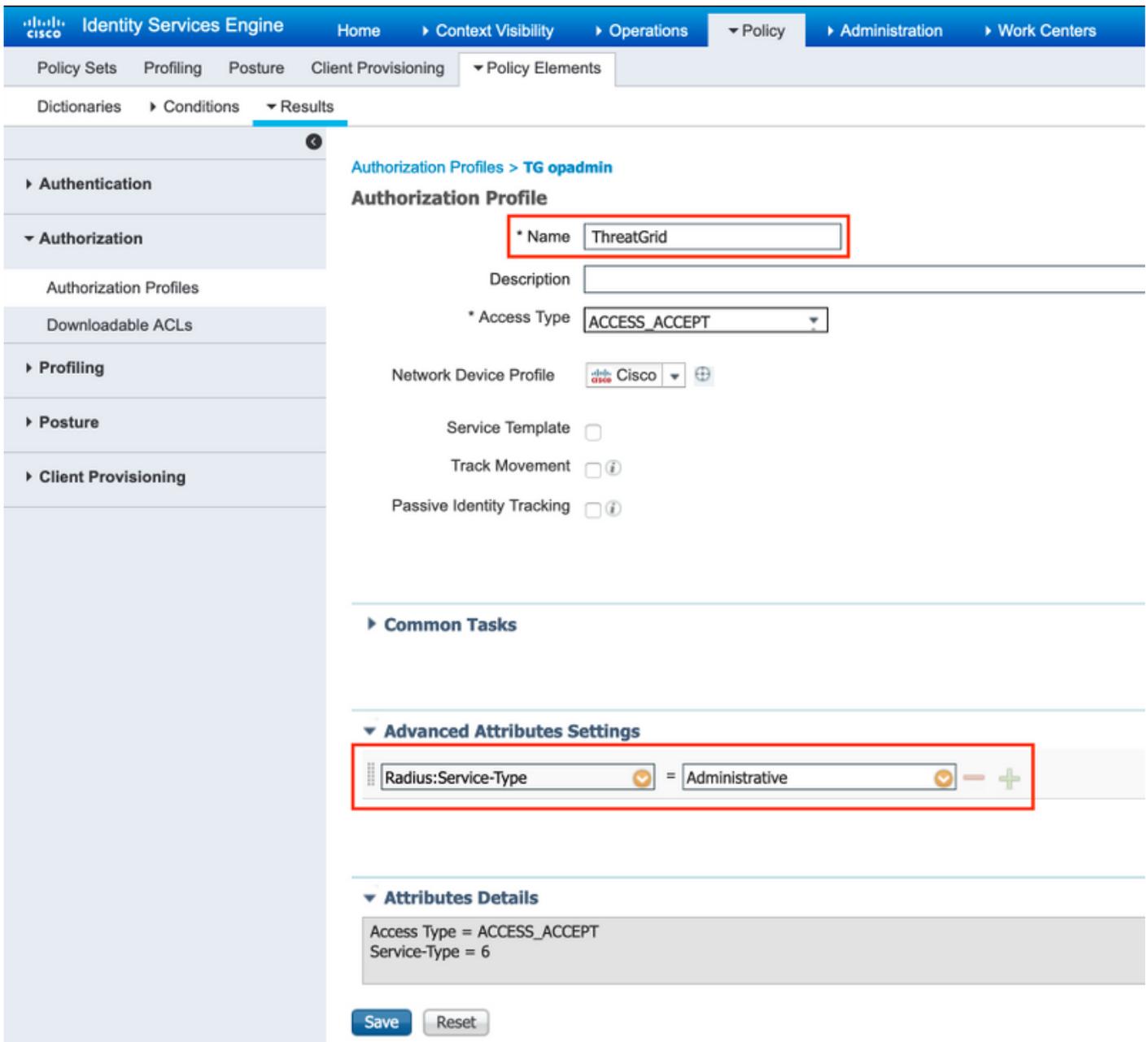
TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

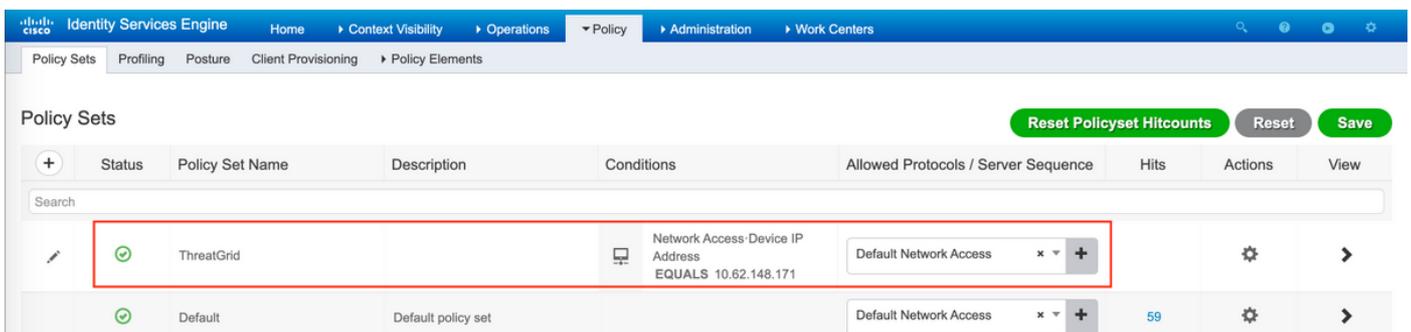
Paso 4. Cree un perfil de autorización para la política de autorización.

Navegue hasta **Política > Elementos de política > Resultados > Autorización > Perfiles de autorización** y haga clic en **Agregar**. Ingrese **Name** y seleccione **Advanced Attributes Settings** como se muestra en la imagen y haga clic en **Save**:



Paso 5. Cree una política de autenticación.

Navegue hasta **Política > Conjuntos de Políticas** y haga clic en "+". Ingrese **Policy Set Name** y establezca la condición en **NAD IP Address**, asignada a la interfaz limpia de TG, haga clic en **Save** como se muestra en la imagen:



Paso 6. Cree una política de autorización.

Haga clic en el botón ">" para ir a la política de autorización, expanda la política de autorización,

haga clic en "+" y configure como se muestra en la imagen, después de finalizar, haga clic en **Guardar**:

Authorization Policy (3)				Results					
				Profiles	Security Groups	Hits	Actions		
+	Status	Rule Name	Conditions						
Search									
+	✔	ThreatGrid Admin	Radius-NAS-Identifier EQUALS Threat Grid Admin	ThreatGrid	+	Select from list	+	1	⚙️
+	✔	ThreatGrid Console	Radius-NAS-Identifier EQUALS Threat Grid UI	ThreatGrid	+	Select from list	+	1	⚙️
+	✔	Default		DenyAccess	+	Select from list	+	17	⚙️

Sugerencia: puede crear una regla de autorización para todos los usuarios que coincidan con ambas condiciones, Admin y UI.

Paso 7. Cree un certificado de identidad para ThreatGrid.

El certificado de cliente de ThreatGrid debe basarse en la clave de curva elíptica:

```
openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem
```

Debe estar firmado por la CA en la que confía ISE. Marque [Importar los certificados raíz a la página almacén de certificados de confianza](#) para obtener más información sobre cómo agregar el certificado de CA al almacén de certificados de confianza de ISE.

Paso 8. Configure ThreatGrid para utilizar RADIUS.

Inicie sesión en el portal de administración, navegue hasta **Configuration>RADIUS**. En RADIUS CA Certificate , pegue el contenido del archivo PEM recolectado de ISE, en Client Certificate pegue el certificado con formato PEM recibido de CA y en Client Key pegue el contenido del archivo private-ec-key.pem del paso anterior, como se muestra en la imagen. Haga clic en Save (Guardar):

RADIUS DTLS Configuration

Authentication Mode		Either System Or RADIUS Authentication
RADIUS Host		10.48.17.135
RADIUS DTLS Port	HELP	2083
RADIUS CA Certificate	HELP	rVOxvUhoHai7g+B -----END CERTIFICATE-----
RADIUS Client Certificate	HELP	QFrtRNBHrKa -----END CERTIFICATE-----
RADIUS Client Key	HELP	2TOKEY4waktmOluw== -----END EC PRIVATE KEY-----
Initial Application Admin Username	HELP	radek

Nota: Debe volver a configurar el dispositivo TG después de guardar la configuración RADIUS.

Paso 9. Agregue el nombre de usuario RADIUS a los usuarios de la consola.

Para iniciar sesión en el portal de la consola, debe agregar el atributo RADIUS Username al usuario respectivo como se muestra en la imagen:

Details

Login	radek
Name	radek /
Title	Add... /
Email	rolszowy@cisco.com /
Integration ?	<input type="text" value="none"/>
Role	admin
Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
RADIUS Username ?	<input type="text" value="radek"/>
Default UI Submission Privacy ?	<input type="radio"/> Private <input type="radio"/> Public <input checked="" type="radio"/> Unset
EULA Accepted ?	No
CSA Auto-Submit Types ?	Add... /
Can Flag Entities ?	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset
Enable Direct SSO Setup ?	<input type="radio"/> True <input type="radio"/> False <input checked="" type="radio"/> Unset

Paso 10. Habilite la autenticación sólo RADIUS.

Después de iniciar sesión correctamente en el portal de administración, aparece una nueva opción, que desactiva completamente la autenticación del sistema local y deja el único basado en RADIUS.

Threat Grid Appliance Administration Portal

Support ? Help
Logout

Configuration Operations Status Support

RADIUS DTLS Configuration

Authentication Mode	<input type="radio"/> RADIUS Authentication Not Enabled <input checked="" type="radio"/> Either System Or RADIUS Authentication Permitted <input checked="" type="radio"/> Only RADIUS Authentication Permitted
RADIUS Host	<input type="text" value="10.48.17.135"/>

Verificación

Una vez reconfigurado TG, cierre la sesión y ahora las páginas de inicio de sesión se ven como en las imágenes, el administrador y el portal de consola respectivamente:



Authentication Required

Authenticate using RADIUS:



Authenticate

or

Authenticate using System Password:



Authenticate

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+



Threat Grid

i Use your RADIUS username and password.

RADIUS username

RADIUS password

Log In

[Forgot password?](#)

Troubleshoot

Hay tres componentes que podrían causar problemas: ISE, conectividad de red y ThreatGrid.

- En ISE, asegúrese de devolver ServiceType=Administrative a ThreatGrid las solicitudes de autenticación. Navegue hasta **Operaciones > RADIUS > Registros en Directo** en ISE y verifique los detalles:

Time	Status	Details	Repeat ...	Identity	Authentication Policy	Authorization Policy	Authorizati...	Network Device	
x				Identity	ThreatGrid	x	Authorization Policy	Authorization	Network Device
Feb 20, 2020 09:40:38.753 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean	
Feb 20, 2020 09:40:18.260 AM	✓			radek	ThreatGrid >> Default	ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean	

Authentication Details

Source Timestamp	2020-02-20 09:40:38.753
Received Timestamp	2020-02-20 09:40:38.753
Policy Server	wcecot-ise27-1
Event	5200 Authentication succeeded
Username	radek
User Type	User
Authentication Identity Store	Internal Users
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Service Type	Administrative
Network Device	ksec-threatgrid02-clean
Device Type	All Device Types
Location	All Locations
Authorization Profile	TG opadmin
Response Time	13 milliseconds

- Si no ve estas solicitudes, realice una captura de paquetes en ISE. Navegue hasta Operaciones > Solución de problemas > Herramientas de diagnóstico > TCP Dump, proporcione la IP en el campo Filtro de la interfaz de limpieza de TG, haga clic en Inicio e

intente iniciar sesión en ThreatGrid:

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Monitoring... (approximate file size: 8192 bytes) [Stop](#)

Host Name

Network Interface

Promiscuous Mode On Off

Filter
Example: 'ip host helios and not iceberg'

Format

Dump File

[Download](#)

[Delete](#)

Debe ver que el número de bytes aumentó. Abra el archivo pcap en Wireshark para obtener más información.

- Si aparece el error "Lo sentimos, pero algo salió mal" después de hacer clic en Guardar en ThreatGrid y la página se muestra de la siguiente manera:

 Threat Grid Appliance Administration Portal [Support](#) [Help](#)
[Logout](#)

[Home](#) [Configuration](#) [Operations](#) [Status](#) [Support](#)

We're sorry, but something went wrong.

The server experienced an error while processing your request. Please retry your request later.

If this problem persists, [contact support](#).

Esto significa que lo más probable es que haya utilizado la clave RSA para el certificado de cliente. Debe utilizar la clave ECC con los parámetros especificados en el paso 7.