El ESA con el amperio recibe “el servicio de la reputación del archivo en la nube es” error inalcanzable

Contenido

Introducción

Este documento describe la alerta atribuida al dispositivo de seguridad del correo electrónico de Cisco (ESA) con la protección avanzada de Malware (amperio) habilitó, donde el servicio no comunica sobre el puerto 32137 para la reputación del archivo.

Corrija “el servicio de la reputación del archivo en la nube es” error inalcanzable recibido para el amperio

El amperio fue liberado para el uso en el ESA en la versión 8.5.5 de AsyncOS para la Seguridad del correo electrónico. Con el amperio autorizado y habilitado en el ESA, los administradores reciben este mensaje:

```
The Warning message is:

amp The File Reputation service in the cloud is unreachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 10.0.0-125
Serial Number: 123A82F6780EEE9E1E10-AAA5DBEFCEEE
Timestamp: 26 Jul 2016 10:56:28 -0600
```

El servicio amperio se pudo habilitar, pero no comunica probablemente en la red vía el puerto 32137 para la reputación del archivo.

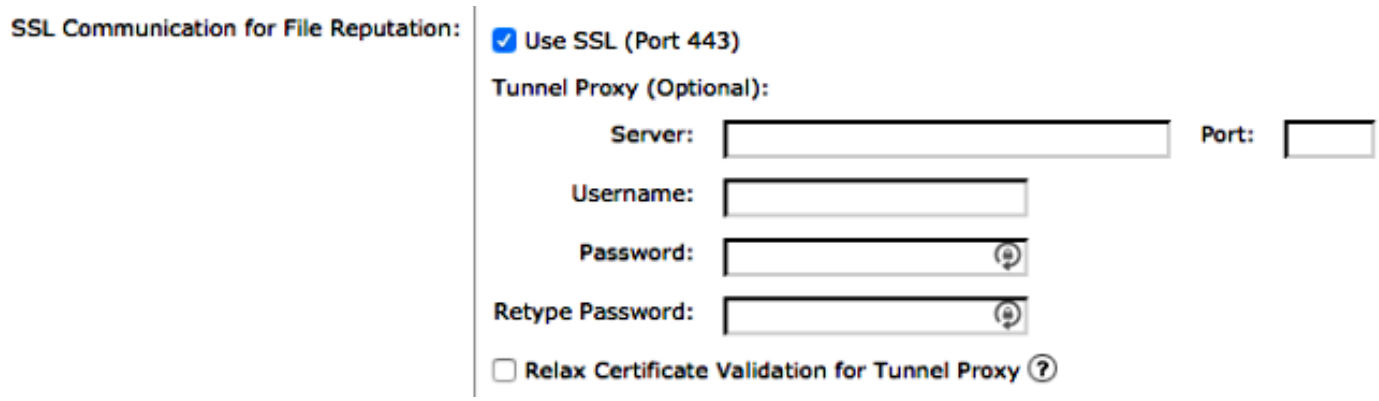
Si ése es el caso, el administrador ESA puede elegir hacer que la reputación del archivo comunique sobre el puerto 443.

¿Para hacer así pues, ejecute el **ampconfig > avanzado del** CLI y esté seguro que **Y** está seleccionada para *usted quiere habilitar la comunicación SSL (puerto 443) para la reputación del archivo? [n] >*:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
```

```
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Si usted utiliza el GUI, elija los **Servicios de seguridad > la reputación del archivo y el análisis > edita las configuraciones globales > avanzó (descenso-abajo)** y se asegura que la casilla de verificación del **uso SSL** está marcada como se muestra aquí:



Confíe cualquiera y todos los cambios a la configuración.

Finalmente, revise la orden actual del login amperio para ver el servicio y el éxito o el error de la Conectividad. Usted puede lograr esto del CLI con el **amperio de la cola.**

Antes de los cambios realizados al **ampconfig > avanzó**, usted habría visto esto en los registros amperio:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Después de que el cambio se realice al **ampconfig > avanzado**, usted ve esto en los registros amperio:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
```

```
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

El archivo de **amp_watchdog.txt** tal y como se muestra en del ejemplo anterior funcionará con cada 10 minutos y será seguido en el registro amperio. Este archivo es parte del señal de mantenimiento para el amperio.

Una interrogación normal en el registro amperio contra un mensaje con el tipo de archivo configurado para la reputación del archivo y el análisis del archivo sería similar a esto:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
```

```
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Con esta información de registro, el administrador debe poder correlacionar el ID del mensaje (MEDIADOS DE) en los registros del correo.

Troubleshooting

Firewall y configuraciones de red del estudio para asegurarse de que la comunicación SSL esté abierta para éstos:

Puerto	Protocolo	In/out	Nombre del host	Descripción
443	TCP	Hacia fuera	Como está configurado en los Servicios de seguridad > la reputación y el análisis del archivo, sección avanzada.	Acceso para nublarse los servicios para el análisis archivo.
32137	TCP	Hacia fuera	Como está configurado en los Servicios de seguridad > la reputación y el análisis del archivo, sección avanzada, sección avanzada, parámetro del pool del servidor de la nube.	Acceso para nublarse los servicios para obtener la reputación del archivo.

Usted puede probar la conectividad básica de su ESA al servicio de la nube sobre 443 vía Telnet para asegurarse de que su dispositivo puede alcanzar con éxito los servicios amperio, clasifiar la reputación, y clasifiar el análisis.

> Nota: Los direccionamientos para la reputación del archivo y el análisis del archivo se configuran en el CLI con el **ampconfig > avanzado**, o del GUI con los **Servicios de seguridad > la reputación y el análisis del archivo > edite las configuraciones globales > avanzado (descenso-abajo)**.

Clasifíe el ejemplo de la reputación:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
```

```
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Clasifíe el ejemplo del análisis:

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>
```

```
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private analysis cloud
[1]>

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Información Relacionada

- Prueba avanzada de la protección ESA Malware (amperio)
- Guías del usuario ESA
- ESA FAQ: ¿Cuál es un ID del mensaje (MEDIADOS DE), el ID de conexión de la inyección (ICID), o el ID de conexión de la salida (DCID)?
- ¿Cómo busco y ver el correo abre una sesión el ESA?
- Soporte Técnico y Documentación - Cisco Systems