ESA con AMP riceve l'errore "The File Reputation Service is not reachable" (Il servizio di reputazione file non è raggiungibile)

Sommario

Introduzione

Questo documento descrive l'avviso attribuito a Cisco Email Security Appliance (ESA) con Advanced Malware Protection (AMP) abilitato, dove il servizio non è in grado di comunicare sulla porta 32137 o 443 per la reputazione dei file.

Correggere l'errore "Il servizio di reputazione file non è raggiungibile" ricevuto per AMP

AMP è stato rilasciato per l'uso sull'ESA in AsyncOS versione 8.5.5 for Email Security. Se AMP è concesso in licenza e abilitato sull'ESA, gli amministratori ricevono questo messaggio:

```
The Warning message is:

The File Reputation service is not reachable.

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

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

Èpossibile che il servizio AMP sia abilitato, ma probabilmente non comunica in rete tramite la porta 32137 per la reputazione dei file.

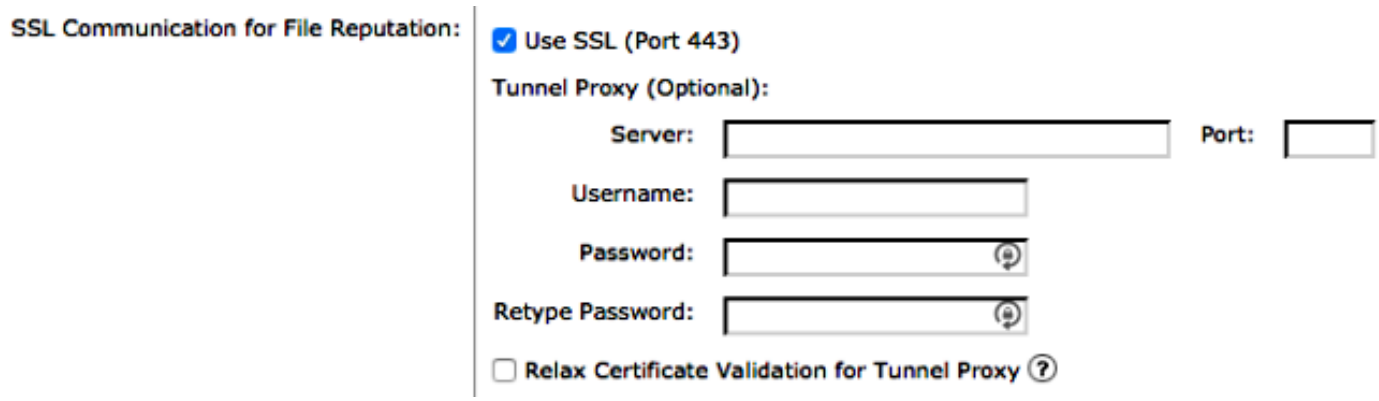
In questo caso, l'amministratore ESA può scegliere di far comunicare la reputazione del file sulla porta 443.

A tale scopo, eseguire **ampconfig > advanced** dalla CLI e assicurarsi che **Y** sia selezionato in *Do you want to enable SSL communication (port 443) for file reputation* (Abilitare la comunicazione SSL (porta 443) per la reputazione del file? *[N]>*:

```
(Cluster example.com)> ampconfig

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.
- CACHESETTINGS - Configure the cache settings for AMP.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

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

Enter heartbeat interval?
[15]>

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

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

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

Se si utilizza la GUI, scegliere **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (a discesa)** e assicurarsi che la casella di controllo **Use SSL** sia selezionata come mostrato di seguito:



Eseguire il **commit su** qualsiasi modifica apportata alla configurazione.

Infine, esaminare il registro AMP corrente per verificare se il servizio e la connettività hanno avuto esito positivo o negativo. A tale scopo, è possibile dalla CLI con **tail amp**.

Prima di apportare le modifiche ad **ampconfig > advanced**, nei log di AMP viene visualizzato quanto segue:

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

Dopo aver apportato la modifica ad **ampconfig > advanced**, nei log di AMP viene visualizzato quanto segue:

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

Il file **amp_watchdog.txt**, come illustrato nell'esempio precedente, verrà eseguito ogni 10 minuti e verrà registrato nel registro AMP. Questo file fa parte del servizio keep-alive per AMP.

Una normale query nel registro AMP relativa a un messaggio con i tipi di file configurati per Reputazione file e Analisi file sarebbe simile alla seguente:

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

Con queste informazioni di log, l'amministratore dovrebbe essere in grado di correlare l'ID messaggio (MID) nei log di posta.

Risoluzione dei problemi

Verificare le impostazioni del firewall e della rete per accertarsi che la comunicazione SSL sia aperta per:

Port	Protocollo	Entrata/Uscita	Nome host	Descrizione
443	TCP	Uscita	Come configurato in Servizi di sicurezza > Reputazione e analisi file, sezione Avanzate.	Accesso ai servizi clo per l'analisi dei file.

32137	TCP	Uscita	Come configurato in Servizi di sicurezza > Reputazione e analisi file, sezione Avanzate, sezione Avanzate, parametro Cloud Server Pool.	Accesso ai servizi clo per ottenere la reputa dei file.

Èpossibile testare la connettività di base dall'ESA al servizio cloud su 443 tramite Telnet per assicurarsi che l'appliance possa raggiungere correttamente i servizi AMP, la reputazione dei file e l'analisi dei file.

> **Nota**: gli indirizzi per la reputazione e l'analisi dei file sono configurati sulla CLI con **ampconfig > advanced** o dalla GUI con **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (a discesa)**.

> **Nota:** Se si utilizza un proxy tunnel tra ESA e i server File Reputation, potrebbe essere necessario abilitare l'opzione per rilasciare la convalida del certificato per il proxy tunnel. Questa opzione viene fornita per ignorare la convalida del certificato standard se il certificato del server proxy tunnel non è firmato da un'autorità radice considerata attendibile dall'ESA. Ad esempio, selezionare questa opzione se si utilizza un certificato autofirmato su un server proxy tunnel interno attendibile.

Esempio di reputazione del file:

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Esempio di analisi file:

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Se l'ESA è in grado di connettersi al file reputation server in modalità telnet e non è disponibile un proxy a monte che decrittografa la connessione, potrebbe essere necessario registrare nuovamente l'appliance con Threat Grid. Sulla CLI dell'ESA è presente un comando nascosto:

```
10.0.0-125.local> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
```

```
- SERVICES - Service Utilities.
[]> ampregister

AMP registration initiated.
```

Informazioni correlate

- Test ESA Advanced Malware Protection
- Guide per l'utente ESA
- Domande frequenti ESA: Che cos'è un ID messaggio (MID), un ID connessione di iniezione (ICID) o un ID connessione consegna (DCID)?
- Come posso cercare e visualizzare i log di posta sull'ESA?
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).