Raccolta di dati diagnostici da AMP for Endpoints Linux Connector

Sommario

Introduzione

In questo documento viene descritto come generare un file di diagnostica da AMP For Endpoints Linux Connector. Se si verifica un problema tecnico con Linux Connector, è possibile che un tecnico dell'assistenza Cisco desideri analizzare i messaggi di log disponibili in un file di diagnostica.

Genera file di diagnostica

Con questo comando, è possibile generare un file di diagnostica direttamente dall'interfaccia della riga di comando (CLI) di Linux:

```
/opt/cisco/amp/bin/ampsupport
```

Verrà creato un file .7z sul desktop. Il file può essere fornito a Cisco Technical Assistance Center (TAC) per ulteriori analisi.

Modalità debug

La modalità di debug del connettore fornisce un livello di dettaglio aggiuntivo per la registrazione. Consente di analizzare in modo più approfondito un problema relativo al connettore. In questa sezione viene descritto come abilitare la modalità di debug in un connettore.

> **Avviso:** La modalità di debug deve essere abilitata solo se Cisco richiede questi dati. Se si attiva la modalità di debug per un periodo di tempo più lungo, lo spazio su disco potrebbe esaurirsi molto rapidamente e il file di diagnostica del supporto potrebbe non essere in grado

di raccogliere il **registro del connettore** a causa di dimensioni eccessive del file.

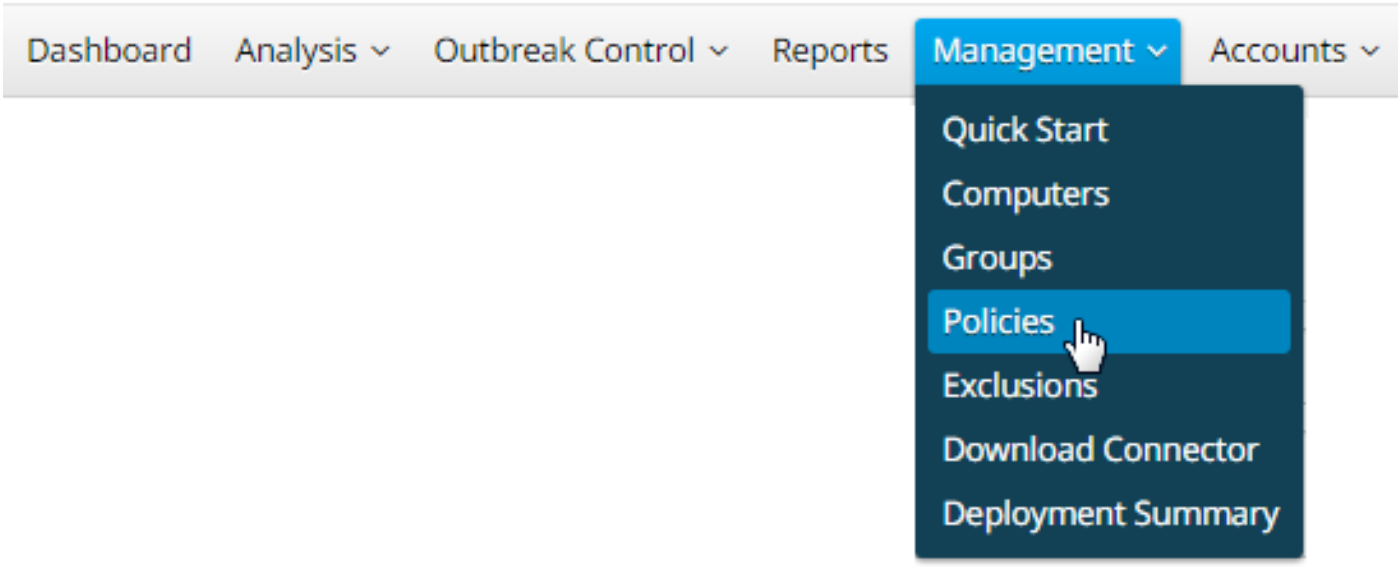
Usa console AMP

Abilita modalità debug

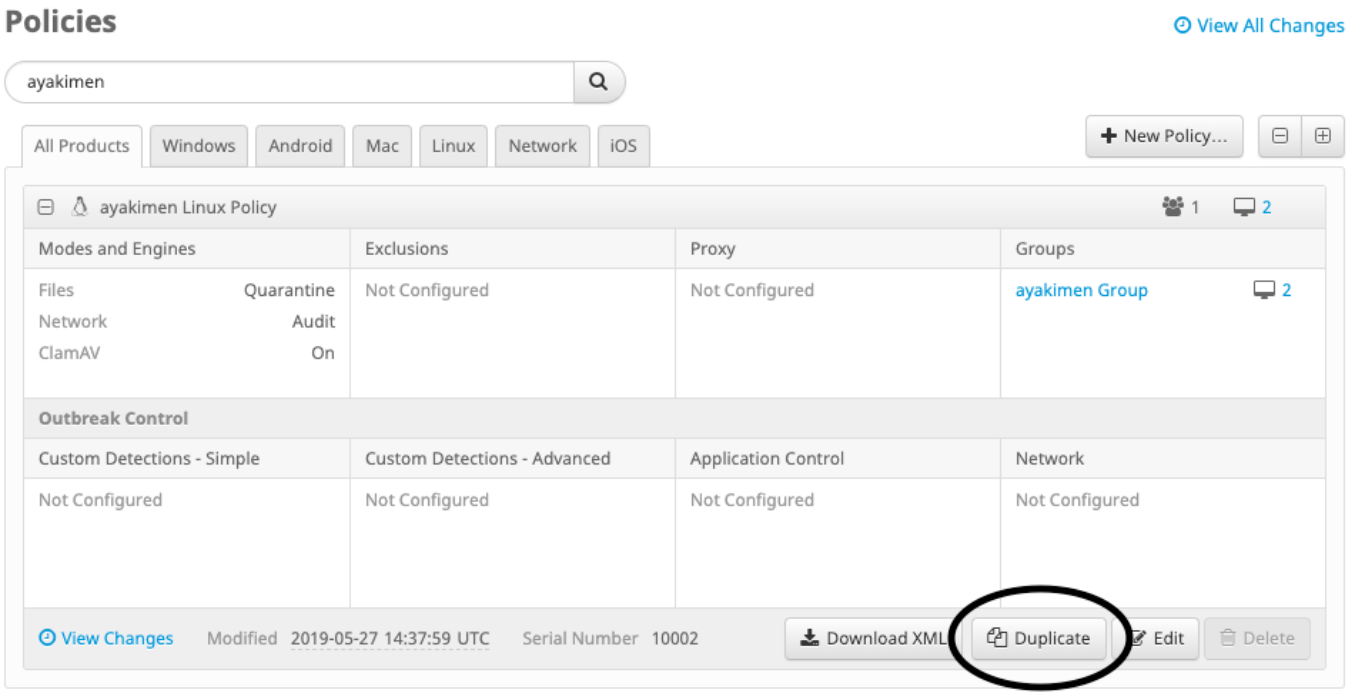
Èpossibile abilitare la modalità di debug nel criterio corrente con i passaggi da 5 a 7 oppure creare un nuovo criterio in modalità di debug con tutti i passaggi seguenti:

Passaggio 1. Accedere alla console AMP.

Passaggio 2. Selezionare **Gestione > Criteri**.

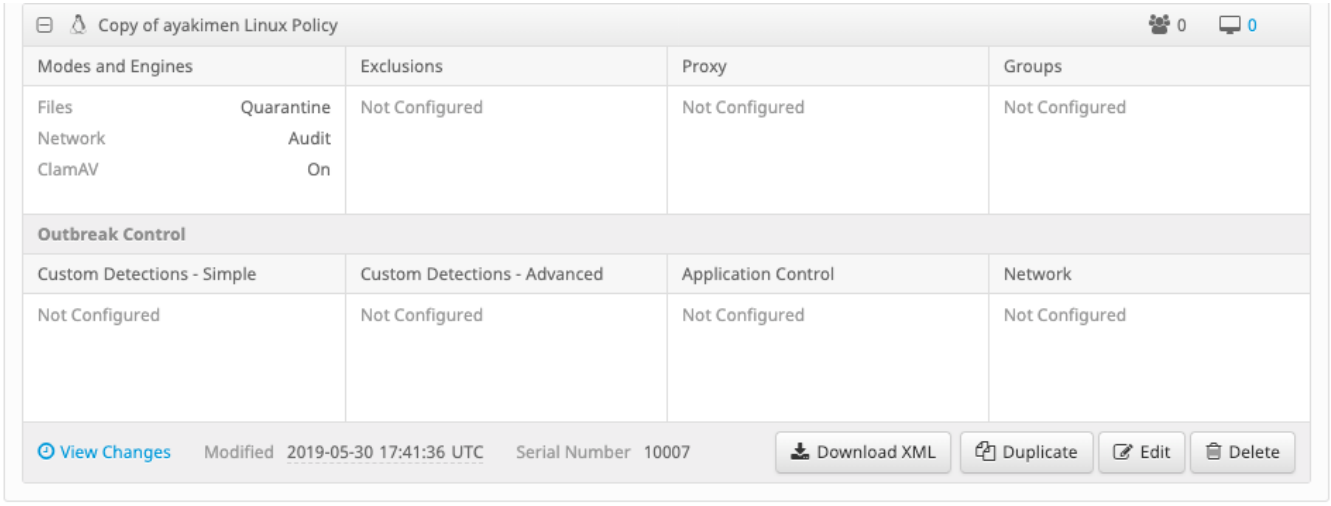


Passaggio 3. Individuare il criterio applicato al dispositivo o al computer terminale e fare clic sul criterio. La finestra del criterio verrà espansa. **Fare clic su Duplica**.

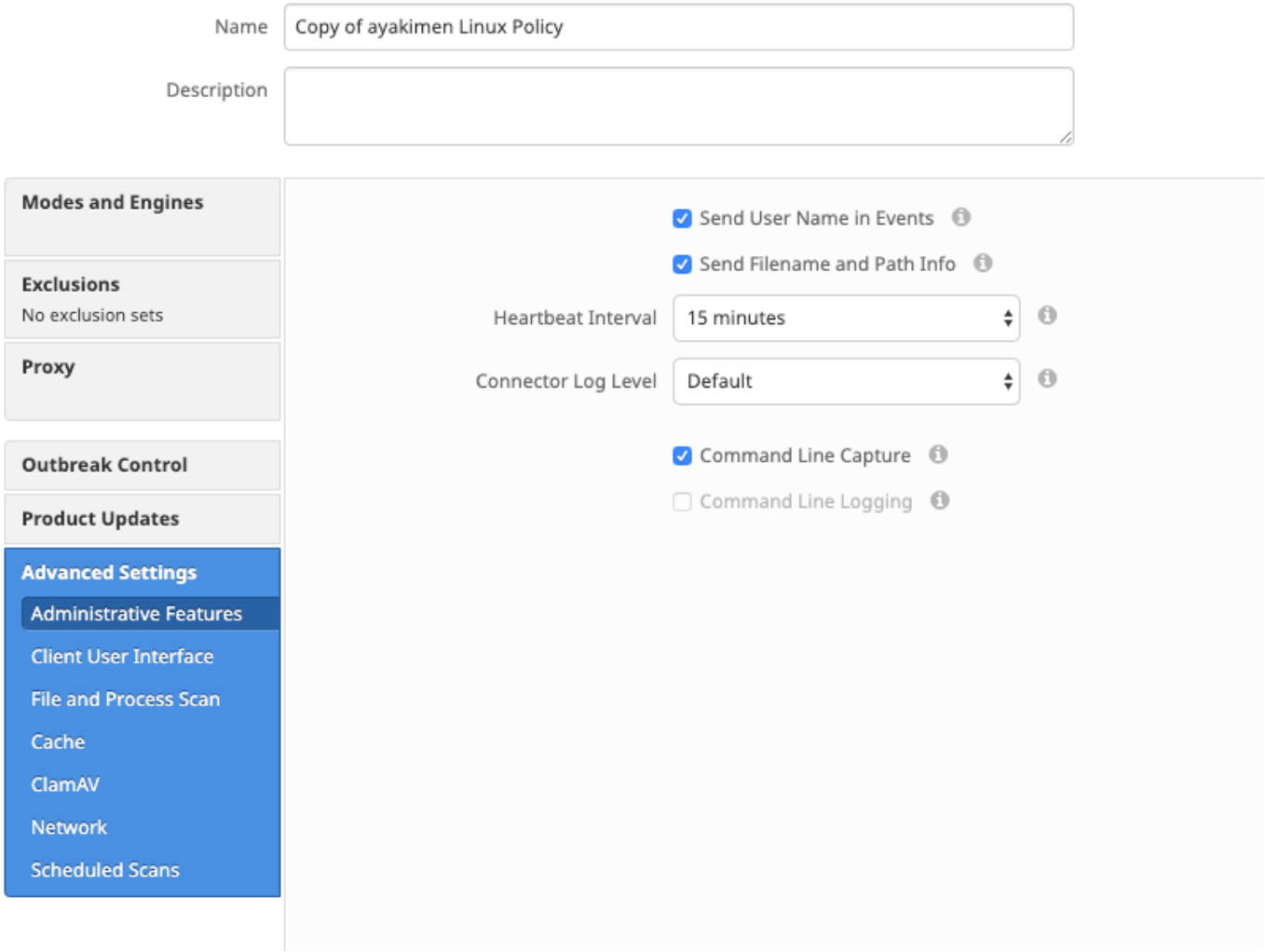


Passaggio 4. Dopo aver **fatto clic su Duplica**, la console AMP viene aggiornata con il criterio

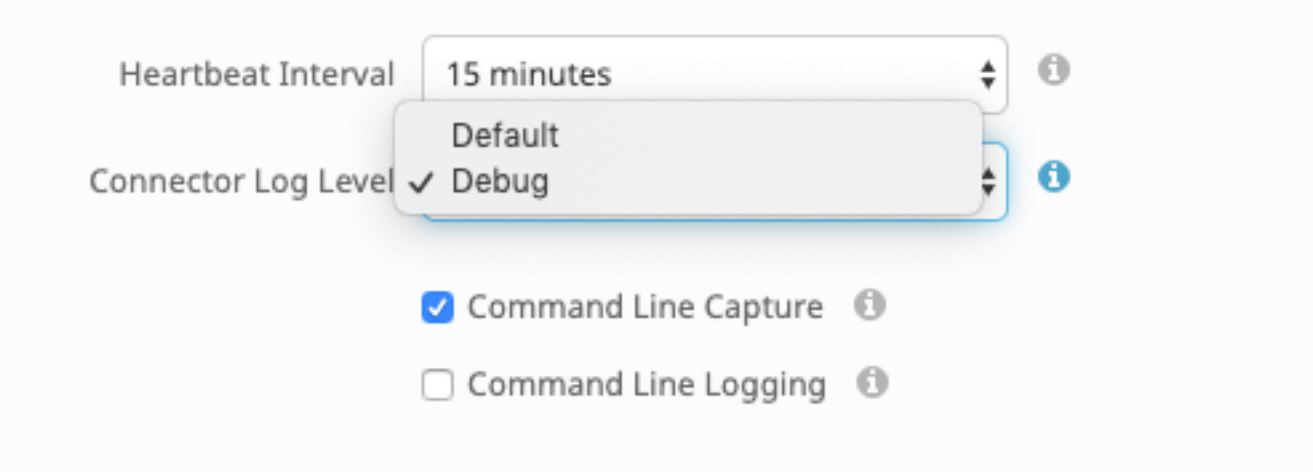
copiato.



Passaggio 5. **Fare clic su Modifica**, **su Impostazioni avanzate**, quindi selezionare **clic su** Funzioni **amministrative** dalla barra laterale.



Passaggio 6. **Per Livello log connettore**, selezionare Debug dagli elenchi a discesa.



Passaggio 7. Per salvare le modifiche, fare clic su Salva.

Passaggio 8. Dopo aver salvato il nuovo criterio, è necessario creare/modificare un gruppo per includere *il nuovo criterio* e *il* dispositivo *finale* in cui si desidera generare le informazioni di debug.

Disabilita modalità di debug

Per disabilitare la modalità di debug, seguire la stessa procedura utilizzata per abilitare la modalità di debug, ma impostare **Connector Log Level** su **Default**.

Usa riga di comando

Abilita modalità debug

Se si verificano problemi di connettività alla console e si desidera abilitare la modalità debug, eseguire questi comandi dalla CLI:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

Di seguito viene riportato l'output:

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

Disabilita modalità di debug

Per disabilitare la modalità debug, utilizzare i seguenti comandi:

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

Strumento di supporto Ottimizzazione durante il debug

Prima di iniziare l'ottimizzazione dei file di supporto, è necessario attivare la modalità di registrazione debug del daemon del connettore. Questa operazione viene eseguita tramite la console AMP, tramite le impostazioni dei criteri del connettore *in Gestione -> Criteri*. Modificare il

criterio e passare *alla* sezione Funzioni *amministrative della* scheda Impostazioni *avanzate*. Modificare *l'*impostazione *Connector Log* Level **in Debug**.

Quindi, salvare il criterio. Dopo aver salvato il criterio, verificare che sia stato sincronizzato con il connettore. Eseguire il Connettore in questa modalità per almeno 15-20 minuti prima di continuare con il resto della sintonizzazione.

NB: Al termine della regolazione, non dimenticare di modificare *l'impostazione Connector Log* Levelimpostando nuovamente su Default in modo che il connettore funzioni nella modalità più efficiente ed efficace.

Esecuzione dello strumento di supporto

Questo metodo prevede l'utilizzo dello strumento di supporto, un'applicazione installata con il connettore AMP Mac. È possibile accedervi dalla cartella Applications facendo doppio clic su /Applications->Cisco AMP->Support Tool.app. Verrà generato un pacchetto di supporto completo contenente ulteriori file di diagnostica.

Un alternativa, e più veloce, il metodo consiste nell'eseguire riga di comando seguenteda a Terminale sessione:

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```

La prima opzione consente di ottenere un file di supporto molto più piccolo contenente solo i file di ottimizzazione rilevanti. La seconda opzione fornisce un pacchetto di supporto completo che contiene ulteriori informazioni, ad esempio i log, che potrebbero essere necessari per regolare le esclusioni di processo (disponibili in Connector versione 1.1.0 e successive).

In entrambi i casi, Support Tool (Strumento di supporto) genera un file zip sulla ~home contenente due file di supporto per il tuning: fileops.txt ed excel.txt. fileops.txt contiene un elenco dei file creati e modificati più di frequente nel computer. Tali file sono utili per le esclusioni di percorsi e caratteri jolly. excel.txt conterrà l'elenco dei file eseguiti più di frequente, utili per le esclusioni di processo. Entrambi gli elenchi sono ordinati in base al numero di scansioni, il che significa che i percorsi digitalizzati con maggiore frequenza vengono visualizzati in cima all'elenco.

Lasciare il connettore in esecuzione in modalità di debug per un periodo di 15-20 minuti, quindi eseguire lo strumento di supporto. Una buona regola pratica consiste nel fatto che qualsiasi file o percorso con una media di 1000 accessi o più durante tale periodo è un buon candidato da escludere.

Ottimizzazione dell'esclusione

Creazione di percorsi, caratteri jolly, nomi e estensioni di file

Per iniziare a utilizzare le regole di esclusione dei percorsi, è possibile individuare i percorsi di file e cartelle digitalizzati con maggiore frequenza dal file fileops.txt e quindi creare regole per tali percorsi. Una volta scaricato il criterio, monitorare il nuovo utilizzo della CPU. L'aggiornamento della regola potrebbe richiedere dai 5 ai 10 minuti prima che l'utilizzo della CPU diminuisca, in quanto il daemon potrebbe impiegare del tempo per recuperare il tempo necessario. Se i problemi persistono, eseguire nuovamente lo strumento per visualizzare i nuovi percorsi osservati.

- Una buona regola pratica consiste nel considerare qualsiasi elemento con un'estensione di file di registro o di diario come candidato di esclusione appropriato.

Creazione di esclusioni di processo

NOTE: Process Exclusions on Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
Per informazioni sulle procedure consigliate relative alle esclusioni di processo, vedere: AMP for Endpoints: Esclusioni dei processi in macOS e Linux

Per prima cosa, un buon pattern di tuning identifica i processi con un elevato volume di esecuzioni da excs.txt, trova il percorso dell'eseguibile e crea un'esclusione per questo percorso. Esistono tuttavia alcuni processi che non devono essere inclusi, tra cui:

- Programmi di utilità generali - Non si consiglia di escludere i programmi di utilità generali (es: usr/bin/grep) senza tenere conto di quanto segue.

  L'utente può determinare l'applicazione che chiama il processo, ad esempio trovare il processo padre che esegue grep ed escludere il processo padre.

  Questa operazione deve essere eseguita solo se il processo padre può essere trasformato in una esclusione sicura. Se l'esclusione padre si applica ai

figli, verranno escluse anche le chiamate a qualsiasi figlio dal processo padre.È possibile determinare l'utente che esegue il processo. (es: se un processo viene chiamato a un volume elevato dall'utente "root", è possibile escludere il processo, ma solo per l'utente "root" specificato, ciò consentirà ad AMP di monitorare le esecuzioni di un determinato processo da parte di qualsiasi utente che non sia "root").**NOTA: le esclusioni di processo sono state introdotte nelle versioni Connector 1.11.0 e successive. Per questo motivo, i programmi di utilità generale possono essere utilizzati come esclusione di percorso in Connector versione 1.10.2 e successive. Tuttavia, questa pratica è consigliata solo quando è assolutamente necessario un compromesso sulle prestazioni.**

L'individuazione del processo padre è importante per le esclusioni di processo. Una volta individuato il processo principale e/o l'utente del processo, l'utente può creare l'esclusione per un utente specifico e applicare l'esclusione del processo ai processi secondari, che a loro volta escluderanno i processi rumorosi che non possono essere trasformati in esclusioni di processo.

Identifica processo padre

1. Seguire i passi da 1 a 3 di Identificazione del processo padre dall'alto.
2. Identificare l'utente di un processo utilizzando uno dei seguenti metodi: Trova l'ID utente del processo specificato da `U:` nella riga di registro (ad esempio: U:0).Dalla finestra del terminale eseguire il seguente comando: `getent passwd # | taglio -d: -f1`, dove # è l'ID utente.Viene visualizzato un output simile a:`Username`, dove Username è l'Utente del processo specificato.
3. Questo Il nome utente può essere aggiunto a un'esclusione di processo nella categoria Utente per ridurre l'ambito dell'esclusione, che per alcune esclusioni di processo è importante. **NOTA: se l'utente di un processo è l'utente locale del computer e questa esclusione deve essere applicata a più computer con utenti locali diversi, la categoria Utente deve essere lasciata vuota per consentire l'applicazione dell'esclusione di processo a tutti gli utenti.**

Informazioni correlate

- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Windows
- Raccolta di dati diagnostici da un connettore FireAMP in esecuzione su Mac OS
- **Documentazione e supporto tecnico – Cisco Systems**