Analizar el paquete de diagnóstico de AMP para una CPU elevada

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Troubleshoot Compruebe si hay otro antivirus instalado en el equipo Identificar si la CPU alta ocurre cuando una aplicación específica está en uso Recopile el paquete de diagnóstico para su análisis Activar nivel de registro de depuración Nivel de depuración en el terminal Nivel de depuración en la política Reproduzca el problema y recopile un paquete de diagnóstico Realizar el análisis Diag_Analyzer.exe Anphandlecount.ps1 Exclusiones de ajuste Enviar el paquete para su análisis al TAC

Introducción

Este documento describe los pasos para analizar un paquete de diagnóstico de la protección frente a malware avanzado (AMP) para terminales de nube pública en dispositivos Windows para solucionar problemas de uso elevado de la CPU.

Colaborado por Luis Velázquez y editado por Yeraldin Sánchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Acceso a la consola de AMP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de AMP para terminales 5.4.20200204
- Dispositivos del sistema operativo Windows

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Compruebe si hay otro antivirus instalado en el equipo

Si se instala otro antivirus, asegúrese de que el proceso principal del antivirus esté excluido en la configuración de políticas

Consejo: Utilice las exclusiones de Cisco-Mantenimiento si el software que se utiliza está incluido en la lista, recuerde que estas exclusiones se pueden agregar a las nuevas versiones de una aplicación.

Para ver las listas disponibles en la sección de exclusiones mantenidas por Cisco, navegue hasta Administración > Políticas > Editar > Exclusiones > Exclusiones Mantenidas por Cisco.

Seleccione los que el terminal necesitaría según el software instalado actualmente en el equipo y, a continuación, guarde la política, como se muestra en la imagen.

Name	haivelaz-W7_Policy			
Description				
on and Engines	Cisco-Maintai ed Exe	2 clusions 💿	đ	
lusions	5 selected v			
chodon sets	Bearch	^	3 Exclusions	
ĸy	C All		11 Exclusions	
	Altiris by Symantec	3 Exclusions	1 Exclusion	
break Control	Appsense	6 Exclusions	29 Exclusions	
duct Updates	AVAST	3 Exclusions	3 Exclusions 💌	
anced Settings	Avita	3 Exclusions		
	Citrix AppDNA	2 Exclusions		
	Citrix Cloud Connector	3 Exclusions		
3	Citrix EdgeSight Server	3 Exclusions	85 Exclusions ×	
	Citrix ICA Client	5 Exclusions		
	Citrix Provisioning Server	18 Exclusions		
	Citrix XenApp v6.5 and 7	7 Exclusions		
	Crashplan	3 Exclusions		
	Diebold Warsaw	10 Exclusions		
	Domain Controller	19 Exclusions		<u> </u>
	Hyper-V	17 Exclusions		
	CT 115	7 Exclusions		•

Identificar si la CPU alta ocurre cuando una aplicación específica está en uso

Identifique si el problema ocurre mientras se ejecuta una o varias aplicaciones si puede replicar el problema ayuda en el proceso de identificar posibles exclusiones.

Recopile el paquete de diagnóstico para su análisis

Activar nivel de registro de depuración

Para recopilar un paquete de diagnóstico útil, se debe habilitar el nivel de registro de depuración.

Nivel de depuración en el terminal

Si puede replicar el problema y tener acceso al terminal, a continuación se muestra el mejor procedimiento para capturar el paquete de diagnóstico:

1. Abrir AMP GUI

< Edit Policy

- 2. Vaya a Settings
- 3. Desplácese hasta la parte inferior de AMP GUI y abra **Configuración del conector de Cisco AMP**
- 4. Haga clic en Habilitar registro de depuración
- 5. El estado de registro de depuración debe cambiar a Iniciado. Este procedimiento habilita el

nivel de depuración hasta el siguiente latido de política, de forma predeterminada 15 minutos

^[A-Za-z]:\\/Wildcard/A	I/Drive
^[A-Za-z]:\\Wildcard\ a ^[A-Za-z]:\\pagefile\.sy	l\ drives s
Cara Callla an	
Scan Settings	
Notification Settings	▼
Proxy Settings	•
Cisco AMP Connector Settings	
Service Status:	Started
Password:	
Stop Service	
Debug Logging Chatug	Ctopped

Nivel de depuración en la política

Si no tiene acceso al punto final o el problema no se puede reproducir de forma consistente, el nivel de registro de depuración debe estar habilitado en la política.

Para habilitar el nivel de registro de depuración mediante la política, navegue hasta Administración > Políticas > Editar > Configuración avanzada > **Nivel de registro del conector** y Administración > Políticas > Editar > Configuración avanzada > Nivel de registro de la bandeja, seleccione Depurar y guarde la política, como se muestra en la imagen.

Name Indexta - W7_goldy Description Modes and Engines Exclusions	#Windows				
Description Modes and Engines Exclusions B axclasion ands Peay Outbreak Centrel Peay Outbreak Centrel Peduct Updates Advanced Settings Connector Protection Passavor Q Automated Crash Dump Uploteds Q Command Line Logging Command Line Logging	Name	luivelaz-W7_Policy			
Modes and Engines Exclusions Castlations min Peasy Outbreak Control Peaduct Updates Advanced Settings Advanced Settings Advanced Settings Connector Protection Passwort Control Control <th>Description</th> <th></th> <th></th> <th>đ</th> <th></th>	Description			đ	
Exclusions Exclusions Exclusions Exclusions Preay Outbreak Centrel Preduct Updates Advanced Settings Advanced Settings Advanced Settings Advanced Settings Connector Protection Passweri Connector Passweri Connector Passweri Connector Passweri Connector Passweri Conn	Modes and Engines		Send User Name in Events		
Preazy Outbreak Control Preduct Updates Advanced Settings Advanced Settings Advanced Settings Advanced Settings Connector Protection Password Connector Password <tr< th=""><th>Exclusions 6 exclusion sets</th><th></th><th>Send Filename and Path Info 0</th><th></th><th></th></tr<>	Exclusions 6 exclusion sets		Send Filename and Path Info 0		
Outbreak Control Product Updates Advanced Settings Advanced Settings Advanced Settings Advanced Settings Advanced Settings Connector Protection Password Connector Protection Connector Protection Password Connector Protection Password Connector Protection Password Connector Protection Password Connector Password Connector Password Connector Password Connector Pass	Proxy	2 Connector Log Level	Debug v	0	
Product Updates Advanced Settings Advanced Settings Advanced Settings Advanced Settings Advanced Settings Connector Protection Password Connector Protection Password Connector Protection Password Connector Protection Password Charle Connector Protection Password Connector Protection Password Connector Protection Password Connector Protection Connector Protection Connector Protection Password Connector Protection Password Connector Protection Connector Protection Charles Connector Protection Connector Protection Connector Protection Connector Protection Connector Protection Connector Protection Connector Protectin Protection <t< th=""><th>Outbreak Control</th><th>Tray Log Level</th><th>Debug v</th><th>0</th><th></th></t<>	Outbreak Control	Tray Log Level	Debug v	0	
Advanced Settings Advanced Settings Advanced Settings Advanced Settings Advanced Settings Classif Liber Initialized File and Process Scan Classif Classif Classif Endsoint Isolation Child Engines It TBA Network Schwalakad Scans Identity Presistence	Product Updates		Enable Connector Protection		
Cheat Ishatiaa Image: Automated Crash Dump Uploads File and Process Scan Image: Original Une Capture Cashat Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture Engines Image: Original Une Capture File and Process Scan Image: Original Une Capture File and Process Scan Image: Original Une Capture File and Process Scan Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File and Original Une Capture Image: Original Une Capture File an	Advanced Settings Administrative Features	Connector Protection Password	•••••	0	
Caulter Command Line Capture Endpoint Isolation Command Line Logging Ontable Command Line Logging Engines IT TRA Network Schwalskat Scars Kdentey Persistence It Testence	Client User Interface File and Process Scan		Automated Crash Dump Uploads		
Endpoint Isolation ChisId Engines II TISA Network Schwaluket Scarp Kdentry Persistence	Cache		Command Line Capture		
Engines IETBA Network Schwebuled Scars Identry Persistence	Endpoint Isolation Orbital		Command Line Logging		
IETIBA Network Sichwishland Scans Identity Persistence	Engines				
Network Schwalaket Scam Identity Persistence	ITTBA				
Identity Persistence	Network Schwitzland Scians				
	Identity Persistence				

Precaución: Si el modo de depuración se habilita desde la política, todos los terminales reciben este cambio.

Nota: Sincronice la política del punto final para asegurarse de que se aplica el nivel de depuración o espere el intervalo de latido, de forma predeterminada es de 15 minutos.

Reproduzca el problema y recopile un paquete de diagnóstico

Cuando se configura el nivel de depuración, espere hasta que se produzca el estado de CPU alta en el sistema o reproduzca manualmente las condiciones previamente identificadas y luego reúna el paquete de diagnóstico.

Para recopilar el paquete, navegue hasta C:\Program Files\Cisco\AMP\X.X.X (donde X.X.X es la última versión de AMP instalada en el sistema) y ejecute la aplicación ipsupporttool.exe, este proceso crea un archivo .7z en el escritorio denominado CiscoAMP_Support_Tool_%date%.7z

Nota: La versión 6.2.3 y posterior del conector pueden solicitar un paquete remotamente, navegar a **Administración > Equipos**, expandir el registro del terminal y utilizar la opción Diagnose.

Nota: El paquete de diagnóstico también puede ejecutarse desde un mensaje CMD con el

comando: "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe", o "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To", donde X.X.X es la última versión de AMP instalada, se puede utilizar el segundo comando para seleccionar la carpeta de resultados para el archivo .7z.

Realizar el análisis

Hay dos maneras de analizar un archivo de diagnóstico:

- Diag_Analyzer.exe
- Anphandlecount.ps1

Diag_Analyzer.exe

Paso 1. Descargue la aplicación aquí.

Paso 2. En la página GitHub, hay un archivo README con más instrucciones sobre el uso.

Paso 3. Copie el archivo de diagnóstico **CiscoAMP_Support_Tool_%date%.7z** en la misma carpeta en la que se encuentra Diag_Analyzer.exe.

Paso 4. Ejecutar la aplicación Diag_Analyzer.exe.



Paso 5. En el nuevo mensaje confirme si desea obtener las exclusiones de la política con una Y o una N.

Paso 6. El resultado del script contiene:

- Los 10 procesos principales
- 10 archivos principales
- 10 principales extensiones

- 100 rutas principales
- Todos los archivos

Nota: Diag_Analyzer.exe comprueba el archivo de diagnóstico de AMP proporcionado para los archivos sfc.exe.log. a continuación, crea un nuevo directorio con el nombre del archivo de diagnóstico y almacena los archivos de registro fuera del .7z, en el directorio primario del diagnóstico, después de esto, analiza los registros y determina los 10 principales procesos, archivos, extensiones y rutas, por último, imprime información en la pantalla y también en un archivo {Diagnostic}-summary.txt.

Anphandlecount.ps1

Paso 1. Descargue el script **amphandlecounts.txt** desde la parte inferior de esta publicación de la comunidad <u>Revisar archivos escaneados desde AMP.</u>

Paso 2. Para ejecutar el script en Windows, cámbielo a anphandlecount.ps1.

Paso 3. Para mayor comodidad, copie el archivo amphandlecount.ps1 en su propia carpeta.



Paso 4. Descomprima el archivo CiscoAMP_Support_Tool_%date%.7z e identifique los archivos sfc.log en la ruta CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X .

	Name	Date modified	Туре	Size	
	ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB	
*	5 global.xml	08/06/2019 11:23	XML File	24 KB	
*	sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB	
1	sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB	
th: dre	sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB	
	5 sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB	
	sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB	
	5 sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB	
	sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB	
	sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB	
	sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB	
	sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB	

Paso 5. Copie los archivos sfc.log en la carpeta anphandlecount.ps1.

	Name	Date modified	Туре	Size	
	ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB	
*	🧧 globalaml	08/06/2019 11:23	XML File	24 KB	
*	📕 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB	
*	5 sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB	
nt: xh	sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB	
	5 sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB	
	sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB	
	sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB	
	5 sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB	
	sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB	
	5 sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB	
	sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB	

Paso 6. Ejecute **amphandlecount.ps1** con PowerShell, después se abre una ventana y, según la política de ejecución del terminal, se puede solicitar permiso para ejecutarse.

Consejo: Para cambiar la política de ejecución, abra un Windows PowerShell y utilice los siguientes comandos:

Establezca la política para permitir el acceso sin restricciones a la ejecución - Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted

Establezca la política para restringir el acceso a la ejecución - Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restringido

Paso 7. Permita que PowerShell finalice (puede que tarde algún tiempo, dependiendo de cuántos sfc.log haya en la carpeta) después de que PowerShell termine, se crean cuatro archivos en la carpeta:

- data.csv
- results.txt
- sorted_results.txt
- terms.txt

۰ 📙	> This	is PC > Documents > Review Bundle			~ Ö	Search Review Bundle	٩,
		Name	Date modified	Туре	Size		
ess hots		amphandlecount.ps1	26/04/2019 09:44 a	Windows PowerS	3 KB		
and a	<u>_</u>	data.csv	22/06/2019 03:28	Microsoft Excel C	754 KB		
ads	я	results.bit	22/06/2019 03:28	TXT File	3 KB		
	A	5 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB		
ire		5fc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB		
6		sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB		
Bundle		5fc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB		
		5 sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB		
		5fc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB		
		5fc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB		
		sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB		
		5fc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB		
cts		sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB		
·	_	sorted_results.txt	22/06/2019 03:28	TXT File	3 KB		
ents		🗾 terms.txt	22/06/2019 03:28	TXT File	3 KB		
a de							

Paso 8. Los 4 nuevos archivos contienen el resultado del análisis:

- data.csv: contiene la ruta completa de los archivos analizados y el proceso padre que creó/modificó/movió el archivo
- results.txt: contiene la lista de procesos escaneados por AMP
- sorted_results.txt: contienen la lista de procesos que AMP analiza con el proceso más analizado
- terms.txt: contiene el nombre de los procesos analizados por AMP

Paso 9. Filtre el nombre del proceso con recuentos altos de **sort_results.txt** en **data.csv** puede identificar el proceso primario con su ruta de acceso completa y, a continuación, continúe agregando una exclusión a la política en una lista personalizada si es de confianza.

Procesos a buscar:

- 1. Ctrl + F en "data.csv" y buscar
- 2. Ruta del archivo analizado por AMP
- 3. Ruta del proceso primario que copia/mueve/modifica el archivo

Nota: Nota: Normalmente, la exclusión es del tipo "Proceso: Análisis de archivos" con "Procesos secundarios" para el proceso principal que está recibiendo los análisis:

4 Þ	sorted_results.txt •	A2 🛐 🗄 🔀 🖉 Jun 18 13:42:40, C:\Temp\NVIDIA 🕢 Panelinstaller?Temp\nwmobESN.chm, C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.(C9752557-A557-4AE9-
1 2	1075 setup.exe 442 firefox.exe	A C D E F G H I J K L M N O P Q R S T
4	243 Container.exe	Jun 18 13:42:40 CC\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobESM.chm, C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-4A557-4A59-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
5	243 container.exe	Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobESN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.[C9752557-A557-4A59-B7D4-551FE0F3AFE7]\NvCplSetupInt.exe
6	243 Container.exe	Inn 18 13:43:40.C\Tomo\NUIDIA\ControlDanolInctallerTomo\numphFIN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-4557-44E9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
7	243 container.exe	Find and Replace 7 X A.chm,C:\Program Files\NVIDIA Corporation\installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
å	243 container.exe	8.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.[C9752557-A557-4AE9-B7D4-551FE0F3AFE7]\NvCplSetupInt.exe
10	120 NvCplSetupInt.exe	Find Reglace N.chm.C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.(C9752557-A557-A4E9-B7D4-S51FE0F3AFE7)\NvColSetupInt.exe
11	54 ch. e.exe	Find what: NrColSetupInt.exe chm. C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.(09752557-A557-A559-87D4-551FE0F3AFE7)\NvColSetupInt.exe
12	p_ershell.exe	A service of the serv
13	1 sass.exe	Commiscue for an integration in the formation (in statilized to share) contract, Contract, State and Compared to the comparison of the state of t
15	/ OUTLOOK.EXE	Contines >> Options >>
16	7 nvstinst.exe	2 2 D.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.[C9752557-A557-4AE9-B7D4-551FE0F3AFE7]\NvCpISetupInt.exe
17	5 explorer.exe	R.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.[C9752557-A557-4AE9-B7D4-551FE0F3AFE7]\NvCplSetupInt.exe
18	4 rundl132.exe	2 Find All Find Next Close C.chm, C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
19	3 Indexe	3 Jun 18 13:42:41, C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobPTB.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
20	J OUCLOOK-CKC	in the second seco

Nota: <u>Aquí</u> puede encontrar más información relacionada con las mejores prácticas para crear exclusiones.

Exclusiones de ajuste

Una vez que se identifican los procesos o las trayectorias, puede agregarlos a la lista de exclusión vinculada a la política aplicada en el punto final, navegue hasta **Administración > Exclusiones > Nombre de exclusión > Editar,** como se muestra en la imagen.

Threat	CSIDL_W	/INDOWS\Temp_avast_\		J	
Path	[Any Driv	e]:\ pagefile.sys	Ì		
File Extension	Apply	to all drive letters			
Wildcard	Path excl	usion	Ì	1	
Process:	Threat ex	clusion		í	
File Scan					
Malicious Activity	Wildcard				
System Process		to all drive letters			
Process	Path	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55	Ì		
Process File Scan	Path SHA	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55	Ĩ		
Process	Path SHA You can p be met fo	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55	Ĩ		
Process	Path SHA You can p be met fo	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55 provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must or the process to be excluded. to child processes	Ì		

Enviar el paquete para su análisis al TAC

El TAC de ATS puede ayudar a resolver estos problemas, si es así, esté listo para proporcionar la siguiente información al crear el caso:

- ¿Cuándo comienza este problema?
- ¿Hay algún cambio reciente?
- ¿El problema ocurre con una aplicación determinada?En caso afirmativo, ¿qué aplicación?
- ¿Hay otro antivirus en el sistema?En caso afirmativo, ¿qué antivirus?
- Recopile un paquete de depuración mientras se reproduce el problema: <u>Pasos para recopilar</u> <u>un paquete de depuración</u>