

Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro

Publié: 2024-04-10

Dans les métriques TCP, la taille de la fenêtre indique la quantité de données qu'un équipement peut recevoir et traiter au cours d'un flux. Lorsque la taille de la fenêtre est nulle, les transmissions sont interrompues jusqu'à ce que l'équipement indique qu'il dispose de l'espace nécessaire pour recevoir à nouveau des données.

Il n'est pas rare que les fenêtres ne durent qu'une ou deux secondes, surtout en période de fort trafic. Cependant, des conditions de fenêtre zéro qui durent plus longtemps peuvent indiquer un problème plus grave et entraîner des problèmes de performances.

Vous pouvez créer un tableau de bord ou configurer des notifications d'alerte pour ne suivre aucune occurrence de fenêtre, mais la cause peut être difficile à déterminer. Par exemple, l'utilisation du processeur, de la mémoire et de la carte réseau peut être normale et vous ne savez pas si le problème provient du réseau, des serveurs ou de l'application. Mais vous pouvez toujours trouver la vérité dans le paquet !


Dans cette procédure pas à pas, vous allez créer un déclencheur qui capture les paquets sans conditions de fenêtre sur les transactions HTTP. Vous téléchargerez ensuite les captures afin de pouvoir télécharger les données vers un analyseur de paquets afin de vous aider à déterminer l'état du client et du serveur sur un flux lorsque des conditions de fenêtre zéro se sont produites.

Prérequis

- Vous devez disposer de privilèges d'administration du système et des droits d'accès ou de privilèges d'écriture complets avec l'accès aux paquets activé.
- Vous devez [activer la capture de paquets via la page d'administration](#).
- Vous devez disposer d'un analyseur de paquets, tel que Wireshark ou Microsoft Network Monitor.
- Familiarisez-vous avec [DÉCLENCHEURS](#) les concepts et les procédures dans [Créez un déclencheur](#).

Écrivez le déclencheur de capture de précision

Dans les étapes suivantes, vous allez écrire un déclencheur qui lance une capture de paquets de précision chaque fois qu'une condition de fenêtre zéro se produit sur une transaction HTTP.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Spécifiez les paramètres de configuration du déclencheur suivants :
 - a) Type PCAP de taille de fenêtre à zéro dans le **Nom** champ.
 - b) Dans le champ Affectations, tapez `HTTP Servers`, puis sélectionnez **Serveurs HTTP**.
 - c) Dans la liste des événements, sélectionnez **FLOW_TICK**.
 - d) Sélectionnez le **Activer le journal de débogage** case à cocher.
 - e) Cliquez **Afficher les options avancées** et tapez 128 dans le champ Octets par paquet à capturer.



Conseil valeur par défaut est 0. Conservez cette valeur pour capturer tous les octets de chaque paquet.

- Dans le volet droit, tapez le code suivant pour lancer la capture du paquet lorsqu'une condition de fenêtre zéro se produit :

```
// Check to make sure that this is an HTTP transaction
if ( Flow.l7proto !== 'HTTP' ){
  return;
}


//The packet capture name, which includes the client and server
//IP addresses and port numbers
var pcapName = 'Zero Windows_'
  + Flow.client.ipaddr + ':' + Flow.client.port
  + '-'
  + Flow.server.ipaddr + ':' + Flow.server.port;

//Initiate packet capture each time a zero window occurs on
//the client or the server
if ( Flow.zeroWnd1 > 0 || Flow.zeroWnd2 > 0 ) {
  var opts = {
    maxPackets: 30,           // Capture up to 30 packets
    maxPacketsLookback: 15 // Capture up to 15 lookback packets
  };
  Flow.captureStart(pcapName, opts);
  //Show capture activity in debug log
  debug('Start Zero PCAP: ' + pcapName);
}
```



- Cliquez **Enregistrer**.

Afficher la sortie de débogage dans le journal de débogage

Au cours des étapes suivantes, vous allez consulter la sortie de débogage du déclencheur pour confirmer que le déclencheur est en cours d'exécution et qu'il capture des paquets. Une fois que vous avez attribué le déclencheur à vos sources de données, le système exécute le déclencheur lorsque le trafic HTTP se produit, et si une transaction contient une fenêtre zéro, le système envoie les résultats du débogage au journal de débogage.

- Cliquez sur l'icône des paramètres système , puis cliquez sur **DÉCLENCHEURS**.
- Cliquez sur **PCAP de taille de fenêtre à zéro** déclencheur que vous venez de créer.
- Cliquez **Modifier le script de déclenchement**.
- Cliquez sur le **Journal de débogage** onglet.

Le journal de débogage affiche des résultats similaires à ceux de la figure suivante :

PROBLEMS  	DEBUG LOG
	[Fri Jun 14 13:01:59] Start Zero PCAP: Zero Windows_192.0.2.11:56428-192.0.2.111:5989
	[Fri Jun 14 13:02:29] Packet capture already in progress
	[Fri Jun 14 13:02:57] Start Zero PCAP: Zero Windows_192.0.2.115:48208-192.0.2.151:443
	[Fri Jun 14 13:02:59] Start Zero PCAP: Zero Windows_192.0.2.11:50663-192.0.2.251:5989


Télécharger et afficher les captures de paquets

Dans les étapes suivantes, vous allez télécharger les captures de paquets.




Note: Les étapes suivantes montrent comment télécharger des paquets depuis les systèmes Reveal (x) Enterprise. Pour plus d'informations sur le téléchargement de paquets depuis les

systèmes ExtraHop Performance, voir [Téléchargez des paquets sur les systèmes ExtraHop Performance](#).

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Enregistrements**.
3. Cliquez **Afficher les enregistrements**.
4. Dans la liste déroulante Type d'enregistrement, sélectionnez **Capture de paquets**.
5. Une fois que les enregistrements associés à votre capture de paquets apparaissent, cliquez sur l'icône Paquets , puis cliquez sur **Télécharger PCAP**.

Téléchargez des paquets sur les systèmes ExtraHop Performance

1. Cliquez sur l'icône des paramètres système , puis cliquez sur **Toute l'administration**.
2. À partir du Captures de paquets section, cliquez **Afficher et télécharger des captures de paquets**.
Le Liste de capture de paquets affiche des résultats similaires à la figure suivante :

Packet Capture List

Delete Selected Captures		Download Selected Captures	
<input type="checkbox"/>	Name ^		
<input type="checkbox"/>	Zero Windows_192.0.2.246:60849-203.0.113.95:443	Packets: 562	Bytes: 430286 Duration: 4m53s VLAN: 0 IP Proto: TCP
<input type="checkbox"/>	Zero Windows_192.0.2.246:56071-203.0.113.14:443	Packets: 841	Bytes: 969344 Duration: 35s VLAN: 0 IP Proto: TCP
<input type="checkbox"/>	Zero Windows_192.0.2.246:52675-198.51.100.9:443	Packets: 2603	Bytes: 2990518 Duration: 6s VLAN: 0 IP Proto: TCP

Chaque capture de paquet de la liste représente un flux de données entre les appareils et fournit des informations sur les appareils, les ports et la plage horaire pour vous aider à affiner les captures à télécharger.

3. Sélectionnez n'importe quelle capture nommée **Zéro Windows_** et cliquez **Télécharger les captures sélectionnées**.

La capture est enregistrée sur votre machine locale à l'aide du `.pcap` extension de fichier.

4. Ouvrez le fichier de capture à l'aide d'un analyseur de paquets, tel que Wireshark.

Le résultat ressemblera à la figure suivante :

The screenshot displays a network traffic capture in Wireshark. The packet list pane shows several packets, with packet 26 highlighted in red, indicating a 'Zero Window' condition. The packet details pane for packet 26 shows the following information:

- Checksum: 0xc5dd [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [SEQ/ACK analysis]
 - [This is an ACK to the segment in frame: 23]
 - [The RTT to ACK the segment was: 0.31564000 seconds]
- [TCP Analysis Flags]
 - [Expert Info (Warning/Sequence): TCP Zero Window segment]
 - [TCP Zero Window segment]
 - [Severity level: Warning]
 - [Group: Sequence]

The hex dump at the bottom of the packet details pane shows the raw data of the packet:

```

0000 00 08 e3 ff fc 28 38 c9 86 f0 c7 e5 81 00 03 fc .....(8. ....
0010 08 00 45 00 00 34 8e 7f 40 00 40 06 75 87 0a 14 ..E..4.. @.@.u...
0020 e3 f6 34 54 14 5f ed b1 01 bb f7 90 f8 01 f2 1a ..4T_... ..
0030 1e 48 80 10 00 00 c5 dd 00 00 01 01 08 0a 34 8e .H.....4.
0040 8e 64 cf 6f f8 5c .d.o.\

```

5. Ouvrez les paquets qui indiquent une occurrence nulle dans la fenêtre.

Vous verrez des détails tels que les indicateurs TCP, le moment où aucune condition de fenêtre s'est produite, la durée de chaque occurrence et les appareils concernés.

Recherchez des modèles dans les données et examinez l'état des appareils client et serveur pour vous aider à en déterminer la cause et à y remédier.