FAQ sur le système de santé

Publié: 2023-09-19

Voici quelques réponses aux questions fréquemment posées sur l'état de santé du système.

Comment puis-je vérifier une éventuelle perte de données ?

Les meilleurs indicateurs de perte de données sont les paquets abandonnés, les désynchronisations TCP et les taux de paquets ou de débit excessivement élevés.

- Consultez le tableau Capture Drop Rate (taux de chute de la capture) pour connaître les paquets abandonnés au niveau de l'interface de la carte réseau, du SPAN ou de la prise réseau.
- Vérifiez le graphique Desyncs pour les désynchronisations à l'échelle du système, qui indiquent que la synchronisation a été perdue lors du traitement d'une connexion TCP.
- Surveillez les graphiques suivants pour vous assurer que le système ExtraHop ne dépasse pas les seuils des capteurs :

  - Débit
  - Taux de paquets

  Un taux de paquets ou un débit élevé peut entraîner la chute de paquets au niveau de la source du span ou d'un agrégateur de span. Reportez-vous à la fiche technique des capteurs ExtraHop pour en savoir plus sur les taux et les limites des capteurs.

Comment surveiller la consommation des ressources ?

Le site Appareil Discover alloue des ressources mémoire pour la capture des paquets, l'exécution des déclencheurs, la transmission des données aux serveurs distants et l'enregistrement dans le magasin de données.

Consultez les graphiques suivants pour connaître la quantité de mémoire que le site Appareil Discover consacre à chaque zone de ressources sur une période donnée :

- Capture et allocation de la mémoire vive du datastore
- Allocation de la mémoire vive des déclencheurs et de la mémoire distante
- Charge de déclenchement du magasin de données

Comment puis-je vérifier les performances de mes déploiements RPCAP ?

Après la configuration initiale d'un déploiement de capture de paquets à distance (RPCAP), il est bon de s'assurer que votre déploiement fonctionne comme prévu.

- Consultez le graphique Transmis par l'homologue pour vous assurer que le volume de paquets envoyés au système ExtraHop correspond aux règles de filtrage spécifiées pour vos dispositifs homologues RPCAP.

- Surveillez le graphique Reçus par le système ExtraHop pour vous assurer que les systèmes ExtraHop reçoivent efficacement les paquets de leurs homologues RPCAP.

Mes déclencheurs fonctionnent-ils correctement ?

Pour tirer le meilleur parti de vos déclencheurs, assurez-vous que les nouveaux déclencheurs et les déclencheurs modifiés produisent des données précises sans dégrader les performances du système.

- Consultez le tableau Déclencheurs exécutés et abandonnés pour vous assurer que la quantité d'activité des déclencheurs correspond à vos attentes. Recherchez les sursauts d'activité des déclencheurs qui pourraient indiquer un comportement inefficace de la part d'un ou plusieurs déclencheurs. Ce graphique vous permet également de suivre le nombre de déclencheurs qui ont été supprimés de la file d'attente des déclencheurs. Le système ExtraHop peut abandonner un déclencheur de longue durée qui domine la consommation de ressources.
- Consultez le graphique Exécution des déclencheurs par déclencheur après avoir créé un nouveau déclencheur ou modifié un déclencheur existant pour vous assurer que le déclencheur est en cours d'exécution. Tout déclencheur consommant plus de ressources que la moyenne peut avoir un script mal optimisé qui affecte les performances.
- Consultez le graphique Exceptions par déclencheur pour afficher toutes les exceptions de déclencheurs non gérées. Les exceptions contribuent largement aux problèmes de performances du système et doivent être corrigées immédiatement.

Vous pouvez vérifier si vos déclencheurs de magasin de données, également appelés déclencheurs de pont, s'exécutent correctement à l'aide des graphiques suivants :

- Exécutions et abandons de déclencheurs de magasin de données
- Exceptions des déclencheurs de magasin de données par déclencheur

Comment les déclencheurs affectent-ils mon système ExtraHop ?

Outre le contrôle du bon fonctionnement de vos déclencheurs, la page Santé du système fournit des graphiques qui vous permettent de contrôler et d'évaluer l'impact de l'exécution des déclencheurs sur votre système ExtraHop.

- Consultez le graphique Charge de déclenchement pour afficher plusieurs mesures de la consommation de ressources par tous les déclencheurs en cours d'exécution. Recherchez les pics de consommation qui peuvent indiquer qu'un nouveau déclencheur a été introduit ou qu'un déclencheur existant rencontre des problèmes.
- Consultez le graphique Charge de déclenchement par déclencheur pour voir le nombre de cycles consommés par chaque déclencheur en cours d'exécution. Un déclencheur qui s'exécute rarement mais qui consomme plus de cycles que la moyenne peut entraîner l'élimination d'autres déclencheurs de la file d'attente.
- Consultez le graphique Cycles de déclenchement par thread pour voir le nombre de cycles que chaque thread a alloué aux opérations de déclenchement. Recherchez une consommation égale entre plusieurs threads. Des abandons de déclencheurs peuvent se produire si la consommation d'un thread est considérablement plus élevée que celle des autres.

Vous pouvez surveiller l'impact des déclencheurs de magasin de données, également appelés déclencheurs de pont, qui s'exécutent sur votre système ExtraHop à l'aide des graphiques suivants :

- Charge de déclenchement du magasin de données
- Exécutions et abandons de déclencheurs de magasin de données

Quelles sont les performances de mes flux de données ouverts ?

Vous pouvez surveiller les graphiques relatifs à l'état et aux performances des transmissions de flux de données ouverts (ODS) vers un syslog, une base de données ou un serveur tiers.

- Cliquez sur le graphique Messages envoyés pour afficher le nombre total de messages transmis par tous les flux de données actifs et le nombre d'erreurs survenues lors de ces transmissions.

Surveillez ce graphique pour vous assurer que les messages sont transmis comme prévu. Si aucun octet n'est envoyé, il peut y avoir un problème avec la configuration d'un flux de données ouvert ou d'un déclencheur ODS.

- Cliquez sur le graphique Débit des messages pour afficher le nombre total d'octets transmis par tous les flux de données actifs. Surveillez ce graphique pour vous assurer que les octets sont transmis comme prévu. Si aucun octet n'est envoyé, il se peut que la configuration d'un flux de données ouvert ou d'un déclencheur ODS pose problème.
- Consultez le graphique Connexions pour obtenir une vue d'ensemble des tentatives de connexion aux cibles ODS et des erreurs survenues au cours de ces tentatives.
- Surveillez le graphique Messages abandonnés par type de message distant pour connaître le taux d'abandon des messages avant qu'ils n'atteignent un magasin d'enregistrements ou une cible ODS. Un nombre élevé d'abandons peut indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. .
- Surveillez les graphiques Longueur de la file d'attente des messages à distance et Longueur de la file d'attente des messages de capture pour afficher le nombre de messages en attente dans les files d'attente ExtraHop Remote (exremote) et Capture (excap). Un nombre élevé de messages dans ces files d'attente peut indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.

Quelle est la capacité estimée du lookback ?

Le terme "lookback" fait référence à l'ancienneté des données historiques que vous êtes actuellement en mesure de consulter. Par exemple, vous pouvez consulter des intervalles de données d'une heure en remontant jusqu'à 9 jours en arrière.

- Surveillez le graphique Estimations des métriques de lookback des données pour déterminer la capacité de consultation actuelle estimée de votre Appareil Discover. Le graphique affiche les mesures de rétroaction pour des intervalles de 1 heure, 5 minutes et 30 secondes en fonction du débit d'écriture.

Combien de périphériques le système ExtraHop surveille-t-il ?

La page Santé du système fournit des graphiques qui vous aident à déterminer le nombre de périphériques L2, de passerelles, personnalisés et L3 surveillés par votre système ExtraHop.

- Consultez le tableau Périphériques actifs pour vous assurer que le nombre total de périphériques actifs surveillés est conforme aux prévisions.
- Consultez le tableau Total des dispositifs pour vous assurer que le nombre total de périphériques reconnus par le système ExtraHop, qu'ils soient actifs ou inactifs, est conforme aux prévisions.

Mes certificats SSL sont-ils décryptés comme prévu ?

Vous pouvez accéder à une liste de tous les certificats qui effectuent un décryptage sur le système ExtraHop en cliquant sur **Certificats** en haut de la page Santé du système.

- Consultez le tableau Détails du certificat pour vous assurer que les bons certificats SSL sont installés sur le système ExtraHop et pour afficher les mesures de chiffrement de chaque certificat. Les mesures de chiffrement vous aident à déterminer si vos certificats effectuent le déchiffrement comme prévu. Par exemple, vous pouvez vérifier le nombre de sessions chiffrées avec succès ou le nombre de sessions qui n'ont pas été déchiffrées en raison d'erreurs matérielles.

Comment ajouter des mesures de santé du système à un tableau de bord ?

Vous pouvez créer un nouveau tableau de bord personnalisé de mesures du système ou ajouter un seul graphique de santé du système à un tableau de bord existant. Localisez le graphique souhaité dans le tableau de bord Santé du système, cliquez sur son titre, puis sélectionnez **Copier sur ....**.

Conseil: Si vous n'êtes pas familiarisé avec la création et la modification de tableaux de bord, consultez notre guide des tableaux de bord.

.

Quels sont les autres outils qui peuvent m'aider à évaluer la santé du système ?

La section État et diagnostics des paramètres d'administration fournit des mesures sur l'état général du système ExtraHop et des outils de diagnostic qui permettent à l'assistance ExtraHop de dépanner les erreurs du système.

- Consultez les statistiques de santé pour voir les mesures qui indiquent l'efficacité du fonctionnement du système ExtraHop.
- Consultez le journal d'audit pour voir les données d'enregistrement des événements et pour modifier les paramètres syslog.
- En savoir plus sur les fichiers d'exception et sur la manière de les activer ou de les désactiver sur le système ExtraHop.
- Découvrez les scripts d'assistance et comment les télécharger et les exécuter sur le système ExtraHop.

Vous pouvez également consulter les ressources suivantes pour en savoir plus sur l'état du système :

- Visite guidée de l'état de santé du système : Évaluer les performances des déclencheurs
- Offre groupée ExtraHealth