FAQ sur l'état du système

Publié: 2024-09-26

Voici quelques réponses aux questions fréquemment posées sur la santé du système.

Comment puis-je vérifier s'il n'y a pas de perte de données ?

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

- Vérifiez le Taux de perte de capture graphique des paquets déposés au niveau de l'interface de la carte réseau, du SPAN ou de l'interface réseau
- Vérifiez le Désynchronisations graphique des désynchronisations à l'échelle du système, qui indique 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 sondes :
  - Débit
  - Débit de paquets

  Un débit ou un débit de paquets élevé peuvent entraîner la perte de paquets à la source de span ou à un agrégateur de span. Reportez-vous à la Fiche technique des capteurs ExtraHop pour en savoir plus sur les débits et les limites des sondes.

Comment puis-je surveiller la consommation de ressources ?

Le Découvrez l'appareil alloue des ressources mémoire pour capturer des paquets, exécuter des déclencheurs, transmettre des données à des serveurs distants et enregistrer dans la banque de données.

Consultez les tableaux suivants pour connaître la quantité de mémoire que Découvrez l'appareil est dédié à chaque domaine de ressources sur une période donnée :

- Capture et allocation de tas de données
- Déclencheur et allocation de tas à distance
- Chargement déclencheur de la banque 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 conseillé de s' assurer que votre déploiement fonctionne comme prévu.

- Vérifiez le Transmis par Peer graphique pour s'assurer que le volume de paquets envoyés au système ExtraHop correspond aux règles de filtrage spécifiées pour vos périphériques homologues RPCAP.
- Surveillez le Reçu par le système ExtraHop graphique pour s'assurer que les systèmes ExtraHop reçoivent efficacement les paquets des homologues RPCAP.

Mes déclencheurs fonctionnent-ils correctement ?

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

- Consultez le Le déclencheur s'exécute et s'arrête tableau pour vous assurer que le niveau d'activité du déclencheur correspond à vos attentes. Recherchez les poussées d'activité des déclencheurs qui pourraient indiquer un comportement inefficace dû à 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 supprimer un déclencheur de longue durée qui domine la consommation de ressources.
- Consultez le Le déclencheur s'exécute par déclencheur graphique une fois que vous avez créé un nouveau déclencheur ou modifié un déclencheur existant pour vous assurer qu' il fonctionne. Tout déclencheur consommant plus de ressources que la moyenne peut avoir un script mal optimisé qui affecte les performances.
- Vérifiez le Déclenchez des exceptions par déclencheur graphique pour afficher toutes les exceptions de déclencheur non gérées. Les exceptions contribuent largement aux problèmes de performances du système et doivent être corrigées immédiatement.

Vous pouvez vérifier si les déclencheurs de votre banque de données, également appelés déclencheurs de pont, fonctionnent correctement à l'aide des graphiques suivants :

- Le déclencheur de la banque de données s'exécute et s'arrête
- Exceptions de déclenchement de la banque de données par déclencheur

Comment les déclencheurs affectent-ils mon système ExtraHop ?

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

- Consultez le Charge du déclencheur graphique pour afficher plusieurs mesures de la consommation de ressources par tous les déclencheurs en cours d'exécution. Surveillez les pics de consommation qui peuvent indiquer qu'un nouveau déclencheur a été introduit ou qu'un déclencheur existant rencontre des problèmes.
- Vérifiez le Déclencheur, charge par gâchette graphique pour afficher le nombre de cycles consommés par chaque déclencheur en cours d'exécution. Un déclencheur qui s'exécute rarement mais consomme plus de cycles que la moyenne peut entraîner la suppression d'autres déclencheurs de la file d'attente.
- Vérifiez le Cycles de déclenchement par fil graphique pour afficher le nombre de cycles que chaque thread a alloués aux opérations de déclencheur. Veillez à ce que la consommation soit uniforme entre les différents fils de discussion. Des chutes de déclenchement peuvent survenir si la consommation d'un thread est considérablement plus élevée que celle des autres.

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

- Chargement déclencheur de la banque de données
- Le déclencheur de la banque de données s'exécute et s'arrête

Quelles sont les performances de mes flux de données ouvertes ?

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

- Cliquez sur Messages envoyés graphique 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 Débit des messages graphique 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 peut y avoir un problème avec la configuration d'un flux de données ouvert ou d'un déclencheur ODS.
- Vérifiez le Connexions graphique pour une vue d'ensemble des tentatives de connexion aux cibles ODS et des erreurs survenues lors de ces tentatives.
- Surveillez le Messages supprimés par type de télécommande graphique pour afficher le taux de suppression des messages avant qu'ils n'atteignent un espace de stockage des enregistrements ou une cible ODS. Un nombre élevé de pertes peut indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.
- Surveillez le Longueur de la file d'attente de messages Exremote et Longueur de la file de messages de capture graphiques 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 de rétrospective estimée ?

La fonction Lookback fait référence à la date à laquelle vous pouvez actuellement consulter des données historiques. Par exemple, vous pourriez être en mesure de consulter des intervalles d'une heure de données remontant à 9 jours.

- Surveillez le Estimations rétrospectives des données métriques graphique pour déterminer la capacité de rétrospective estimée actuelle de votre Découvrez l'appareil. Le graphique affiche les statistiques rétrospectives pour des intervalles de 1 heure, 5 minutes et 30 secondes en fonction du débit d'écriture.

Combien d'appareils sont surveillés par le système ExtraHop ?

La page État du système fournit des graphiques qui vous aident à déterminer le nombre d'appareils L2, de passerelle, personnalisés et L3 qui sont surveillés par votre système ExtraHop.

- Vérifiez le Appareils actifs graphique pour s'assurer que le nombre total d'appareils actifs surveillés est conforme aux attentes.

Mes certificats TLS sont-ils déchiffrés comme prévu ?

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

- Vérifiez le Détails du certificat tableau pour s'assurer que les certificats TLS appropriés sont installés sur le système ExtraHop et pour afficher les mesures de chiffrement pour 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 indicateurs de santé du système à un tableau de bord ?

Vous pouvez créer un nouveau tableau de bord personnalisé des mesures du système ou ajouter un seul tableau de santé du système à un tableau de bord existant. Localisez le graphique souhaité dans le tableau de bord de l'état du système, cliquez sur le titre, puis sélectionnez **Copier vers...**. Sélectionnez **Nouveau tableau de bord** ou sélectionnez un tableau de bord existant.

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

Quels autres outils peuvent m'aider à évaluer l'état de 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 Assistance ExtraHop pour résoudre les erreurs du système.

- Vérifiez statistiques sur la santé pour afficher les mesures qui indiquent l'efficacité opérationnelle du système ExtraHop.
- Vérifiez le journal d'audit pour consulter les données de journalisation des événements et modifier les paramètres du Syslog.
- En savoir plus sur fichiers d'exceptions et comment les activer ou les désactiver sur le système ExtraHop.
- En savoir plus sur scripts de support 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 de santé du système :

- Procédure pas à pas sur l'état du système : évaluez les performances des déclencheurs