tableau de bord de l'état du système

Publié: 2024-09-26

Le tableau de bord de l'état du système fournit une grande collection de graphiques qui vous permettent de vous assurer que votre système ExtraHop fonctionne comme prévu, de résoudre les problèmes et d' évaluer les domaines qui affectent les performances. Par exemple, vous pouvez surveiller le nombre de paquets traités par le système ExtraHop pour vous assurer que les paquets sont capturés en permanence.

Chaque graphique du tableau de bord des performances du réseau contient des visualisations des données de performance du système qui ont été générées sur intervalle de temps sélectionné, organisé par région.

Le tableau de bord System Health est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord de l'état du système et ajoutez-le à un tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Note: La page des paramètres d'administration fournit également informations d'état et outils de diagnostic pour tous les systèmes ExtraHop.

Naviguez dans le tableau de bord de l'état du système

Accédez à la page État du système en cliquant sur l'icône Paramètres du système ou en cliquant **Tableaux de bord** depuis le haut de la page. Le tableau de bord de l'état du système affiche automatiquement des informations sur le système ExtraHop auquel vous êtes connecté. Si vous consultez le tableau de bord de l'état du système depuis une console, vous pouvez cliquer sur le sélecteur de site en haut de la page pour afficher les données d'un site spécifique ou de tous les sites de votre environnement.

Les graphiques du tableau de bord de l'état du système sont répartis dans les sections suivantes :

Découverte d'appareils

Consultez le nombre total d'appareils sur votre réseau. Découvrez quels appareils ont été découverts et combien d'entre eux sont actuellement actifs.

Flux de données

Évaluez l'efficacité du processus de collecte de données Wire Data à l'aide de graphiques relatifs au débit, au débit de paquets, aux désynchronisations et aux pertes de capture.

Enregistrements

Afficher le nombre total d'enregistrements envoyés vers un espace de stockage des enregistrements joint.

DÉCLENCHEURS

Surveillez l'impact des déclencheurs sur votre système ExtraHop. Découvrez à quelle fréquence les déclencheurs sont exécutés, à quelle fréquence ils échouent et quels déclencheurs sollicitent le plus votre processeur.

Flux de données ouvert et magasin d'enregistrements

Suivez l'activité des transmissions de flux de données ouvertes (ODS) à destination et en provenance de votre système. Consultez le nombre total de connexions distantes, le débit des messages et les informations relatives à des cibles distantes spécifiques.

Certificats TLS

Consultez les informations d'état de tous les certificats TLS de votre système ExtraHop.

Capture de paquets à distance (RPCAP)

Afficher le nombre de paquets et de trames envoyés et reçus par les homologues RPCAP.

Indicateurs de santé avancés

Suivez l'allocation des tas liée à la capture des données, à la banque de données du système, aux déclencheurs et aux transmissions à distance. Surveillez le débit d'écriture, la taille de l'ensemble de travail et l'activité des déclencheurs sur la banque de données système.

Découverte d'appareils

Le Découverte d'appareils La section du tableau de bord de l'état du système fournit une vue du nombre total d'appareils sur votre réseau. Découvrez quels types d'appareils sont connectés et combien d'entre eux sont actuellement actifs.

Le Découverte d'appareils La section fournit les graphiques suivants :

- Appareils actifs

Appareils actifs

Un graphique en aires qui affiche le nombre de périphériques L2, L3, de passerelle et personnalisés qui ont communiqué activement sur le réseau pendant l'intervalle de temps sélectionné. À côté du graphique en aires, un diagramme de valeurs affiche le nombre de périphériques L2, L3, de passerelle et personnalisés actifs au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Surveillez ce graphique après avoir apporté des modifications à la configuration du SPAN pour vous assurer qu'il n'y ait aucune conséquence imprévue susceptible de mettre le système ExtraHop en mauvais état. Par exemple, l'inclusion accidentelle d'un réseau peut mettre à rude épreuve les capacités du système ExtraHop en consommant davantage de ressources et en nécessitant une plus grande gestion des paquets, ce qui entraîne de mauvaises performances. Vérifiez que le système ExtraHop surveille le nombre attendu d'appareils actifs.

Flux de données

Le Flux de données Une section du tableau de bord de l'état du système vous permet d' observer l'efficacité du processus de collecte de données Wire Data à l'aide de graphiques relatifs au débit, au débit de paquets, aux désynchronisations et aux pertes de capture.

Le Flux de données La section fournit les graphiques suivants :

- Débit
- Débit par interface
- Débit de paquets
- Débit de paquets par interface
- Erreurs de paquets par interface
- Flux analysés
- Désynchronisations
- Taux de perte de capture
- Métriques écrites sur le disque (Log Scale)
- Estimations rétrospectives des données métriques

Débit

Un graphique en aires illustrant le débit des paquets entrants sur l' intervalle de temps sélectionné, exprimé en octets par seconde. Le graphique affiche les informations de débit pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3.

Comment ces informations peuvent vous aider

Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un débit élevé peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur d'span. De même, un grand nombre de doublons L2 ou L3 peut également indiquer un problème au niveau de la source ou de l' agrégateur d'intervalles et peut entraîner des mesures asymétriques ou incorrectes.

Le taux acceptable d'octets par seconde dépend de votre produit. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le taux d'octets par seconde est trop élevé.

Débit par interface

Un graphique en courbes illustrant le débit des paquets entrants, répertorié par chaque interface configurée sur la sonde. Le débit est exprimé en octets par seconde pendant l'intervalle de temps sélectionné. Le graphique affiche les informations de débit pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3.

Lorsque vous visualisez plusieurs capteurs depuis une console ExtraHop, le graphique représente le taux de transfert moyen agrégé à partir d'interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Le dépassement des seuils de produit peut entraîner une perte de données. Par exemple, un débit élevé peut entraîner la perte de paquets à la source de span ou à un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur de span et peuvent entraîner des mesures biaisées ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous à la Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le débit de paquets par seconde est trop élevé.

Surveillez ce graphique pour résoudre les problèmes de débit des paquets à un niveau granulaire et ajuster la configuration de l'interface si nécessaire.

Débit de paquets

Un graphique en aires qui affiche le taux de paquets entrants, exprimé en paquets par seconde. Le graphique affiche les informations relatives au débit des paquets analysés et filtrés, ainsi que les doublons L2 et L3.

Comment ces informations peuvent vous aider

Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un débit de paquets élevé peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur d'intervalles et peuvent entraîner des mesures asymétriques ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le taux de paquets par seconde est trop élevé.

Débit de paquets par interface

Un graphique en courbes qui affiche le taux de paquets entrants et un graphique à colonnes qui affiche le nombre de paquets abandonnés, répertoriés par chaque interface configurée sur la sonde. Le débit de paquets est exprimé en paquets reçus par seconde pendant l'intervalle de temps sélectionné. Le graphique affiche les informations relatives au débit des paquets analysés et filtrés, ainsi que des doublons L2 et L3.

Lorsque vous visualisez plusieurs capteurs depuis une console ExtraHop, le graphique représente le débit de paquets agrégé et le nombre de paquets abandonnés par les interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Le dépassement des seuils de produit peut entraîner une perte de données. Par exemple, un débit de paquets élevé peut entraîner la suppression de paquets à la source de span ou à un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur de span et peuvent entraîner des mesures biaisées ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous à Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le débit de paquets par seconde est trop élevé.

Surveillez ce graphique pour résoudre les problèmes de débit de paquets à un niveau granulaire et ajuster la configuration de l'interface si nécessaire.

Erreurs de paquets par interface

Un graphique en courbes qui affiche le nombre d'erreurs de paquets reçues pendant l'intervalle de temps sélectionné, répertoriées par chaque interface configurée sur la sonde. Le graphique affiche les informations relatives aux erreurs de paquets pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3 .

Lorsque vous visualisez plusieurs capteurs à partir d'une console ExtraHop, le graphique représente le nombre agrégé d'erreurs de paquets survenues sur des interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Surveillez ce graphique pour résoudre les erreurs de paquets à un niveau granulaire. L'augmentation du nombre d'erreurs de paquets peut entraîner une perte de données. Assurez-vous que les paquets sont envoyés comme prévu et modifiez la configuration de l'interface si nécessaire.

Flux analysés

Un graphique en courbes qui affiche le nombre de flux analysés par le système ExtraHop au cours de l'intervalle de temps sélectionné. Le graphique indique également le nombre de flux unidirectionnels survenus au cours de la même période. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de flux analysés et unidirectionnels survenus au cours de l'intervalle de temps sélectionné. Un flux est un ensemble de paquets qui font partie d'une transaction entre deux points de terminaison via un protocole tel que TCP, UDP ou ICMP.

Comment ces informations peuvent vous aider
Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un nombre élevé de flux analysés peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur de span.

Désynchronisations

Un graphique en courbes qui affiche les occurrences de désynchronisations à l'échelle du système sur le système ExtraHop au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de désynchronisations survenues au cours de l'intervalle de temps sélectionné. Une désynchronisation se produit lorsque le flux de données ExtraHop supprime un paquet TCP et, par conséquent, n'est plus synchronisé avec une connexion TCP.

Comment ces informations peuvent vous aider
Un grand nombre de désynchronisations peut indiquer la perte de paquets sur l'interface de surveillance, le SPAN ou le réseau.

Si les ajustements apportés à votre SPAN ne réduisent pas le nombre important de désynchronisations, contactez Assistance ExtraHop.

Paquets tronqués

Un graphique en courbes qui affiche les occurrences de paquets tronqués sur le système ExtraHop au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de paquets tronqués survenus au cours de l'intervalle de temps sélectionné. Un paquet tronqué se produit lorsque la longueur totale réelle du paquet est inférieure à la longueur totale indiquée dans l'en-tête IP.

Comment ces informations peuvent vous aider
Les paquets tronqués peuvent indiquer un découpage en tranches. Une sonde rejette tous les paquets tronqués qu'elle reçoit, ce qui peut provoquer désynchronise à se produire.

Taux de perte de capture

Un graphique en courbes qui affiche le pourcentage de paquets déposés sur l' interface de la carte réseau sur un système ExtraHop sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Les pertes de paquets se produisent souvent lorsque les seuils des sondes sont dépassés. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop.

Charge de capture

Un graphique en courbes qui affiche le pourcentage de cycles du système ExtraHop consommés par les threads de capture actifs sur l'intervalle de temps sélectionné, en fonction de la durée totale du thread de capture. Cliquez sur le lien associé Charge de capture moyenne graphique permettant d' effectuer une analyse détaillée par thread et de déterminer quels threads consomment le plus de ressources.

Comment ces informations peuvent vous aider
Surveillez les pics ou l'augmentation de la charge de capture pour vérifier si vous vous approchez des limites de la sonde. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir les limites de votre système ExtraHop.

Métriques écrites sur le disque (Log Scale)

Un graphique en courbes qui affiche la quantité d'espace consommée par les métriques écrites sur le disque au cours de l'intervalle de temps sélectionné, exprimée en octets par seconde. Comme il existe une large plage entre les points de données, l'utilisation du disque est affichée sur une échelle logarithmique.

Comment ces informations peuvent vous aider
Il est important de connaître la quantité d'espace consommée par les métriques dans votre banque de données. La quantité d'espace disponible dans votre banque de données aura une incidence sur la quantité de lookback disponible. Si certaines mesures consomment trop d' espace, vous pouvez examiner les déclencheurs associés pour voir si vous pouvez modifier le déclencheur pour le rendre plus efficace.

Estimations rétrospectives des données métriques

Affiche les statistiques estimées de la banque de données sur le système ExtraHop. Les métriques Lookback sont disponibles par intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes en fonction du débit d'écriture, exprimé en octets par seconde.

Comment ces informations peuvent vous aider

Reportez-vous à ce tableau pour déterminer jusqu'où vous pouvez rechercher des données historiques pour des intervalles de temps donnés. Par exemple, vous pourriez être en mesure de consulter des intervalles d'une heure de données remontant à 9 jours.

Enregistrements

Le Enregistrements la section du tableau de bord System Health vous permet d'observer l'efficacité du processus de collecte de données filaires à l'aide de graphiques relatifs au nombre d' enregistrements et au débit.

Le Flux de données La section fournit les graphiques suivants :

- Nombre d'enregistrements
- Débit record

Nombre d'enregistrements

Un graphique en courbes qui affiche le nombre d'enregistrements envoyés à un espace de stockage des enregistrements au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total d' enregistrements envoyés au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Un nombre extrêmement élevé d'enregistrements envoyés à un espace de stockage des enregistrements peut entraîner de longues files d'attente de messages et la suppression de messages dans l'espace de stockage des enregistrements. Consultez les graphiques dans le Flux de données ouvert et magasin d'enregistrements section du tableau de bord System Health pour plus d'informations sur les transmissions dans l'espace de stockage des enregistrements.

Débit record

Un graphique en courbes qui affiche le nombre d'enregistrements en octets envoyés à un espace de stockage des enregistrements. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total d'enregistrements envoyés en octets sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Ce graphique ne reflète pas les ajustements de taille basés sur la compression ou la déduplication et ne doit pas être référencé pour estimer les coûts de l'espace de stockage des enregistrements. Un débit d'enregistrement extrêmement élevé peut entraîner de longues files d'attente de messages et la suppression de messages dans l'espace de stockage des enregistrements. Consultez les graphiques dans le Flux de données ouvert et magasin d'enregistrements section du tableau de bord System Health pour plus d'informations sur les transmissions dans l'espace de stockage des enregistrements.

DÉCLENCHEURS

Le DÉCLENCHEURS la section du tableau de bord de l'état du système vous permet de surveiller l'impact des déclencheurs sur votre système. Découvrez à quelle fréquence les déclencheurs sont exécutés, à quelle fréquence ils échouent et quels déclencheurs sollicitent le plus votre processeur.

Le DÉCLENCHEURS La section fournit les graphiques suivants :

- Charge du déclencheur
- Retard de déclenchement
- Le déclencheur s'exécute et s'arrête
- Détails du déclencheur
- Déclencheur, charge par gâchette
- Le déclencheur s'exécute par déclencheur
- Déclenchez des exceptions par déclencheur
- Cycles de déclenchement par fil

Charge du déclencheur

Un graphique en courbes qui affiche le pourcentage de cycles de processeur alloués aux processus de déclenchement qui ont été consommés par les déclencheurs pendant l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Surveillez les pics ou la croissance de la charge du déclencheur, en particulier après avoir créé un nouveau déclencheur ou modifié un déclencheur existant. Si vous remarquez l'une ou l'autre de ces conditions, consultez le Déclencheur, charge par gâchette graphique pour voir quels déclencheurs consomment le plus de ressources.

Retard de déclenchement

Un graphique à colonnes qui affiche les délais de déclenchement maximaux survenus au cours de l'intervalle de temps sélectionné en millisecondes. À côté du graphique à colonnes, un diagramme de valeurs affiche le délai de déclenchement le plus long enregistré au cours de l'intervalle de temps sélectionné. Un délai de déclenchement est le délai entre le moment où un événement déclencheur est capturé et le moment où un thread de déclenchement est créé pour cet événement.

Comment ces informations peuvent vous aider

Les longs délais de déclenchement peuvent indiquer des problèmes de traitement, consultez le Déclenchez des exceptions par déclencheuret Déclencheur, charge par gâchette des graphiques pour voir quel déclencheur commet le plus d'exceptions non gérées et lesquels consomment le plus de ressources.

Le déclencheur s'exécute et s'arrête

Un graphique en courbes et à colonnes dans lequel le graphique en courbes indique le nombre de fois que les déclencheurs ont été exécutés, et le graphique à colonnes qui l'accompagne indique le nombre de fois où les déclencheurs ont été supprimés, sur l'intervalle de temps sélectionné. À côté du graphique linéaire et à colonnes, un diagramme de valeurs affiche le nombre total d'exécutions et de baisses de déclencheurs survenues au cours de l'intervalle de temps sélectionné. Ces graphiques fournissent un aperçu global de tous les déclencheurs actuellement en cours d'exécution sur le système ExtraHop.

Comment ces informations peuvent vous aider
Recherchez les pics dans le graphique linéaire et à colonnes et examinez les facteurs déclencheurs qui ont entraîné ces pics. Par exemple, vous remarquerez peut-être une augmentation de l'activité si un déclencheur a été modifié ou si un nouveau déclencheur a été activé. Consultez le Le déclencheur s'exécute par déclencheur graphique pour voir quels déclencheurs s'exécutent le plus fréquemment.

Détails du déclencheur

Un graphique en listes qui affiche les déclencheurs individuels ainsi que le nombre de cycles, d'exécutions et d' exceptions attribués à chacun sur l'intervalle de temps sélectionné. Par défaut, la liste des déclencheurs est triée par ordre décroissant par cycle de déclencheur.

Comment ces informations peuvent vous aider
Identifiez les déclencheurs qui consomment le plus de cycles. Les déclencheurs qui s'exécutent trop fréquemment ou qui consomment plus de cycles qu' ils ne le devraient peuvent être affectés à un plus grand nombre de sources que nécessaire. Assurez-vous que tout déclencheur hyperactif est uniquement attribué à la source spécifique à partir de laquelle vous devez collecter des données.

Déclencheur, charge par gâchette

Un graphique en courbes qui affiche le pourcentage de cycles de processeur alloués aux processus de déclenchement qui ont été consommés par les déclencheurs pendant l'intervalle de temps sélectionné, listés par nom de déclencheur.

Comment ces informations peuvent vous aider
Identifiez les déclencheurs qui consomment le plus de cycles. Les déclencheurs qui consomment plus de cycles qu'ils ne le devraient peuvent être affectés à un plus grand nombre de sources que nécessaire. Assurez-vous que tout déclencheur hyperactif est uniquement attribué à la source spécifique à partir de laquelle vous devez collecter des données.

Le déclencheur s'exécute par déclencheur

Un graphique en courbes qui affiche le nombre de fois que chaque déclencheur actif s'est exécuté sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Recherchez les déclencheurs qui s'exécutent plus fréquemment que prévu, ce qui peut indiquer que le déclencheur est attribué de manière trop large. Un déclencheur attribué à toutes les applications ou à tous les appareils peut avoir un coût élevé en termes de performances. Un déclencheur attribué à un groupe déquipements qui a été étendu peut collecter des métriques que vous ne souhaitez pas. Pour minimiser l'impact sur les performances, un déclencheur doit être attribué uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

Une activité élevée peut également indiquer qu' un déclencheur fonctionne plus que nécessaire. Par exemple, un déclencheur peut s'exécuter sur plusieurs événements pour lesquels il serait plus efficace de créer des déclencheurs distincts, ou un script de déclenchement peut ne pas respecter les directives de script recommandées, telles que décrites dans le Guide des meilleures pratiques en matière de déclencheurs.

Déclenchez des exceptions par déclencheur

Un graphique en courbes qui affiche le nombre d'exceptions non gérées, triées par déclencheur, survenues sur le système ExtraHop au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Les exceptions aux déclencheurs sont la principale cause des problèmes de performances des déclencheurs. Si ce graphique indique qu'une exception de déclencheur s'est produite , vous devez immédiatement examiner le déclencheur.

Cycles de déclenchement par fil

Un graphique en courbes qui affiche le nombre de cycles de déclenchement consommés par les déclencheurs pour un thread.

Comment ces informations peuvent vous aider
Des baisses de déclenchement peuvent se produire si la consommation d'un thread est considérablement supérieure à celle des autres, même si le pourcentage de consommation des threads est faible. Recherchez une consommation de cycle uniforme entre les threads.

Flux de données ouvert et magasin d'enregistrements

La section Open Data Stream (ODS) and Recordstore du tableau de bord System Health vous permet de suivre l'activité des transmissions ODS et de l'espace de stockage des enregistrements vers et depuis votre système. Vous pouvez également afficher le nombre total de connexions à distance, le débit des messages et les détails relatifs à des cibles distantes spécifiques.

Le Open Data Stream (ODS) et Recordstore La section fournit les graphiques suivants :

- Débit des messages
- Messages envoyés
- Messages supprimés par type de télécommande
- Erreurs d'envoi de message

- Connexions
- Longueur de la file d'attente de messages Exremote par cible
- Longueur de la file d'attente de messages Excap par type de télécommande
- Détails de la cible

Débit des messages

Un graphique en courbes qui affiche le débit des données des messages distants, exprimé en octets. À côté du graphique en courbes, un diagramme de valeurs affiche le débit moyen des données des messages distants sur l'intervalle de temps sélectionné. Les messages distants sont des transmissions envoyées à un espace de stockage des enregistrements ou à des systèmes tiers depuis le système ExtraHop via un flux de données ouvert (ODS).

Comment ces informations peuvent vous aider
Surveillez ce graphique pour vous assurer que les octets sont transférés comme prévu. Si vous constatez un faible débit, cela peut être dû à un problème de configuration d'un ODS ou d'un espace de stockage des enregistrements rattaché. Des baisses de débit importantes peuvent indiquer des problèmes liés à vos flux de données.

Messages envoyés

Un graphique en courbes qui affiche le taux moyen d'envoi de messages distants depuis le système ExtraHop vers un espace de stockage des enregistrements ou une cible de flux de données ouvert (ODS). À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de messages envoyés au cours de l' intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Surveillez ce graphique pour vous assurer que les paquets sont envoyés comme prévu. Si aucun paquet n'est envoyé, il se peut qu'il y ait un problème de configuration d'un ODS ou d'un espace de stockage des enregistrements attaché.

Messages supprimés par type de télécommande

Un graphique en courbes qui affiche le taux moyen de messages distants abandonnés avant d'atteindre un espace de stockage des enregistrements ou une cible ODS.

Comment ces informations peuvent vous aider
Les messages supprimés indiquent des problèmes de connectivité avec la cible distante. Un nombre élevé de pertes peut également indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.

Erreurs d'envoi de message

Un graphique en courbes qui affiche le nombre d'erreurs survenues lors de l'envoi d'un message distant à un espace de stockage des enregistrements ou à une cible ODS. Surveillez ce graphique pour vous assurer que les paquets sont envoyés comme prévu. Les erreurs de transmission peuvent avoir les conséquences suivantes :

Erreurs du serveur cible

Nombre d'erreurs renvoyées au système ExtraHop par les magasins de disques ou les cibles ODS. Ces erreurs se sont produites sur le serveur cible et n'indiquent aucun problème avec le système ExtraHop.

Messages supprimés dans la file d'attente complète

Nombre de messages envoyés aux magasins de disques et aux cibles ODS qui ont été supprimés parce que la file d'attente de messages sur le serveur cible était pleine. Un nombre élevé de messages supprimés peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Regardez le Longueur de la file d'attente de messages

Exremote par cible et le Détails de la cible des graphiques pour voir si vos erreurs de transmission peuvent être liées à une longue file d'attente de messages.

Messages supprimés qui ne correspondent pas à la cible

Nombre de messages distants supprimés parce que le système distant spécifié dans le script déclencheur Open Data Stream (ODS) ne correspond pas au nom configuré sur la page Open Data Streams dans les paramètres d'administration. Assurez-vous que les noms des systèmes distants sont cohérents dans les scripts de déclencheur et les paramètres d' administration.

Erreurs de décodage Messages supprimés

Nombre de messages supprimés en raison de problèmes d'encodage interne entre ExtraHop Capture (excap) et ExtraHop Remote (exremote).

Connexions

Un graphique en courbes et en colonnes dans lequel le graphique en courbes indique le nombre de tentatives effectuées par le système pour se connecter à un serveur cible distant et le graphique à colonnes qui l'accompagne indique le nombre d'erreurs survenues à la suite de ces tentatives. À côté du graphique à lignes et à colonnes, un diagramme de valeurs affiche le nombre total de tentatives de connexion et d'erreurs de connexion survenues au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Identifiez les serveurs cibles qui nécessitent un nombre inhabituel de tentatives de connexion ou qui génèrent un nombre disproportionné d'erreurs de connexion. Un pic de tentatives de connexion peut indiquer que le serveur cible n'est pas disponible.

Longueur de la file d'attente de messages Exremote par cible

Un graphique en courbes qui affiche le nombre de messages dans la file d'attente ExtraHop Remote (exremote) en attente de traitement par le système ExtraHop.

Comment ces informations peuvent vous aider

Un nombre élevé de messages dans la file d'attente peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Reportez-vous à la valeur Exremote Full Queue Dropped Messages dans le Erreurs d'envoi de message tableau pour déterminer si des messages ont été envoyés.

Longueur de la file d'attente de messages Excap par type de télécommande

Un graphique en courbes qui affiche le nombre de messages cibles distants dans la file d'attente ExtraHop Capture (excap) en attente de traitement par le système ExtraHop.

Comment ces informations peuvent vous aider

Un nombre élevé de messages dans la file d'attente peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.

Reportez-vous au Messages supprimés par type de télécommande tableau pour déterminer si des messages ont été envoyés.

Détails de la cible

Un graphique en listes qui affiche les mesures suivantes relatives à l'espace de stockage des enregistrements ou aux cibles distantes ODS sur l'intervalle de temps sélectionné : nom de la cible, octets de message cible envoyés, erreurs du serveur cible, messages supprimés dans la file d'attente complète, erreurs de décodage, messages supprimés, tentatives de connexion au serveur cible et erreurs de connexion au serveur cible.

Comment ces informations peuvent vous aider
Si des erreurs de message sont signalées dans le Messages envoyés graphique, les détails de ce graphique peuvent vous aider à déterminer la cause première des erreurs de message à distance.

Certificats TLS

La section Certificats TLS du tableau de bord de l'état du système vous permet de consulter les informations d' état de tous les certificats TLS de votre système.

Le Certificats TLS la section fournit le tableau suivant :

- Détails du certificat

Détails du certificat

Un graphique en listes qui affiche les informations suivantes pour chaque certificat :

Sessions déchiffrées
Le nombre de sessions qui ont été déchiffrées avec succès.

Sessions non prises en charge
Le nombre de sessions qui n'ont pas pu être déchiffrées à l'aide d'une analyse passive, telle que l'échange de clés DHE.

Sessions isolées
Le nombre de sessions qui n'ont pas été déchiffrées ou qui n'ont été que partiellement déchiffrées en raison de désynchronisations.

Sessions directes
Le nombre de sessions qui n'ont pas été déchiffrées en raison d'erreurs matérielles, telles que celles causées par un dépassement des spécifications du matériel d'accélération TLS.

Sessions déchiffrées avec un secret partagé
Le nombre de sessions qui ont été déchiffrées à l'aide d'une clé secrète partagée.

Comment ces informations peuvent vous aider
Surveillez ce graphique pour vous assurer que les certificats TLS appropriés sont installés sur le système ExtraHop et qu'ils effectuent le déchiffrement comme prévu.

Capture de paquets à distance (RPCAP)

La section Remote Packet Capture (RPCAP) du tableau de bord System Health vous permet de visualiser le nombre de paquets et de trames envoyés par des homologues RPCAP et reçus par le système ExtraHop.

Le Capture de paquets à distance (RPCAP) La section fournit les graphiques suivants :

- Transmis par Peer
- Reçu par le système ExtraHop

Transmis par Peer

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames transférés par un homologue RPCAP :

Paquets transférés
Le nombre de paquets qu'un pair RPCAP a tenté de transférer vers un système ExtraHop .

Paquets d'interface du redirecteur
Nombre total de paquets consultés par le redirecteur. Les redirecteurs des appareils RPCAP se coordonneront entre eux pour empêcher plusieurs appareils d'envoyer le même paquet . Il s'agit du

nombre de paquets qui ont été visualisés avant que les trames ne soient supprimées pour réduire le trafic transféré, et avant que les trames ne soient supprimées par des filtres définis par l'utilisateur.

Forwarder Kernel Frame Drops

Nombre d'images supprimées parce que le noyau de l'homologue RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées par le noyau pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur.

Abandon de l'interface du redirecteur

Nombre de paquets supprimés parce que le redirecteur RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur .

Comment ces informations peuvent vous aider

Chaque fois que vous voyez des paquets abandonnés par l'homologue RPCAP, cela indique qu'il y a un problème avec le logiciel RPCAP.

Reçu par le système ExtraHop

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames reçus par un système ExtraHop depuis un homologue RPCAP (Remote Packet Capture) :

Octets encapsulés

Taille totale de tous les paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop, en octets. Ces informations vous indiquent le volume de trafic que le redirecteur RPCAP ajoute à votre réseau.

Paquets encapsulés

Le nombre de paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop.

Octets de tunnel

Taille totale des paquets, sans compter les en-têtes d'encapsulation, que le système ExtraHop a reçus d'un équipement RPCAP, en octets.

Paquets de tunnels

Le nombre de paquets que le système ExtraHop a reçus d'un homologue RPCAP. Ce nombre doit être très proche du nombre de paquets transférés dans le tableau des paquets envoyés par un périphérique distant. S'il y a un écart important entre ces deux nombres, des paquets tombent entre l'équipement RPCAP et le système ExtraHop.

Comment ces informations peuvent vous aider

Le suivi des paquets et des octets encapsulés est un bon moyen de s'assurer que les redirecteurs RPCAP n'imposent pas de charge inutile à votre réseau. Vous pouvez surveiller les paquets et les octets du tunnel pour vous assurer que le système ExtraHop reçoit tout ce que l' équipement RPCAP envoie.

Indicateurs de santé avancés

La section Advanced Health Metrics du tableau de bord de l'état du système vous permet de suivre l'allocation de tas liée à la capture de données, à la banque de données du système, aux déclencheurs et aux transmissions à distance. Surveillez le débit d'écriture, la taille de l'ensemble de travail et l'activité du déclencheur sur la banque de données du système.

Le Indicateurs de santé avancés La section fournit les graphiques suivants :

- Capture et allocation de tas de données
- Déclencheur et allocation de tas à distance
- Stocker le débit d'écriture

- Taille de l'ensemble de travail
- Chargement déclencheur de la banque de données
- Le déclencheur de la banque de données s'exécute et s'arrête
- Exceptions de déclenchement de la banque de données par déclencheur

Capture et allocation de tas de données

Un graphique en courbes qui affiche la quantité de mémoire que le système ExtraHop consacre à la capture de paquets réseau et à la banque de données.

Comment ces informations peuvent vous aider
Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Déclencheur et allocation de tas à distance

Un graphique en courbes qui affiche la quantité de mémoire, exprimée en octets, que le système ExtraHop consacre au traitement des déclencheurs de capture et aux flux de données ouverts (ODS).

Comment ces informations peuvent vous aider
Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Stocker le débit d'écriture

Un graphique en aires qui affiche le débit d'écriture de la banque de données, exprimé en octets, sur le système ExtraHop. Le graphique affiche les données pour l'intervalle de temps sélectionné et pour des intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes.

Comment ces informations peuvent vous aider
Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Taille de l'ensemble de travail

Un graphique en aires qui affiche la taille définie de travail du cache d'écriture pour les métriques sur le système ExtraHop. La taille de l'ensemble de travail indique le nombre de mesures pouvant être écrites dans le cache pour l'intervalle de temps sélectionné et pour des intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes.

Comment ces informations peuvent vous aider
Les données de ce graphique peuvent augmenter après la création ou la modification du déclencheur si le script de déclenchement ne collecte pas les métriques de manière efficace.

Chargement déclencheur de la banque de données

Un graphique en courbes qui affiche le pourcentage de cycles consommés par les déclencheurs spécifiques à une banque de données sur le système ExtraHop, en fonction de la durée totale du thread de capture.

Comment ces informations peuvent vous aider
Recherchez des pics ou une augmentation de la charge du déclencheur de banque de données, en particulier après avoir créé un nouveau déclencheur de banque de données ou modifié un déclencheur de banque de données existant. Si vous remarquez l'un ou l'autre, cliquez sur **Charge du déclencheur** étiquette métrique permettant d'effectuer une analyse détaillée et de déterminer quels déclencheurs de banque de données consomment le plus de ressources.

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

Un graphique à lignes et à colonnes dans lequel le graphique en courbes indique le nombre de fois que des déclencheurs spécifiques à une banque de données ont été exécutés sur le système ExtraHop pendant l'intervalle de temps sélectionné, et le graphique à colonnes correspondant affiche le nombre de déclencheurs spécifiques à la banque de données supprimés de la file de déclencheurs en attente d'exécution sur le système ExtraHop pendant l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Un seul déclencheur de banque de données qui s'exécute souvent peut indiquer que le déclencheur a été attribué à toutes les sources, telles que les applications ou les appareils. Pour minimiser l'impact sur les performances, un déclencheur doit être attribué uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

À partir du Chargement déclencheur de la banque de données graphique, cliquez sur **Charge du déclencheur** étiquette métrique pour effectuer une analyse détaillée et voir quels déclencheurs de banque de données s'exécutent le plus fréquemment.

Toutes les données de dépôt affichées sur le histogramme indiquent que des abandons déclencheurs de la banque de données se produisent et que les files d'attente des déclencheurs sont sauvegardées.

Le système met en file d'attente les opérations de déclenchement si un thread de déclenchement est surchargé. Si la file d'attente des déclencheurs de la banque de données devient trop longue, le système arrête d'ajouter des opérations de déclenchement à la file d'attente et supprime les déclencheurs. Les déclencheurs en cours d'exécution ne sont pas affectés.

La principale cause des longues files d'attente, et des abandons de déclencheurs qui en découlent, est un déclencheur de longue durée dans une banque de données.

Exceptions de déclenchement de la banque de données par déclencheur

Un graphique en listes qui affiche le nombre d'exceptions non gérées causées par des déclencheurs spécifiques à une banque de données sur le système ExtraHop.

Comment ces informations peuvent vous aider
Les exceptions aux déclencheurs de la banque de données sont la principale cause des problèmes de performances des déclencheurs. Si ce graphique indique qu'une exception de déclencheur s'est produite, le déclencheur de la banque de données doit être corrigé immédiatement.

Outils d'état et de diagnostic dans les paramètres d'administration

Les paramètres d'administration constituent une autre source d'informations et de diagnostics sur le système.

Pour plus de statistiques sur l'état général du système ExtraHop et pour les outils de diagnostic qui permettent Assistance ExtraHop pour résoudre les erreurs du système, consultez le État et diagnostics section des paramètres d'administration.