

Tableau de bord de l'état du système

Publié: 2023-09-19

Le tableau de bord Santé du système fournit un grand nombre 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 Performances du réseau contient des visualisations des données de performances du système qui ont été générées au cours de l'[intervalle de temps sélectionné](#), organisées par région.

Le tableau de bord Santé du système est un tableau de bord système intégré et vous ne pouvez pas modifier, supprimer ou ajouter un tableau de bord système à une collection. Cependant, vous pouvez copier [un graphique](#) du tableau de bord Santé du système et l'ajouter à un [tableau de bord personnalisé](#), ou vous pouvez [faire une copie du tableau de bord](#) et le modifier pour surveiller les paramètres qui vous intéressent.



Note: La page Administration settings (Paramètres d'administration) fournit également des [informations sur l'état et des outils de diagnostic](#) pour tous les systèmes ExtraHop.

Naviguer dans le tableau de bord Santé du système

Accédez à la page Santé du système en cliquant sur l'icône Paramètres du système  ou en cliquant sur **Tableaux de bord** en haut de la page. Le tableau de bord System Health affiche automatiquement des informations sur le système ExtraHop auquel vous êtes connecté. Si vous consultez le tableau de bord de l'état du système à partir d'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 de santé du système sont répartis dans les sections suivantes :

Découverte de périphériques

Affichez le nombre total de périphériques sur votre réseau. Voir quels dispositifs ont été découverts et combien de ces dispositifs sont actuellement actifs.

Flux de données

Évaluez l'efficacité du processus de collecte des données filaires à l'aide de graphiques relatifs au débit, au taux de paquets, aux désynchronisations et aux chutes de capture.

Enregistrements

Visualisez la quantité totale d'enregistrements envoyés à un magasin d'enregistrements attaché.

Déclencheurs

Surveillez l'impact des déclencheurs sur votre système ExtraHop. Voyez à quelle fréquence les déclencheurs s'exécutent, à quelle fréquence ils échouent et quels sont les déclencheurs qui sollicitent le plus l'unité centrale.

Open Data Stream et Recordstore

Suivez l'activité des transmissions de flux de données ouvertes (ODS) vers et depuis votre système. Affichez le nombre total de connexions à distance, le débit des messages et les détails relatifs à des cibles distantes spécifiques.

Certificats SSL

Examinez les informations relatives à l'état de tous les certificats SSL sur votre système ExtraHop.

Capture de paquets à distance (RPCAP)

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

Mesures avancées de l'état de santé

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

Découverte de périphériques

La section Découverte de périphériques du tableau de bord Santé du système fournit une vue du nombre total de périphériques sur votre réseau. Elle permet de voir quels types de dispositifs sont connectés et combien de ces dispositifs sont actuellement actifs.

La section Découverte de périphériques fournit les graphiques suivants :

- [Périphériques actifs](#)
- [Total des dispositifs](#)

Périphériques actifs

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

Comment ces informations peuvent vous aider

Surveillez ce graphique après avoir apporté des modifications à la configuration SPAN pour vous assurer qu'il n'y a pas eu de conséquences imprévues susceptibles de mettre le système ExtraHop dans un mauvais état. Par exemple, l'inclusion accidentelle d'un réseau peut mettre à rude épreuve les capacités du système ExtraHop en consommant plus de ressources et en exigeant plus de traitement de paquets, ce qui se traduit par des performances médiocres. Vérifiez que le système ExtraHop surveille le nombre prévu de périphériques actifs.

Total des dispositifs

Un graphique linéaire qui affiche le nombre total de périphériques L3 et personnalisés surveillés par le système ExtraHop, qu'ils soient actifs ou inactifs, au cours de l'intervalle de temps sélectionné. À côté du diagramme de zone, un diagramme de valeurs affiche le nombre total de périphériques L3 et personnalisés actuellement surveillés par le système ExtraHop.

Comment ces informations peuvent vous aider

Surveillez ce graphique après avoir apporté des modifications à la configuration SPAN pour vous assurer qu'il n'y a pas eu de conséquences imprévues susceptibles de mettre le système ExtraHop dans un mauvais état. Par exemple, l'inclusion accidentelle d'un réseau peut mettre à l'épreuve les capacités du système ExtraHop en consommant plus de ressources et en exigeant plus de traitement de paquets, ce qui se traduit par des performances médiocres. Vérifiez que le système ExtraHop contient le nombre total de périphériques prévu.

Flux de données

La section Flux de données du tableau de bord Santé du système vous permet d'observer l'efficacité du processus de collecte des données filaires à l'aide de graphiques relatifs au débit, au taux de paquets, aux désynchronisations et aux chutes de capture.

La section Flux de données fournit les graphiques suivants :

- [Débit](#)

- [Taux de paquets](#)
- [Flux analysés](#)
- [Desyncs](#)
- [Capture Drop Rate \(taux de chute de la capture\)](#)
- [Mesures écrites sur le disque \(échelle logarithmique\)](#)
- [Estimations des métriques de lookback des données](#)

Débit

Graphique représentant le débit des paquets entrants sur l'intervalle de temps sélectionné, exprimé en octets par seconde. Le graphique affiche des informations sur le débit des paquets analysés et filtrés, ainsi que des 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 perte de paquets au niveau de la source du span ou d'un agrégateur de span. De même, une grande quantité de doublons L2 ou L3 peut également indiquer un problème au niveau de la source ou de l'agrégateur de span et peut entraîner des métriques faussées ou incorrectes.

Le taux acceptable d'octets par seconde dépend de votre produit. Reportez-vous à la [fiche technique des capteurs ExtraHop](#) pour connaître les limites de votre système ExtraHop et déterminer si le taux d'octets par seconde est trop élevé.

Taux de paquets

Un diagramme de zone qui affiche le taux de paquets entrants, exprimé en paquets par seconde. Le graphique affiche des informations sur le taux de paquets 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 taux de paquets élevé peut entraîner l'abandon de paquets au niveau de la source du span ou d'un agrégateur de 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 de span et entraîner des mesures faussées ou incorrectes.

Le taux acceptable de paquets par seconde dépend de votre produit. Reportez-vous à la [fiche technique des capteurs ExtraHop](#) pour connaître les limites de votre système ExtraHop et déterminer si le taux de paquets par seconde est trop élevé.

Flux analysés

Un graphique linéaire 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 diagramme linéaire, 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 faisant partie d'une transaction entre deux points d'extrémité 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 l'abandon de paquets au niveau de la source du span ou d'un agrégateur de span.

Desyncs

Un graphique linéaire qui affiche les occurrences de désynchronisations à l'échelle du système ExtraHop sur l'intervalle de temps sélectionné. À côté du graphique linéaire, un graphique de valeurs affiche le

nombre total de désynchronisations qui se sont produites pendant l'intervalle de temps sélectionné. Une désynchronisation se produit lorsque le flux de données ExtraHop laisse tomber 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 que des paquets sont tombés sur l'interface de surveillance, le SPAN ou la prise réseau

. Si les ajustements de votre SPAN ne réduisent pas un grand nombre de désynchronisations, contactez le [support ExtraHop](#)

Paquets tronqués

Un graphique linéaire qui affiche les occurrences de paquets tronqués sur le système ExtraHop au cours de l'intervalle de temps sélectionné. À côté du diagramme linéaire, un diagramme de valeurs affiche le nombre total de paquets tronqués survenus au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Un capteur rejette tous les paquets tronqués qu'il reçoit, ce qui peut entraîner des [désynchronisations](#).

Capture Drop Rate (taux de chute de la capture)

Un graphique linéaire qui affiche le pourcentage de paquets perdus au niveau de l'interface de la carte réseau sur un système ExtraHop au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Les chutes de

paquets

se produisent souvent lorsque les seuils des capteurs sont dépassés. Reportez-vous à la [fiche technique des capteurs ExtraHop](#) pour connaître les limites de votre système ExtraHop.

Charge de capture

Graphique linéaire qui affiche le pourcentage de cycles du système ExtraHop consommés par les threads de capture actifs au cours de l'intervalle de temps sélectionné, en fonction de la durée totale des threads de capture. Cliquez sur le diagramme Charge de capture moyenne associé pour effectuer une analyse détaillée par thread et déterminer les threads qui consomment le plus de ressources.

Comment ces informations peuvent-elles vous aider ? Recherchez

les pics ou la croissance à la hausse de la charge de capture pour vérifier si vous approchez des limites du capteur. Reportez-vous à la [fiche technique des capteurs ExtraHop](#) pour connaître les limites de votre système ExtraHop.

Mesures écrites sur le disque (échelle logarithmique)

Graphique linéaire affichant l'espace consommé par les mesures écrites sur le disque au cours de l'intervalle de temps sélectionné, exprimé en octets par seconde. En raison de l'écart important entre les points de données, l'utilisation du disque est affichée sur une échelle logarithmique.

Il

est important de connaître la quantité d'espace consommée par les métriques sur votre datastore. L'espace disponible dans votre magasin de données affecte la quantité de données disponibles. Si certaines mesures consomment trop d'espace, vous pouvez étudier les déclencheurs associés pour voir si vous pouvez les modifier afin de les rendre plus efficaces.

Estimations des métriques de lookback des données

Les mesures de lookback sont disponibles par intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes sur la base du débit d'écriture, exprimé en octets par seconde.

Comment ces informations peuvent-elles vous aider ?

Consultez ce tableau pour déterminer jusqu'à quand vous pouvez consulter des données historiques pour des intervalles de temps donnés. Par exemple, vous pouvez consulter des intervalles de données d'une heure en remontant jusqu'à 9 jours en arrière.

Enregistrements

La section Enregistrements du tableau de bord Santé du système vous permet d'observer l'efficacité du processus de collecte des données de fil de fer à l'aide de graphiques relatifs au nombre d'enregistrements et au débit.

La section Flux de données fournit les graphiques suivants :

- [Nombre d'enregistrements](#)
- [Débit d'enregistrement](#)

Nombre d'enregistrements

Un graphique linéaire qui affiche le nombre d'enregistrements envoyés à un magasin d'enregistrements pendant l'intervalle de temps sélectionné. À côté du graphique linéaire, un graphique de valeurs affiche le nombre total d'enregistrements envoyés pendant l'intervalle de temps sélectionné.

Comment ces informations peuvent-elles vous aider ?

Un nombre extrêmement élevé d'enregistrements envoyés à un magasin d'enregistrement peut entraîner de longues files d'attente de messages et des messages abandonnés au magasin d'enregistrement. Consultez les graphiques de la section [Open Data Stream et Recordstore](#) du tableau de bord Santé du système pour obtenir plus d'informations sur les transmissions aux magasins d'enregistrements.

Débit d'enregistrement

Graphique linéaire qui affiche le nombre d'enregistrements en octets envoyés à un magasin d'enregistrements. À côté du graphique linéaire, un graphique de valeur affiche le nombre total d'enregistrements envoyés en octets sur l'intervalle de temps sélectionné.

Comment ces informations peuvent-elles vous aider ?

Ce graphique ne reflète pas les ajustements de taille basés sur la compression ou la déduplication et ne doit pas être utilisé pour estimer les coûts d'un magasin d'enregistrements. Un débit d'enregistrement extrêmement élevé peut entraîner de longues files d'attente de messages et des messages abandonnés dans le magasin d'enregistrement. Consultez les graphiques de la section [Open Data Stream et Recordstore](#) du tableau de bord de l'état du système pour plus d'informations sur les transmissions des magasins d'archives.

Déclencheurs

La section Déclencheurs du tableau de bord Santé du système vous permet de surveiller l'impact des déclencheurs sur votre système. Découvrez la fréquence d'exécution des déclencheurs, la fréquence de leurs échecs et les déclencheurs qui sollicitent le plus votre processeur.

La section Déclencheurs fournit les graphiques suivants :

- [Charge de déclenchement](#)
- [Délai de déclenchement](#)

- [Déclencheurs exécutés et abandonnés](#)
- [Détails des déclencheurs](#)
- [Charge de déclenchement par déclencheur](#)
- [Exécution des déclencheurs par déclencheur](#)
- [Exceptions par déclencheur](#)
- [Cycles de déclenchement par thread](#)

Charge de déclenchement

Graphique linéaire qui affiche le pourcentage de cycles de CPU alloués aux processus de déclenchement qui ont été consommés par les déclencheurs au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent-elles vous aider ? Recherchez

les pics ou la croissance de la charge des déclencheurs, en particulier après la création d'un nouveau déclencheur ou la modification d'un déclencheur existant. Si vous remarquez l'une ou l'autre de ces conditions, consultez le graphique [Charge de déclenchement par déclencheur](#) pour voir quels sont les déclencheurs qui consomment le plus de ressources.

Délai de déclenchement

Un diagramme à colonnes affiche les délais de déclenchement maximaux qui se sont produits pendant l'intervalle de temps sélectionné, en millisecondes. À côté du diagramme à colonnes, un diagramme de valeurs affiche le délai de déclenchement le plus long qui s'est produit pendant l'intervalle de temps sélectionné. Un délai de déclenchement est le temps qui s'écoule entre le moment où un événement de déclenchement est capturé et celui où un fil de déclenchement est créé pour l'événement.

Comment ces informations peuvent-elles vous aider ?

Les longs délais de déclenchement peuvent indiquer des problèmes de traitement. Consultez les graphiques [Exceptions par déclencheur](#) et [Charge de déclenchement par déclencheur](#) pour voir quel déclencheur génère le plus grand nombre d'exceptions non gérées et quels déclencheurs consomment le plus de ressources.

Déclencheurs exécutés et abandonnés

Un graphique à lignes et à colonnes dans lequel les lignes indiquent le nombre d'exécutions de déclencheurs et les colonnes le nombre d'abandons de déclencheurs au cours de l'intervalle de temps sélectionné. À côté du graphique à lignes et à colonnes, un graphique de valeurs affiche le nombre total d'exécutions et d'abandons de déclencheurs survenus au cours de l'intervalle de temps sélectionné. Ces graphiques fournissent un aperçu global de tous les déclencheurs en cours d'exécution sur le système ExtraHop.

Comment ces informations peuvent-elles vous aider ? Recherchez

les pics dans les graphiques à lignes et à colonnes et examinez les déclencheurs qui ont entraîné cette hausse. Par exemple, vous pouvez remarquer une augmentation de l'activité si un déclencheur a été modifié ou si un nouveau déclencheur a été activé. Consultez le graphique [Exécution des déclencheurs par déclencheur](#) pour voir quels sont les déclencheurs qui s'exécutent le plus fréquemment.

Détails des déclencheurs

Un diagramme en liste qui affiche les déclencheurs individuels et le nombre de cycles, d'exécutions et d'exceptions attribués à chacun d'entre eux sur l'intervalle de temps sélectionné. Par défaut, la liste des déclencheurs est triée par ordre décroissant des cycles de déclenchement.

Comment ces informations peuvent vous aider Identifier

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. Veillez à ce que tout déclencheur suractif ne soit affecté qu'à la source spécifique dont vous avez besoin pour collecter des données.

Charge de déclenchement par déclencheur

Un graphique linéaire qui affiche le pourcentage de cycles CPU alloués aux processus de déclenchement qui ont été consommés par les déclencheurs au cours de l'intervalle de temps sélectionné, répertorié par nom de déclencheur.

Comment ces informations peuvent vous aider Identifier

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 suractif n'est affecté qu'à la source spécifique dont vous avez besoin pour collecter des données.

Exécution des déclencheurs par déclencheur

Un graphique linéaire qui affiche le nombre de fois où chaque déclencheur actif s'est exécuté au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent-elles vous aider ? Recherchez

les déclencheurs qui s'exécutent plus fréquemment que prévu, ce qui peut indiquer que le déclencheur est affecté de manière trop large. Un déclencheur affecté à toutes les applications ou à tous les périphériques peut avoir un coût élevé en termes de performances. Un déclencheur affecté à un groupe de périphériques qui a été élargi peut collecter des métriques que vous ne souhaitez pas. Pour minimiser l'impact sur les performances, un déclencheur ne doit être affecté qu'aux sources spécifiques dont vous avez besoin pour collecter des données

.Une activité élevée peut également indiquer qu'un déclencheur travaille plus qu'il ne le devrait.

Par exemple, un déclencheur peut s'exécuter sur plusieurs événements alors qu'il serait plus efficace de créer des déclencheurs distincts, ou un script de déclencheur peut ne pas respecter les directives de script recommandées, telles que décrites dans le [Guide des meilleures pratiques des déclencheurs](#).

Exceptions par déclencheur

Un graphique linéaire qui affiche le nombre d'exceptions non gérées, triées par déclencheur, qui se sont produites sur le système ExtraHop au cours de l'intervalle de temps sélectionné.

Les exceptions de

déclenchement

sont la cause principale des problèmes de performance des déclencheurs. Si ce graphique indique qu'une exception s'est produite au niveau du déclencheur, vous devez l'examiner immédiatement.

Cycles de déclenchement par thread

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

Les chutes de

déclenchement

peuvent se produire si la consommation d'un thread est considérablement plus élevée que celle des autres, même si la consommation du thread est à un faible pourcentage. Recherchez une consommation de cycles égale pour tous les threads.

Open Data Stream et Recordstore

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

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

- [Débit des messages](#)
- [Messages envoyés](#)
- [Messages abandonnés par type de message distant](#)
- [Erreurs d'envoi de message](#)
- [Connexions](#)
- [Longueur de la file d'attente des messages à distance par cible](#)
- [Longueur de la file d'attente des messages Excap par type de connexion à distance](#)
- [Détails de la cible](#)

Débit des messages

Un graphique linéaire qui affiche le débit des données des messages distants, exprimé en octets. À côté du graphique linéaire, un graphique 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 magasin d'enregistrements ou à des systèmes tiers depuis le système ExtraHop par le biais d'un flux de données ouvert (ODS).

Surveillez

ce graphique pour vous assurer que les octets sont transférés comme prévu. Si le débit est faible, il se peut que la configuration d'un ODS ou d'un magasin d'enregistrements attaché pose problème. Des baisses importantes de débit peuvent indiquer des problèmes avec vos flux de données.

Messages envoyés

Graphique linéaire qui affiche le taux moyen d'envoi de messages distants du système ExtraHop vers un enregistreur ou une cible ODS (Open Data Stream). À côté du graphique linéaire, un graphique 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 que la configuration d'un ODS ou d'un magasin d'enregistrements attaché pose problème.

Messages abandonnés par type de message distant

Un graphique linéaire qui affiche le taux moyen de messages distants qui ont été abandonnés avant d'atteindre un magasin d'enregistrements ou une cible ODS.

Les

messages abandonnés indiquent des problèmes de connectivité avec la cible distante. Un nombre élevé de messages abandonnés 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

Graphique linéaire affichant le nombre d'erreurs survenues lors de l'envoi d'un message distant à un magasin d'enregistrements ou à une cible ODS. Surveillez ce graphique pour vous assurer que les paquets sont envoyés comme prévu. Les erreurs de transmission peuvent concerner les éléments suivants

Erreurs du serveur cible

Nombre d'erreurs renvoyées au système ExtraHop par les magasins d'archives ou les cibles ODS. Ces erreurs sont survenues sur le serveur cible et n'indiquent pas un problème avec le système ExtraHop.

Messages abandonnés dans la file d'attente

Nombre de messages envoyés aux magasins d'archives et aux cibles ODS qui ont été abandonnés parce que la file d'attente du serveur cible était pleine. Un nombre élevé de messages abandonnés peut indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Consultez les graphiques [Longueur de la file d'attente des messages à distance par cible](#) et [Target Details](#) pour voir si vos erreurs de transmission peuvent être liées à une longue file d'attente de messages.

Messages abandonnés en raison d'une inadéquation de la cible

Nombre de messages distants abandonnés parce que le système distant spécifié dans le script de déclenchement 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 déclenchement et les paramètres d'administration.

Erreurs de décodage Messages abandonnés

Nombre de messages abandonnés en raison de problèmes de codage interne entre ExtraHop Capture (excap) et ExtraHop Remote (exremote).

Connexions

Il s'agit d'un diagramme à lignes et à colonnes dans lequel le diagramme à lignes affiche le nombre de tentatives de connexion du système à un serveur cible distant et le diagramme à colonnes qui l'accompagne affiche le nombre d'erreurs qui se sont produites à la suite de ces tentatives. À côté du diagramme à lignes et à colonnes, un diagramme de valeurs affiche le nombre total de tentatives de connexion et d'erreurs de connexion qui se sont produites au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider Identifier les

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

Longueur de la file d'attente des messages à distance par cible

Graphique linéaire 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-elles vous aider ?

Un nombre élevé de messages dans la file d'attente peut indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Consultez la valeur Exremote Full Queue Dropped Messages dans le tableau [Erreurs d'envoi de message](#) pour déterminer si des messages sont tombés.

Longueur de la file d'attente des messages Excap par type de distance

Graphique linéaire affichant le nombre de messages de cibles distantes dans la file d'attente ExtraHop Capture (excap) en attente de traitement par le système ExtraHop.

Le

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

Consultez le tableau [Messages abandonnés par type de message distant](#) pour déterminer si des chutes de messages se sont produites

Détails de la cible

Un graphique en liste qui affiche les mesures suivantes relatives aux cibles distantes recordstore ou ODS sur l'intervalle de temps sélectionné : nom de la cible, nombre d'octets du message cible, messages cibles envoyés, erreurs du serveur cible, messages abandonnés dans la file d'attente complète, messages abandonnés en raison d'erreurs de décodage, tentatives de connexion au serveur cible et erreurs de connexion au serveur cible.

Comment ces informations peuvent vous aider

Si vous voyez des erreurs de message signalées dans le tableau [Messages envoyés](#), les détails de ce tableau peuvent vous aider à déterminer la cause première des erreurs de message à distance.

Certificats SSL

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

La section Certificats SSL présente le tableau suivant :

- [Détails du certificat](#)

Détails du certificat

Un tableau de liste qui affiche les informations suivantes pour chaque certificat :

Sessions décryptées

Le nombre de sessions qui ont été décryptées avec succès.

Sessions non prises en charge

Nombre de sessions qui n'ont pas pu être déchiffrées par une analyse passive, telle que l'échange de clés DHE.

Sessions détachées

Nombre de sessions qui n'ont pas été déchiffrées ou qui n'ont été que partiellement déchiffrées en raison de désynchronisations.

Sessions de passage

Nombre de sessions qui n'ont pas été déchiffrées en raison d'erreurs matérielles, telles que celles causées par le dépassement des spécifications du matériel d'accélération SSL.

Sessions décryptées avec le secret partagé

Nombre de sessions décryptées à l'aide d'une clé secrète partagée.

Comment ces informations peuvent-elles vous aider ?

Surveillez ce graphique pour vous assurer que les bons certificats SSL sont installés sur le système ExtraHop et qu'ils effectuent le décryptage comme prévu.

Capture de paquets à distance (RPCAP)

La section Capture de paquets à distance (RPCAP) du tableau de bord Santé du système permet d'afficher le nombre de paquets et de trames envoyés par les homologues RPCAP et reçus par le système ExtraHop.

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

- [Transmis par l'homologue](#)
- [Reçus par le système ExtraHop](#)

Transmis par l'homologue

Un diagramme de liste qui affiche les informations suivantes concernant les paquets et les trames qui sont transférés par un homologue RPCAP :

Paquets transférés

Nombre de paquets qu'un homologue RPCAP a tenté de transmettre à un système ExtraHop.

Paquets de l'interface du transitaire

Le nombre total de paquets qui ont été vus par le transitaire. Les transitaires des dispositifs RPCAP se coordonnent entre eux pour éviter que plusieurs dispositifs n'envoient le même paquet. Il s'agit du nombre de paquets qui ont été visualisés avant qu'aucune trame ne soit supprimée pour réduire le trafic transféré, et avant que les trames ne soient supprimées par des filtres définis par l'utilisateur.

Trames abandonnées par le noyau du transitaire

Nombre de trames supprimées parce que le noyau du pair RPCAP a été surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées par le noyau pour supprimer les paquets en double ou les paquets qui ne doivent pas être transmis en raison de règles définies par l'utilisateur.

Interface du transitaire Dropps

Le nombre de paquets qui ont été abandonnés parce que le transitaire RPCAP a été surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées pour supprimer les paquets en double ou les paquets qui ne doivent pas être transmis en raison de règles définies par l'utilisateur.

Comment ces informations peuvent vous aider

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

Reçus par le système ExtraHop

Un diagramme de liste qui affiche les informations suivantes concernant les paquets et les trames reçus par un système ExtraHop à partir d'un pair RPCAP (Remote Packet Capture) :

Octets encapsulés

Taille totale de tous les paquets liés au flux UDP entre le périphérique RPCAP et le système ExtraHop, en octets. Cette information vous indique la quantité de trafic que le transitaire RPCAP ajoute à votre réseau.

Paquets encapsulés

Nombre de paquets liés au flux UDP entre le périphérique RPCAP et le système ExtraHop.

Octets du tunnel

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

Paquets du tunnel

Le nombre de paquets que le système ExtraHop a reçu d'un homologue RPCAP. Ce nombre devrait être très proche du nombre de paquets transférés dans le tableau Envoyés par le périphérique distant. S'il y a un écart important entre ces deux nombres, cela signifie que des paquets sont perdus entre le périphérique 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 transitaires RPCAP n'imposent pas une 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 le dispositif RPCAP envoie.

Mesures avancées de l'état de santé

La section Paramètres de santé avancés du tableau de bord Santé du système vous permet de suivre l'allocation du tas liée à la capture de données, au datastore 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 le datastore du système.

La section Paramètres de santé avancés fournit les graphiques suivants :

- [Capture et allocation de la mémoire vive du datastore](#)
- [Allocation de la mémoire vive des déclencheurs et de la mémoire distante](#)
- [Débit d'écriture du magasin](#)
- [Taille de l'ensemble de travail](#)
- [Charge de déclenchement du magasin de données](#)
- [Exécutions et abandons de déclencheurs de magasin de données](#)
- [Exceptions des déclencheurs de magasin de données par déclencheur](#)

Capture et allocation de la mémoire vive du datastore

Un graphique linéaire qui affiche la quantité de mémoire que le système ExtraHop consacre à la capture de paquets réseau et au datastore.

Les

données de ce graphique sont destinées à un usage interne et peuvent être demandées par l'[assistance ExtraHop](#) pour vous aider à diagnostiquer un problème.

Allocation de la mémoire vive des déclencheurs et de la mémoire distante

Graphique linéaire 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).

Les

données de ce graphique sont destinées à un usage interne et peuvent être demandées par l'[assistance ExtraHop](#) pour vous aider à diagnostiquer un problème.

Débit d'écriture du magasin

Graphique affichant le débit d'écriture du datastore, 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.

Les

données de ce graphique sont destinées à un usage interne et peuvent être demandées par l'[assistance ExtraHop](#) pour vous aider à diagnostiquer un problème.

Taille de l'ensemble de travail

Tableau affichant la taille de l'ensemble de travail du cache d'écriture pour les mesures sur le système ExtraHop. La taille de l'ensemble de travail indique le nombre de métriques 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 d'un déclencheur si le script de déclenchement ne collecte pas les métriques de manière efficace.

Charge de déclenchement du magasin de données

Graphique linéaire qui affiche le pourcentage de cycles consommés par les déclencheurs spécifiques au datastore sur le système ExtraHop, en fonction de la durée totale des threads de capture.

Comment ces informations peuvent-elles vous aider ? Recherchez

les pics ou la croissance de la charge de déclenchement du magasin de données, en particulier après la création d'un nouveau déclencheur de magasin de données ou la modification d'un déclencheur de magasin de données existant. Si vous remarquez l'un ou l'autre de ces phénomènes, cliquez sur l'étiquette de la métrique **Charge de déclenchement** pour approfondir et voir quels sont les déclencheurs de magasin de données qui consomment le plus de ressources.

Exécutions et abandons de déclencheurs de magasin de données

Graphique à lignes et à colonnes dans lequel le graphique à lignes affiche le nombre d'exécutions de déclencheurs spécifiques au datastore sur le système ExtraHop pendant l'intervalle de temps sélectionné, et le graphique à colonnes qui l'accompagne affiche le nombre de déclencheurs spécifiques au datastore retirés de la file d'attente des 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 datastore qui s'exécute souvent peut indiquer que le déclencheur a été affecté à toutes les sources, telles que les applications ou les périphériques. Pour minimiser l'impact sur les performances, un déclencheur ne doit être affecté qu'aux sources spécifiques dont vous avez besoin pour collecter des données.

Dans le graphique [Charge de déclenchement du magasin de données](#), cliquez sur l'étiquette de la métrique **Trigger Load** pour effectuer une analyse détaillée et voir quels sont les déclencheurs de datastore qui s'exécutent le plus fréquemment.

Toute donnée de chute affichée sur le graphique en colonnes indique que des chutes de déclencheurs de datastore se produisent et que les files d'attente de déclencheurs sont sauvegardées.

Le système met en file d'attente les opérations de déclenchement si un thread de déclencheur est surchargé. Si la file d'attente des déclencheurs du magasin de données devient trop longue, le système cesse d'ajouter des opérations de déclenchement à la file d'attente et abandonne 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 s'ensuivent est un déclencheur du magasin de données qui s'exécute depuis longtemps.

Exceptions des déclencheurs de magasin de données par déclencheur

Un graphique en liste qui affiche le nombre d'exceptions non gérées causées par les déclencheurs spécifiques au datastore sur le système ExtraHop.

Les exceptions des déclencheurs du

magasin

de données sont la cause principale des problèmes de performance des déclencheurs. Si ce graphique indique qu'une exception s'est produite, le déclencheur du magasin 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 obtenir des informations sur l'état général du système ExtraHop et des outils de diagnostic permettant à l'équipe d'assistance ExtraHop [de résoudre les erreurs du système](#), consultez la section [État et diagnostics](#) des paramètres d'administration.