

Utilisation de vRealize Log Insight

8 septembre 2017
vRealize Log Insight 4.5



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<https://docs.vmware.com/fr/>

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Copyright © 2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

À propos de l'utilisation de vRealize Log Insight 5

1 Utilisation des fonctionnalités de vRealize Log Insight 6

Présentation de l'interface utilisateur Web de vRealize Log Insight 8

Recherche et filtrage d'événements de journaux 9

Regroupement de types d'événements 10

Informations contenues dans les événements de journaux 11

Filtrer les événements de journaux par intervalle de temps 12

Rechercher des événements de journaux contenant un mot clé complet 12

Rechercher les événements de journaux par opérations de champ 13

Rechercher des événements qui se sont produits avant, après ou environ au même moment qu'un autre événement 15

Afficher un événement dans son contexte 15

Analyser les tendances des événements 16

Effacer toutes les règles de filtrage 16

Exemples de requêtes de recherche 17

Exemples d'expressions régulières 19

Utilisation du diagramme Analyse interactive pour analyser des journaux 21

Types de diagramme 22

Diagrammes multifonction 22

Fonction d'agrégation 22

Utilisation de diagrammes 23

Modifier le type de diagramme Analyse interactive 24

Extraction de champs dynamique 25

Extraire des champs à l'aide d'une extraction en un clic 26

Modifier un champ extrait 27

Dupliquer un champ extrait 28

Supprimer un champ extrait 29

Gestion de requêtes de recherche 30

Enregistrer une requête dans vRealize Log Insight 30

Renommer une requête dans vRealize Log Insight 31

Charger une requête dans vRealize Log Insight 31

Supprimer une requête de vRealize Log Insight 32

Partager la requête actuelle 32

Exporter la requête actuelle 32

Prendre un snapshot d'une requête 33

Utilisation de tableaux de bord 34

Gestion de tableaux de bord 35

Ajouter un widget Liste de requêtes au tableau de bord	37
Ajouter une requête à un widget Liste de requêtes dans un tableau de bord	37
Ajouter un widget Tableau de champs à un tableau de bord	38
Ajouter un widget Types d'événements à un tableau de bord	39
Ajouter un widget Tendances des événements à un tableau de bord	39
Filtrer à l'aide de valeurs de champs de diagrammes	40
Utilisation des packs de contenu	40
Installer un pack de contenu à partir du lieu de vente du module de contenu	41
Mettre à jour un pack de contenu installé à partir du lieu de vente du module de contenu	42
Importer un pack de contenu	42
Exporter un pack de contenu	44
Afficher des détails sur des éléments de pack de contenu	45
Désinstaller un pack de contenu	46
Création de packs de contenu	46
Termes des packs de contenu	47
Requêtes	49
Recommandations concernant les tableaux de bord	55
Erreur d'importation de pack de contenu	58
Exigences de publication des packs de contenu	59
Envoyer un pack de contenu	60
Requêtes d'alerte dans vRealize Log Insight	61
Ajouter une requête d'alerte pour envoyer des notifications par e-mail	63
À propos de l'utilisation de webhooks pour envoyer des alertes à des produits tiers	64
Afficher des requêtes d'alerte	69
Modifier des requêtes d'alerte	70
Activer des requêtes d'alerte	72
Supprimer des requêtes d'alerte	74

À propos de l'utilisation de vRealize Log Insight

Les rubriques Utilisation de vRealize Log Insight fournissent des informations sur l'utilisation de l'interface utilisateur Web, notamment les procédures de filtrage et de recherche de messages de journaux, l'exécution d'analyses et la visualisation des résultats de recherche, l'utilisation des requêtes d'alerte, ainsi que l'extraction dynamique de champs de messages de journaux en fonction de requêtes personnalisées.

Utilisation des fonctionnalités de vRealize Log Insight

1

vRealize Log Insight assure l'agrégation et l'indexation évolutives des journaux pour vCloud Suite, notamment toutes les éditions de vSphere, avec des possibilités de recherche et d'analyse en temps quasi réel.

vRealize Log Insight collecte, importe et analyse les journaux pour fournir des réponses en temps quasi réel aux problèmes liés aux systèmes, aux services et aux applications, et apporte un éclairage important.

Ingestion de données haute performance

vRealize Log Insight peut traiter tout type de données générées par un journal ou par une machine. Il prend en charge les débits élevés et la latence faible et accepte les données via Syslog et l'API Ingestion.

Evolutivité

vRealize Log Insight a la possibilité de monter en charge en utilisant plusieurs instances de dispositif virtuel. Grâce à cela, le débit d'ingestion évolue de manière linéaire, les performances des requêtes sont améliorées et l'ingestion est hautement disponible. En mode cluster, vRealize Log Insight fournit les nœuds maître et travailleurs. Ces deux types de nœuds sont responsables d'un sous-ensemble de données ; Les nœuds maîtres et les nœuds de requête peuvent interroger tous les sous-ensembles de données et agréger les résultats.

Recherche en temps quasi réel

Les données ingérées par vRealize Log Insight peuvent faire l'objet de recherche quelques secondes plus tard. Des recherches peuvent également être effectuées dans les données historiques avec la même interface et la même faible latence.

vRealize Log Insight prend en charge les requêtes par mots clés complets. Les mots clés peuvent être composés de tout caractère alphanumérique, de traits d'union et de traits de soulignement. Outre les requêtes par mots clés complets, vRealize Log Insight prend en charge les requêtes comportant des caractères génériques (par exemple, `erro?` ou `vm*`) et le filtrage basé sur les champs (par exemple, `hostname does NOT match test*`, `IP contains "10.64"`). En outre, les champs de message de journal qui contiennent des valeurs numériques peuvent être utilisés pour définir des filtres de sélection (par exemple, `CPU>80`, `10<threads<100`, etc.).

Les résultats de recherche sont présentés comme des événements individuels. Chaque événement provient d'une source unique, mais les résultats de recherche peuvent provenir de plusieurs sources. Vous pouvez utiliser vRealize Log Insight pour corréler les données sur une ou plusieurs dimensions (par exemple, temps et identifiants de recherche) pour ainsi disposer d'une vue cohérente sur toute la pile. L'analyse des causes premières est alors beaucoup plus simple.

Agents Windows et Linux

vRealize Log Insight inclut des agents qui collectent des événements et des fichiers sur les machines Linux et Windows.

Regroupement intelligent

vRealize Log Insight utilise une nouvelle technologie d'apprentissage automatique. Le regroupement intelligent (Intelligent Grouping) analyse les données entrantes non structurées et regroupe les messages par type de problème pour vous permettre de rapidement comprendre les problèmes se produisant dans vos environnements physiques, virtuels et cloud hybrides.

Agrégation

Les champs extraits des données de journaux peuvent être utilisés pour agrégation. Cette fonctionnalité est semblable à celle fournie par les requêtes GROUP-BY dans une base de données relationnelle ou dans des tableaux croisés dynamiques Microsoft Excel. Mais ici, il n'est pas nécessaire d'extraire, de transformer et de charger des processus (ETL), et vRealize Log Insight se redimensionne dynamiquement en fonction de la taille des données.

Vous pouvez générer des vues agrégées des données et identifier des événements ou des erreurs en particulier, sans devoir accéder à plusieurs systèmes et applications. Par exemple, lors de l'affichage d'une mesure système importante, tel que le nombre d'erreurs par minute, vous pouvez explorer des événements sur un intervalle de temps spécifique et examiner les erreurs s'étant produites dans l'environnement.

Extraction de champs au moment de l'exécution

Les données de journaux brutes ne sont pas toujours faciles à comprendre et il est parfois nécessaire de traiter des données pour identifier les champs importants pour la recherche et l'agrégation.

vRealize Log Insight propose une extraction de champs au moment de l'exécution pour résoudre ce problème. Vous pouvez extraire dynamiquement n'importe quel champ des données en fournissant une expression régulière. Les champs extraits peuvent être utilisés à des fins de sélection, de projection et d'agrégation, comme lors de l'extraction des champs au moment de l'analyse.

Tableaux de bord

Vous pouvez créer des tableaux de bord de mesures utiles qu'il convient de surveiller étroitement. Toute requête peut être transformée en un widget de tableau de bord et synthétisée sur tout intervalle de temps. Vous pouvez vérifier les performances du système sur les cinq dernières minutes, la dernière heure ou le dernier jour. Vous pouvez visualiser une liste détaillée d'erreurs par heure et observer les tendances des événements de journaux.

Considérations en matière de sécurité

Les décideurs, les architectes, les administrateurs et les autres utilisateurs du service informatique qui doivent se familiariser avec les composants de sécurité de vRealize Log Insight doivent lire les rubriques de sécurité dans *Administration de vRealize Log Insight*.

Ces rubriques fournissent des références concises vers les fonctionnalités de sécurité de vRealize Log Insight. Les rubriques traitent des interfaces externes du produit, des ports, des mécanismes d'authentification ainsi que des options de configuration et de gestion des fonctionnalités de sécurité.

Ce chapitre aborde les rubriques suivantes :

- [Présentation de l'interface utilisateur Web de vRealize Log Insight](#)
- [Recherche et filtrage d'événements de journaux](#)
- [Utilisation du diagramme Analyse interactive pour analyser des journaux](#)
- [Extraction de champs dynamique](#)
- [Gestion de requêtes de recherche](#)
- [Utilisation de tableaux de bord](#)
- [Utilisation des packs de contenu](#)
- [Création de packs de contenu](#)
- [Requêtes d'alerte dans vRealize Log Insight](#)

Présentation de l'interface utilisateur Web de vRealize Log Insight

La fonctionnalité à laquelle vous pouvez accéder dépend du compte d'utilisateur que vous utilisez pour vous connecter à l'interface utilisateur Web de vRealize Log Insight.

Onglet Tableaux de bord

L'onglet **Tableaux de bord** contient des tableaux de bord personnalisés et des tableaux de bord de packs de contenu. Dans l'onglet **Tableaux de bord**, vous pouvez voir des graphiques d'événements de journaux de votre environnement ou créer des ensembles personnalisés de widgets pour accéder à vos informations importantes.

L'onglet Analyse interactive

Dans l'onglet **Analyse interactive**, vous pouvez rechercher et filtrer des événements de journaux, puis créer des requêtes pour extraire des événements basés sur un horodatage, un texte, une source et des champs d'événements de journaux. vRealize Log Insight présente les diagrammes des résultats de requêtes. Vous pouvez enregistrer ces diagrammes pour les examiner ultérieurement dans l'onglet **Tableaux de bord**.

Packs de contenu

Les packs de contenu contiennent des tableaux de bord, des champs extraits, des requêtes enregistrées et des alertes qui sont associés à un produit spécifique ou à un ensemble de journaux. Vous accédez aux packs de contenu dans le menu déroulant situé dans le coin supérieur droit de l'interface utilisateur Web de vRealize Log Insight.

Les packs de contenu peuvent être importés ou créés par les utilisateurs de vRealize Log Insight. Reportez-vous à [Utilisation des packs de contenu](#).

L'interface utilisateur d'administration

Les administrateurs de vRealize Log Insight peuvent gérer des comptes d'utilisateur, configurer un emplacement de stockage et un archivage, configurer un serveur SMTP sortant pour les notifications par e-mail et modifier plusieurs autres paramètres. Le format d'URL de l'interface utilisateur d'administration est `https://log_insight-host/admin/`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Recherche et filtrage d'événements de journaux

Vous pouvez rechercher et filtrer des événements de journaux dans l'onglet **Analyse interactive**.

Vous pouvez taper des mots clés complets, des caractères génériques ou des phrases dans la zone de texte de recherche, et cliquer sur **Rechercher** pour trouver uniquement les événements contenant les mots clés spécifiés.

Vous pouvez spécifier l'intervalle de temps dans les pages **Tableaux de bord** ou **Analyse interactive** dans l'interface utilisateur Web. Les intervalles de temps sont inclusifs lors d'un filtrage.

Vous pouvez rechercher des événements de journaux correspondant à certaines valeurs de champs spécifiques. Un texte entre guillemets dans le champ de recherche principal permet de rechercher des phrases exactes. Un espace entré dans le champ de recherche principal correspond à un opérateur logique ET. La recherche utilise uniquement des jetons complets : la recherche de « err » ne trouvera pas la correspondance « erreur ».

Vous pouvez spécifier les critères de recherche de champs, ou filtres, à l'aide des menus déroulants et de la zone de texte au-dessus de la liste d'événements de journaux.

Dans un filtre sur une seule ligne, vous pouvez utiliser des valeurs séparées par des virgules pour utiliser des filtres OU. Par exemple, sélectionnez **nom d'hôte contient** et tapez **127.0.0.1, 127.0.0.2**. La recherche renvoie le nom d'hôte 127.0.0.1 ou 127.0.0.2.

Remarque Le filtre **texte contient** traite chaque valeur séparée par des virgules comme un mot clé complet.

Les requêtes comportant des champs utilisant des noms de syntaxe de langage de la requête internes, par exemple, à partir de ou dans, ne peuvent pas être traitées et ne doivent pas être utilisées.

Vous pouvez combiner plusieurs filtres de champ en créant une nouvelle ligne de filtre pour chaque champ. Vous pouvez basculer l'opérateur appliqué à des filtres sur plusieurs lignes.

- Sélectionnez **tout** pour appliquer l'opérateur ET.
- Sélectionnez **quelconque** pour appliquer l'opérateur OU.

Remarque Quelle que soit la valeur de basculement, l'opérateur de valeurs séparées par des virgules sur une ligne de filtres unique est toujours OU.

Vous pouvez utiliser des caractères génériques dans les termes recherchés. Par exemple, vm* ou vmw? re.

- Utilisez * pour 0 caractère ou plus.
- Utilisez ? pour un caractère.

Remarque Les caractères génériques ne peuvent pas être utilisés comme premier caractère d'un terme recherché. Par exemple, vous pouvez utiliser 192.168.0.*, mais vous ne pouvez pas utiliser *.168.0.0 dans vos requêtes de filtrage.

Regroupement de types d'événements

Log Insight utilise l'apprentissage automatique pour grouper des événements similaires. Le regroupement de types d'événements simplifie le dépannage et l'analyse de la cause première.

Lorsque vous exécutez des requêtes dans Log Insight, le nombre de résultats dépend de la requête et de l'intervalle de temps. Les requêtes renvoient souvent de nombreux résultats. L'apprentissage automatique apprend et ajuste dynamiquement des modèles à partir d'événements provenant de Log Insight.

L'onglet **Types d'événements** se trouve dans la page Analyse interactive, sous la barre de recherche. Lorsque vous cliquez sur l'onglet **Types d'événements**, vous voyez une liste d'événements similaires regroupés.

L'apprentissage automatique analyse les événements et repère les types de champs contenus dans des messages de journaux similaires. Par exemple, ces types peuvent être horodatage, chaîne, entier, valeur hexadécimale et autres. Les types identifiés s'affichent sous la forme de liens hypertexte dans la liste **Types d'événements**.

Chaque type identifié par l'apprentissage automatique représente un nouveau type de champ nommé champ intelligent. Le nom par défaut d'un champ intelligent a le format suivant : *type number* [*event_type*]. Vous pouvez modifier le nom par défaut d'un champ intelligent. Après que vous avez nommé un champ intelligent, celui-ci s'affiche sous la section Champs tout comme les autres champs. Vous pouvez renommer ou supprimer un champ intelligent, mais vous ne pouvez pas en modifier la définition.

L'apprentissage automatique introduit un nouveau champ statique nommé *event_type*. Vous pouvez utiliser le champ *event_type* en tant que filtre pour inclure ou exclure certains types d'événements des requêtes.

Informations contenues dans les événements de journaux

vRealize Log Insight collecte et analyse tous les types de données de journaux générés par des machines, notamment les journaux d'applications, les suivis réseau, les fichiers de configuration, les messages, les données de performance et les vidages d'état système.

Vous pouvez connecter vRealize Log Insight à tous les éléments de votre environnement (systèmes d'exploitation, applications, stockage, pare-feu, dispositifs réseau, etc.) pour disposer d'une visibilité à l'échelle de l'entreprise avec une analyse des journaux.

Lorsque vRealize Log Insight est configuré et prêt à collecter des journaux, vous pouvez ingérer les données des journaux de plusieurs manières, notamment :

- **Intégration vSphere** : vRealize Log Insight peut s'intégrer à vSphere pour ingérer automatiquement des événements en provenance de vCenter Server et des journaux des hôtes ESXi.
- **Intégration de vRealize Operations Manager** : vRealize Log Insight peut s'intégrer à vRealize Operations Manager pour activer diverses alertes pour envoyer des événements de notification dans vRealize Operations Manager et des e-mails aux administrateurs.
- **Agents** : vRealize Log Insight dispose d'agents de collecte destinés à envoyer des fichiers et des journaux d'événements en provenance de Linux ou de Windows à vRealize Log Insight
- **Syslog** : vRealize Log Insight peut ingérer des données en provenance de n'importe quelle source via syslog. Définissez simplement le serveur vRealize Log Insight comme votre destination syslog.
- **CFAPI** : les événements sont envoyés dans leur format d'origine à vRealize Log Insight à l'aide de cfapi. Les événements envoyés via le protocole cfapi n'ont pas à suivre les directives d'un événement syslog et ne sont pas modifiés pour se conformer au RFC syslog.

Chaque événement contient les informations suivantes.

Type	Description
Horodatage	Heure à laquelle l'événement s'est produit
Source	Provenance de l'événement. Elle peut correspondre à l'expéditeur de messages syslog, par exemple un hôte ESXi ou un redirecteur comme un agrégateur syslog.

Type	Description
Texte	Texte brut de l'événement.
Champs	Paire nom-valeur extraite de l'événement. Les champs sont livrés au serveur en tant que champs statiques uniquement lorsqu'un agent utilise le protocole CFAPL.

Remarque vRealize Log Insight n'est pas responsable du contenu des messages de journaux provenant d'autres produits VMware. Si vous avez une question sur le contenu d'un journal, contactez l'équipe du produit qui a généré le message de journal.

Filtrer les événements de journaux par intervalle de temps

Vous pouvez filtrer les événements de journaux de manière à afficher uniquement les événements d'une période spécifique.

Vous pouvez spécifier l'intervalle de temps dans les pages **Tableaux de bord** ou **Analyse interactive** dans l'interface utilisateur Web. Les intervalles de temps sont inclusifs lors d'un filtrage.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans le menu déroulant à gauche du bouton **Rechercher**, sélectionnez l'une des périodes prédéfinies.
- 2 (Facultatif) Pour définir les points initial et final de l'intervalle de temps, sélectionnez **Intervalle de temps personnalisé**.

Rechercher des événements de journaux contenant un mot clé complet

Vous pouvez rechercher des événements de journaux contenant un mot clé complet. Les mots clés contiennent des caractères alphanumériques, des traits d'union et des tirets de soulignement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.

- 2 Dans la zone de texte de recherche, tapez le mot clé complet que vous souhaitez rechercher dans les événements de journaux, puis cliquez sur le bouton **Rechercher**.

Les événements de journaux qui contiennent le mot clé complet spécifié s'affichent dans la liste.

La chaîne que vous avez recherchée est mise en surbrillance jaune.

Suivant

Vous pouvez enregistrer la requête actuelle pour la charger ultérieurement.

Rechercher les événements de journaux par opérations de champ

Vous pouvez utiliser la liste de champs existants pour rechercher des événements de journaux comportant des valeurs spécifiques pour un champ.

Important vRealize Log Insight indexe le texte intégral, les caractères alphanumériques, les traits d'union et les tirets de soulignement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Cliquez sur **Ajouter un filtre**.
- 3 Dans la ligne de filtre sous la zone de texte de recherche, utilisez le premier menu déroulant pour sélectionner un champ défini dans vRealize Log Insight.

Par exemple, **hostname**.

La liste contient tous les champs définis qui sont statistiquement disponibles, en packs de contenu, et sous forme de contenu personnalisé. Les champs sont triés par nom, à l'exception du champ **texte**. Comme **texte** est un champ spécial se référant au texte du message, **texte** s'affiche en haut de la liste et est sélectionné par défaut.

Remarque Les champs numériques contiennent des opérateurs supplémentaires absents des champs de chaînes : `=`, `>`, `<`, `>=`, `<=`. Ces opérateurs effectuent des comparaisons numériques et leur utilisation produit des résultats différents de ceux des opérateurs de chaîne. Par exemple, le filtre **response_time = 02** correspondra à un événement contenant un champ **response_time** ayant la valeur 2. Le filtre **response_time contenant 02** n'aura pas la même correspondance.

- 4 Dans la ligne de filtre sous la zone de texte de recherche, utilisez le second menu déroulant pour sélectionner l'opération à appliquer au champ sélectionné dans le premier menu déroulant.

Par exemple, sélectionnez **contient**. Le filtre **contient** correspond à des jetons complets : la recherche de « err » ne trouvera donc pas la correspondance « erreur ».

- 5 Dans la zone de texte à droite du menu déroulant de filtre, tapez la valeur que vous souhaitez utiliser comme filtre.

Vous pouvez répertorier plusieurs valeurs séparées par des virgules. L'opérateur logique entre ces valeurs est OU.

Remarque La zone de texte n'est pas disponible si vous sélectionnez l'opérateur **existe** dans le second menu déroulant.

- 6 (Facultatif) Pour ajouter d'autres filtres, cliquez sur **Ajouter un filtre**.
Un bouton bascule s'affiche au-dessus des lignes de filtre.
- 7 (Facultatif) En présence de plusieurs lignes de filtre, sélectionnez l'opérateur entre les filtres.

Option	Description
tout	Appliquer l'opération ET entre les lignes de filtre
quelconque	Appliquer l'opération OU entre les lignes de filtre

Par défaut, **tout** est sélectionné.

- 8 Cliquez sur le bouton **Rechercher**.

Exemple : Rechercher un groupe d'hôtes ayant une chaîne commune dans leur nom

Supposons que vous ayez plusieurs hôtes dont un premier se nomme w1-stvc-205-prod3 et un autre w1-stvc-206-prod5.

Pour trouver l'ensemble des journaux des deux hôtes, créez la requête suivante.

- 1 1. Laissez la zone de texte de recherche vide.
- 2 Définissez le filtre.
 - a Sélectionnez **hostname** dans le menu déroulant du champ.
 - b Sélectionnez **commence par** dans le menu déroulant de l'opérateur.
 - c Tapez **w1-stvc** dans la zone de texte de la valeur.

Vous pouvez également utiliser l'opérateur **contient**, mais vous devez alors utiliser un caractère générique dans la valeur de recherche. Dans cet exemple, vous devez taper **w1-stvc-*** dans la zone de texte de la valeur.

- 3 Cliquez sur le bouton **Rechercher**.

Suivant

Vous pouvez enregistrer la requête actuelle pour la charger ultérieurement.

Rechercher des événements qui se sont produits avant, après ou environ au même moment qu'un autre événement


Vous pouvez rechercher dans la liste d'événements de journaux les événements qui se sont produits avant, après et autour d'un événement dans la liste.

Si vous souhaitez en savoir plus sur l'état de votre environnement avant et après un événement, vous pouvez vérifier les événements rapprochés de cet événement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, localisez l'événement dans la liste.
- 2 À gauche de la ligne de l'événement, cliquez sur  et sélectionnez **Définir l'intervalle de temps à partir de cet événement**.
- 3 Dans la boîte de dialogue Définir un intervalle de temps à partir de cet événement, utilisez les menus déroulants pour sélectionner la période et la direction de l'intervalle de temps.

Vous pouvez effectuer une sélection dans une liste de périodes prédéfinies allant de 1 seconde à 10 minutes.
- 4 Cliquez sur **Définir une plage**.

Les événements entourant l'événement sélectionné s'affichent dans la liste.

Remarque Cette opération efface tous les paramètres et filtres de recherche que vous avez spécifiés précédemment.

Afficher un événement dans son contexte



Vous pouvez consulter le contexte d'un événement du journal et rechercher les événements de journaux qui se sont produits avant et après lui.

Si vous souhaitez en savoir plus sur l'état de votre environnement avant et après un événement, vous pouvez vérifier les événements rapprochés de cet événement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, localisez l'événement dans la liste.
- 2 À gauche de la ligne de l'événement, cliquez sur  et sélectionnez **Afficher un événement dans son contexte**.
- 3 (Facultatif) Faites défiler vers le haut ou vers le bas sur le bord de la fenêtre pour charger d'autres événements.
- 4 (Facultatif) Cliquez sur l'horodatage violet pour revenir au message en surbrillance.
- 5 (Facultatif) Pour ajouter des filtres, cliquez sur **Ajouter un filtre** en haut ou cliquez sur un champ à l'intérieur de l'événement en surbrillance.
- 6 (Facultatif) Ajoutez ou supprimez des types d'événements spécifiques en pointant sur un événement et en cliquant sur .

Analyser les tendances des événements

Vous pouvez analyser les tendances et les anomalies dans les journaux d'événements.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Créez et exécutez votre requête en utilisant la zone de texte de recherche et en appliquant des filtres.
- 3 Dans la boîte de dialogue Définir un intervalle de temps à partir de cet événement, utilisez les menus déroulants pour sélectionner la période et la direction de l'intervalle de temps.
- 4 Cliquez sur l'onglet **Tendances des événements**.

vRealize Log Insight compare votre requête à la période immédiatement précédente et affiche les résultats.

Effacer toutes les règles de filtrage

Vous pouvez effacer le filtrage et les résultats de recherche pour afficher la liste de tous les événements de journaux.

Une fois que vous avez effectué une recherche sur la liste d'événements, les résultats de la recherche restent affichés jusqu'à ce que vous effaciez toutes les requêtes.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, supprimez tous les filtres.
- 2 Si du texte s'affiche dans la zone de texte, supprimez-le.
- 3 Cliquez sur le bouton **Rechercher**.

Exemples de requêtes de recherche

Vous pouvez utiliser ces exemples lors de la construction de requêtes dans l'onglet **Analyse interactive** de vRealize Log Insight.

Exemple : Requête pour tous les événements de signaux de pulsation signalés par le processus ESX/ESXi hostd hier entre 9 et 10 heures

Important vRealize Log Insight indexe le texte intégral, les caractères alphanumériques, les traits d'union et les tirets de soulignement.

Afin d'effectuer une requête pour tous les événements de signaux de pulsation signalés par le processus ESX/ESXi hostd :

- 1 Dans la zone de texte de recherche, tapez **heartbeat***.
- 2 Définissez un filtre.
 - a Sélectionnez **appname** dans le premier menu déroulant.
 - b Sélectionnez **contient** dans le deuxième menu déroulant.
 - c Tapez **hostd** dans la zone de texte de la valeur.
- 3 Définissez l'intervalle de temps.
 - a Dans le menu déroulant **Intervalle de temps**, sélectionnez **Personnalisé**.
 - b Dans la première zone de texte, entrez la date d'hier et 9:00.
 - c Dans la seconde zone de texte, entrez la date d'hier et 10:00.
- 4 Cliquez sur le bouton **Rechercher**.

Exemple : Rechercher un groupe d'hôtes ayant une chaîne commune dans leur nom

Supposons que vous ayez plusieurs hôtes dont un premier se nomme w1-stvc-205-prod3 et un autre w1-stvc-206-prod5.

Pour trouver l'ensemble des journaux des deux hôtes, créez la requête suivante.

- 1 1. Laissez la zone de texte de recherche vide.
- 2 Définissez le filtre.
 - a Sélectionnez **hostname** dans le menu déroulant du champ.
 - b Sélectionnez **commence par** dans le menu déroulant de l'opérateur.
 - c Tapez **w1-stvc** dans la zone de texte de la valeur.

Vous pouvez également utiliser l'opérateur **contient**, mais vous devez alors utiliser un caractère générique dans la valeur de recherche. Dans cet exemple, vous devez taper **w1-stvc-*** dans la zone de texte de la valeur.

- 3 Cliquez sur le bouton **Rechercher**.

Exemple : Requête pour toutes les erreurs signalées par des tâches, des événements et des alarmes vCenter Server

Afin d'effectuer une requête pour toutes les erreurs signalées par des tâches, des événements et des alarmes vCenter Server :

- 1 Dans la zone de texte de recherche, tapez **error**.
- 2 Définissez un filtre.
 - a Sélectionnez **vc_event_type** dans le premier menu déroulant.
 - b Sélectionnez l'opérateur **existe** dans le second menu déroulant.
- 3 Cliquez sur le bouton **Rechercher**.

Exemple : Effectuez une requête pour la latence SCSI sur une seconde telle que signalée par ESX/ESXi

Pour effectuer une requête pour la latence SCSI sur une seconde telle que signalée par ESX/ESXi

- 1 Dans la zone de texte, tapez **scsi latency "performance has"**.
- 2 Définissez un filtre.
 - a Sélectionnez **vmw_vob_component** dans le premier menu déroulant.
 - b Sélectionnez l'opérateur **contient** dans le second menu déroulant.
 - c Tapez **scsiCorrelator** dans la zone de texte.
- 3 Définissez un second filtre.
 - a Sélectionnez **vmw_latency_in_micros** dans le premier menu déroulant.
 - b Sélectionnez l'opérateur **>** dans le second menu déroulant.
 - c Tapez **1000000** dans la zone de texte.
- 4 Cliquez sur le bouton **Rechercher**.

Exemples d'expressions régulières

Vous pouvez taper des expressions régulières dans les zones de texte de valeur de champ pour extraire certains champs des événements de journaux.

Les expressions tapées doivent respecter la syntaxe des expressions régulières Java.

Tableau 1-1. Opérateurs sur caractères

Expression régulière	Description
\	Interprète un caractère spécial
\b	Limite de mot
\B	Pas une limite de mot
\d	Un seul chiffre
\D	Un seul élément autre qu'un chiffre
\n	Nouvelle ligne
\r	Caractère Retour
\s	Un seul espace
\S	Tout caractère à l'exception d'un espace
\t	Onglet
\w	Un seul caractère alphanumérique ou trait de soulignement
\W	Un seul caractère non alphanumérique ou trait de soulignement

Par exemple, si vous avez la chaîne 1234–5678 et appliquer les expressions régulières suivantes

Expression régulière	Résultat
\d	1
\d+	1234
\w+	1234
\S	1234-5678

Tableau 1-2. Opérateurs quantificateurs

Expression régulière	Description
.	Tout caractère à l'exception du caractère nouvelle ligne
*	Zéro caractère ou plus tant que cela est possible
?	Zéro ou un seul caractère OU aussi court que possible
+	Un ou plus
{<n>}	Exactement <n> fois
{<n>,<m>}	<n> à <m> fois

Par exemple, si vous avez la chaîne aaaaa et appliquer les expressions régulières suivantes

Expression régulière	Résultat
.	a
*	aaaaa
.*?	aaaaa
{1}	a
{1,2}	aa

Tableau 1-3. Opérateurs de combinaisons

Expression régulière	Description
.	N'importe quoi
.*?	N'importe quoi aussi court que possible avant

Par exemple, si vous avez la chaîne a b 3 hi d hi et appliquez les expressions régulières suivantes

Expression régulière	Résultat
a.* hi	b 3 hi d
a . * ? hi	b 3

Tableau 1-4. Opérateurs logiques

Expression régulière	Description
^	Début d'une ligne OU non si entre crochets
\$	Fin de ligne
()	Encapsulation
[]	Un seul caractère entre crochets
	OR
-	Plage
\A	Début d'une chaîne
\Z	Fin d'une chaîne

Par exemple, si vous appliquez les expressions régulières suivantes

Expression régulière	Résultat
(bonjour)?	Contient bonjour OU ne contient pas bonjour
(a b c)	a OU b OU c
[a-cp]	a OU b OU c OU p
monde\$	Se termine avec monde suivi d'aucun autre caractère

Tableau 1-5. Opérateurs d'anticipation

Expression régulière	Description
?=	Anticipation positive (contient)
?!=	Anticipation négative (ne contient pas)

Par exemple, si vous appliquez les expressions régulières suivantes

Expression régulière	Résultat
is (?=w+)\w{2} primary	is FT primary? faux
opid=(?!WfU-1fecf8f9)\S+	WfU-3c9bb994

Tableau 1-6. Autres exemples d'expressions régulières

Expression régulière	Description
[xyz]	x, y ou z
(info avertissement erreur)	info, avertissement ou erreur
[a-z]	Lettre minuscule
[^a-z]	Lettre non minuscule
[a-z]+	Une ou plusieurs lettres minuscules
[a-z]*	Zéro lettre minuscule ou plus
[a-z]?	Zéro ou une lettre minuscule
[a-z] {3}	Exactement trois lettres minuscules
[d]	Un chiffre
\d+\$	Un ou plusieurs chiffres suivis par la fin d'un message
[0-5]	Un nombre compris entre 0 et 5
\w	Un caractère d'un mot (lettre, livre ou trait de soulignement)
\s	Espace
\S	Tout caractère à l'exception d'un espace
[a-zA-Z0-9]+	Un ou plusieurs caractères alphanumériques
([a-z] {2,} [0-9] {3,5})	Deux lettres ou plus suivies de trois à cinq chiffres

Utilisation du diagramme Analyse interactive pour analyser des journaux

Le diagramme en haut de la page **Analyse interactive** vous permet d'effectuer une analyse visuelle des résultats de votre requête.

Les diagrammes représentent des snapshots graphiques des requêtes de recherche de journaux. Vous pouvez utiliser les menus déroulants sous le diagramme pour changer de type de diagramme.

Vous pouvez utiliser le premier menu déroulant à gauche pour contrôler le niveau d'agrégation du diagramme. La fonction **Nombre** est sélectionnée par défaut.

Types de diagramme

Vous pouvez sélectionner différents types de diagramme pour changer le mode de visualisation des données dans la page Analyse interactive.

Différents types de diagrammes nécessitent différentes fonctions d'agrégation, l'utilisation de séries chronologiques et des champs de regroupement. Les affichages de diagramme sont limités aux 2 000 résultats les plus récents.

Type diagramme	Fonction d'agrégation	Exigence de séries chronologiques	Exigence de champ de regroupement
Colonne	Quelconque	Séries chronologiques	S/O
Ligne	Quelconque	Séries chronologiques	S/O
Zone	Quelconque	Séries chronologiques	S/O
Barre	Quelconque	Séries non chronologiques	Au moins un champ
Secteur	Nombre ou nombre unique	Séries non chronologiques	Au moins un champ
Bulle	Quelconque	Séries non chronologiques	Deux champs
Indicateur	Nombre	Séries non chronologiques	S/O
Scalaire	Nombre	Séries non chronologiques	S/O
Comparatif	Quelconque	Quelconque	S/O

Diagrammes multifonction

Vous pouvez utiliser des diagrammes multifonction pour comparer les variables de différentes échelles.

Avec les diagrammes multifonction, vous pouvez attribuer un axe y à chaque série ou un axe x si vous souhaitez comparer des ensembles de données de catégories différentes. Chaque acte peut être placé à droite ou à gauche du diagramme. Vous pouvez changer les fonctions pour changer l'axe y sur lequel elles sont tracées de droite à gauche.

Par exemple, vous pouvez inclure dans un diagramme le nombre d'événements groupé par canal et niveau, ainsi que la moyenne des tâches groupée par canal et niveau.

Fonction d'agrégation

vRealize Log Insight fournit plusieurs fonctions d'agrégation.

Type	Champ	Description
Nombre	Événements seulement	Crée un diagramme du nombre d'événements d'une requête spécifique.
Nombre unique	Tout champ	Crée un diagramme du nombre de valeurs uniques d'un champ.
Minimum	Champs numériques uniquement	Crée un diagramme de la valeur minimale d'un champ.
Maximum	Champs numériques uniquement	Crée un diagramme de la valeur maximale d'un champ.
Moyenne	Champs numériques uniquement	Crée un diagramme de la valeur moyenne d'un champ.
Éc. type	Champs numériques uniquement	Crée un diagramme de l'écart type des valeurs d'un champ.


Type	Champ	Description
Somme	Champs numériques uniquement	Crée un diagramme de la somme des valeurs d'un champ.
Variance	Champs numériques uniquement	Crée un diagramme de la variance des valeurs d'un champ.

Vous ne pouvez pas modifier le mode d'affichage des résultats des requêtes.

Afficher	Description
Pour grouper les résultats des requêtes par valeurs de champ spécifiques	Utilisez le deuxième menu déroulant sous le diagramme pour grouper les résultats des requêtes par valeurs de champ spécifiques plutôt que par séries chronologiques ou en complément de celles-ci.
Pour afficher le nombre d'événements d'un champ	Par exemple, le nombre d'événements par hôte, décochez la case Séries chronologiques et sélectionnez la case de ce champ.
Pour afficher un graphique à barres empilées pour un champ avec groupements dans le temps	Cochez la case Séries chronologiques et la case du champ.

Utilisation de diagrammes

Vous pouvez modifier l'aspect des diagrammes dans l'onglet **Analyse interactive**, ajouter des diagrammes à vos tableaux de bord personnalisés et gérer des diagrammes de tableau de bord.

Tâche	Procédure
Modifier l'intervalle de temps d'un diagramme	Dans l'onglet Analyse interactive , utilisez le menu déroulant à gauche du bouton Rechercher pour modifier la période affichée dans le diagramme.
Modifier la granularité d'un diagramme	Dans l'onglet Analyse interactive , utilisez les boutons dans le coin supérieur droit pour alterner entre différents intervalles de temps pour chaque point représenté dans le diagramme. Les intervalles disponibles varient en fonction de l'intervalle de temps spécifié pour la requête.
Charger un diagramme de tableau de bord dans l'onglet Analyse interactive	<p>Dans l'onglet Tableaux de bord, localisez le diagramme et cliquez sur l'icône Ouvrir dans Analyse interactive .</p> <p>L'intervalle de temps est défini à l'intervalle de temps actuel du tableau de bord. Vous pouvez modifier l'intervalle de temps si nécessaire.</p>
Enregistrer un diagramme dans votre tableau de bord personnalisé	<ol style="list-style-type: none"> 1 En haut à gauche de l'onglet Analyse interactive, cliquez sur Ajouter au tableau de bord. Vous pouvez également aller au menu situé à droite du bouton Rechercher et sélectionner Ajouter la requête actuelle au tableau de bord. 2 Tapez un nom, sélectionnez le tableau de bord de destination dans le menu déroulant, sélectionnez le type de widget, ajoutez des informations sur le widget, puis cliquez sur Ajouter.
Enregistrer une requête sous la forme d'un diagramme dans votre tableau de bord personnalisé	<ol style="list-style-type: none"> 1 Cliquez sur Ajouter la requête actuelle au tableau de bord en regard du bouton Rechercher. 2 Tapez un nom, sélectionnez le tableau de bord de destination dans le menu déroulant, assurez-vous que le type de widget est défini sur Diagramme, ajoutez des informations sur le widget et cliquez sur Ajouter.

Tâche	Procédure
Enregistrer une requête sous la forme d'un tableau de champs dans votre tableau de bord personnalisé	<ol style="list-style-type: none"> 1 Cliquez sur Ajouter la requête actuelle au tableau de bord en regard du bouton Rechercher. 2 Tapez un nom, sélectionnez le tableau de bord de destination dans le menu déroulant, assurez-vous que le type de widget est défini sur Tableau de champs, ajoutez des informations sur le widget, et cliquez sur Ajouter.
Supprimer un widget de votre tableau de bord personnalisé	<ol style="list-style-type: none"> 1 Dans l'onglet Tableaux de bord, sélectionnez le tableau de bord personnalisé qui contient le widget que vous souhaitez supprimer. 2 Dans le coin supérieur droit du widget, cliquez sur l'icône Autres actions ⚙️, puis sélectionnez Supprimer. 3 Dans la boîte de dialogue Supprimer le widget, cliquez sur Supprimer pour confirmer.

Modifier le type de diagramme Analyse interactive

Vous pouvez modifier l'agrégation et le regroupement des résultats de requête affichés dans le diagramme pour analyser graphiquement les événements de journaux.

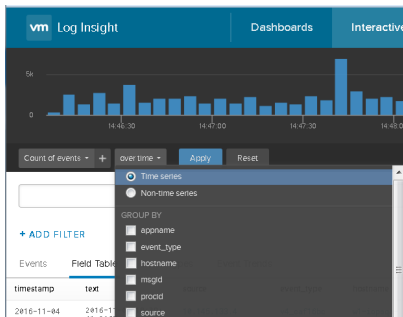
Le nombre de menus déroulants visibles sous le diagramme dépend de la fonction d'agrégation sélectionnée.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Utilisez les menus déroulants sous le diagramme Analyse interactive pour modifier la fonction d'agrégation et le type de regroupement.



- Pour voir le nombre d'événements dans le temps, sélectionnez le bouton **Séries chronologiques**.
 - Pour voir uniquement les valeurs d'événement, sélectionnez le bouton **Séries non chronologiques** et sélectionnez au moins un champ.
- 2 Cliquez sur **Mise à jour**.

Exemple : Agrégation et regroupement dans le diagramme Analyse interactive

Le tableau suivant contient des exemples illustrant l'agrégation et le regroupement dans les diagrammes vRealize Log Insight.

Tableau 1-7. Exemple d'agrégation et de regroupement dans le diagramme Analyse interactive

Sélection dans le premier menu déroulant	Sélection dans le second menu déroulant	Sélection de séries chronologiques	Texte affiché à l'écran	Résultat
Nombre	Séries chronologiques	Séries chronologiques	Nombre d'événements dans le temps	Le diagramme affiche un diagramme à barres indiquant le nombre d'événements pour la requête actuelle dans le temps.
Moyenne	vmw_op_latency (VMware - vSphere)	Séries chronologiques	Moyenne de vmw_op_latency (VMware - vSphere) dans le temps	Le diagramme affiche un diagramme linéaire de la valeur moyenne de la latence des opérations dans le temps.
Nombre	vmw_esx_problem Remarque Le champ Thevmw_esx_problem ne s'affiche pas par défaut. Vous devez extraire le champ vmw_esx_problem et enregistrer la requête afin que vmw_esx_problem s'affiche dans le menu déroulant.	Séries non chronologiques	Nombre d'événements groupés par vmw_esx_problem	Le diagramme affiche un diagramme à barres du nombre d'événements contenant le champ vmw_esx_problem.
Nombre	Séries chronologiques, vmw_esx_problem	Séries chronologiques	Nombre d'événements dans le temps groupés par vmw_esx_problem	Le diagramme affiche un diagramme à barres empilées groupé par vmw_esx_problem dans le temps.

Extraction de champs dynamique

Dans un grand environnement produisant de nombreux événements de journaux, vous ne pouvez pas toujours localiser les champs de données que vous considérez importants.

vRealize Log Insight propose une extraction de champs au moment de l'exécution pour résoudre ce problème. Vous pouvez extraire dynamiquement n'importe quel champ des données en fournissant une expression régulière. Reportez-vous à [Exemples d'expressions régulières](#).

Remarque Les requêtes génériques peuvent être très lentes. Par exemple, si vous tentez d'extraire un champ en utilisant l'expression `\(\d+\)`, la requête renvoie tous les événements de journaux qui contiennent des nombres entre parenthèses. Vérifiez que vos requêtes incluent le maximum de contexte textuel possible. Par exemple, la requête d'extraction de champ `Event for vm\(\d+\)` serait plus efficace.

Vous pouvez utiliser les champs extraits pour effectuer une recherche et un filtrage dans la liste d'événements de journaux ou pour agréger des événements dans le diagramme Analyse interactive.

Extraire des champs à l'aide d'une extraction en un clic

Au lieu de taper des valeurs contextuelles pour l'extraction dynamique de champs, vous pouvez utiliser la fonction d'extraction en un clic.

L'extraction en un clic remplit toutes les valeurs contextuelles correspondant au champ que vous sélectionnez dans un événement de journal.

Remarque L'option d'extraction en un clic est uniquement disponible dans l'onglet Événements.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans la liste d'événements de journaux, mettez en surbrillance le texte qui représente le champ que vous souhaitez extraire.

Un menu d'action s'affiche au-dessus de l'ensemble des noms de champs présents dans cet événement.

- 3 Cliquez sur **Extraire le champ**.

Les valeurs contextuelles avant et après du volet Champs sont remplies automatiquement avec le contexte requis pour extraire le champ mis en surbrillance.

- 4 (Facultatif) Modifiez l'expression régulière de la valeur extraite dans le volet Champ.
- 5 (Facultatif) Modifiez les expressions régulières contextuelles Pre et Post dans le volet Champs.
- 6 (Facultatif) Cliquez sur **+ Ajouter un contexte supplémentaire** pour ajouter d'autres mots clés et filtres.

Vous pouvez ajouter un ou plusieurs mots clés et utiliser un champ unique statique comme filtre.

- 7 Si vous êtes un utilisateur administrateur, sélectionnez les utilisateurs pouvant accéder au champ dans le menu déroulant.

Option	Description
Tous les utilisateurs	Tous les utilisateurs verront le champ dans leurs événements et dans le menu déroulant du filtre.
Moi seulement	Seul le créateur du champ verra ce dernier dans ses événements et dans le menu déroulant du filtre.

- 8 (Facultatif) En haut du volet Champs, cliquez sur  et sur **Modifier** pour ajouter des remarques à ce champ. Ajoutez des remarques dans la fenêtre **Modifier les remarques**, puis cliquez sur **OK**.

- 9 Cliquez sur **Enregistrer**.

Suivant

Vous pouvez utiliser le champ extrait pour effectuer une recherche et un filtrage dans la liste d'événements de journaux, ou pour agréger des événements dans le diagramme Analyse interactive.

Vous pouvez modifier les définitions de champs enregistrées ou les supprimer si vous n'en avez plus besoin.

Modifier un champ extrait

Vous pouvez modifier les définitions de champs extraits.

vRealize Log Insight crée des copies des champs que vous utilisez lors de la création de diagrammes, de requêtes ou d'alertes. Si vous modifiez une définition de champ, tous les diagrammes, les requêtes et les alertes qui utilisent le champ modifié sont mis à jour pour refléter la nouvelle définition.

Les utilisateurs normaux ne peuvent modifier que leur propre contenu. Les utilisateurs administrateurs peuvent modifier leur propre contenu et leur contenu partagé.

Les champs de pack de contenu sont en lecture seule.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 En haut du volet Champs, cliquez sur **Gérer les champs extraits**  et sélectionnez un champ extrait dans la liste.

3 Modifiez les valeurs et cliquez sur **Mettre à jour**.

Une boîte de dialogue affiche une liste de contenus qui seront affectés par le champ mis à jour. Si le champ est partagé par plusieurs utilisateurs, la boîte de dialogue affiche également une liste d'utilisateurs affectés.

4 (Facultatif) En haut du volet Champs, cliquez sur et sur **Modifier** pour ajouter des remarques à ce champ. Ajoutez des remarques dans la fenêtre **Modifier les remarques**, puis cliquez sur **OK**.

5 Cliquez sur **Mettre à jour** pour confirmer vos modifications.

vRealize Log Insight met à jour toutes les requêtes, alertes et diagrammes qui utilisent le champ que vous avez modifié.

Dupliquer un champ extrait

Vous pouvez dupliquer un champ extrait.



Vous utilisez l'option Dupliquer lorsque vous souhaitez extraire plusieurs champs d'un événement et lorsque les deux champs s'affichent dans un contexte similaire. Après que vous avez extrait et enregistré un champ, ouvrez la définition du champ extrait et utilisez l'option Dupliquer. Le champ dupliqué a exactement la même définition que le champ extrait d'origine. Vous pouvez modifier la définition du champ dupliqué pour qu'il corresponde à une autre valeur dans l'événement qui vous intéresse.

Les utilisateurs normaux ne peuvent dupliquer que leur propre contenu. Les utilisateurs administrateurs peuvent modifier leur propre contenu et leur contenu partagé.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 En haut du volet Champs, cliquez sur **Gérer les champs extraits**  et sélectionnez un champ extrait dans la liste.
- 3 Cliquez sur **Dupliquer** pour créer une copie du champ.
- 4 (Facultatif) Modifiez l'expression régulière de la valeur extraite dans le volet Champ.
- 5 (Facultatif) Modifiez les expressions régulières contextuelles Pre et Post dans le volet Champs.
- 6 (Facultatif) Cliquez sur  **Ajouter un contexte supplémentaire** pour ajouter d'autres mots clés et filtres.

Vous pouvez ajouter un ou plusieurs mots clés et utiliser un champ unique statique comme filtre.

- 7 Si vous êtes un utilisateur administrateur, sélectionnez les utilisateurs pouvant accéder au champ dans le menu déroulant.

Option	Description
Tous les utilisateurs	Tous les utilisateurs verront le champ dans leurs événements et dans le menu déroulant du filtre.
Moi seulement	Seul le créateur du champ verra ce dernier dans ses événements et dans le menu déroulant du filtre.

- 8 Cliquez sur **Enregistrer**.

Suivant


Vous pouvez utiliser le champ extrait pour effectuer une recherche et un filtrage dans la liste d'événements de journaux, ou pour agréger des événements dans le diagramme Analyse interactive.

Vous pouvez modifier les définitions de champs enregistrées ou les supprimer si vous n'en avez plus besoin.

Supprimer un champ extrait

Vous pouvez supprimer les champs extraits dont vous n'avez plus besoin.

vRealize Log Insight crée des copies des champs que vous utilisez lors de la création de widgets, de requêtes ou d'alertes. Si vous supprimez un champ qui est utilisé dans des widgets, des requêtes ou des alertes, vRealize Log Insight crée une copie temporaire du champ supprimé pour chaque widget, requête ou alerte qui utilise ce champ.


Vous pouvez supprimer uniquement les champs dont les noms sont accompagnés de l'icône **Modifier ce champ** . Les utilisateurs normaux ne peuvent supprimer que leur propre contenu. Les utilisateurs administrateurs peuvent supprimer leur propre contenu et leur contenu partagé.

Les champs de pack de contenu sont en lecture seule.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 En haut du volet Champs, cliquez sur **Gérer les champs extraits**  et passez le curseur sur un champ extrait dans la liste.

3 Cliquez sur .

Une boîte de dialogue affiche la liste du contenu qui utilise le champ que vous souhaitez supprimer. Si vous êtes un utilisateur administrateur et si le champ est partagé par plusieurs utilisateurs, la boîte de dialogue affiche également la liste des utilisateurs concernés.

4 Cliquez sur **Supprimer** pour confirmer

Si un champ supprimé est utilisé dans des requêtes existantes, vRealize Log Insight crée une copie temporaire de ce champ et l'affiche lorsque vous chargez une requête qui utilise le champ supprimé.

Si vous exportez du contenu contenant des champs temporaires, vRealize Log Insight crée les champs dans le contenu exporté pour éviter la présence de champs temporaires.

Gestion de requêtes de recherche

Vous pouvez exporter des résultats de requêtes, partager vos requêtes avec d'autres utilisateurs, et enregistrer, supprimer, renommer et charger des requêtes existantes. Vous pouvez prendre des snapshots de requêtes et les enregistrer dans les tableaux de bord.


Enregistrer une requête dans vRealize Log Insight

Vous pouvez enregistrer votre requête actuelle et l'intervalle de temps dans vRealize Log Insight pour la consulter ultérieurement. Les requêtes enregistrées peuvent uniquement être chargées à partir de la page **Analyse interactive**.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, effectuez la requête que vous souhaitez enregistrer.
- 2 Cliquez sur l'icône **Ajouter une requête actuelle aux favoris** .
- 3 Tapez un nom et cliquez sur **Enregistrer**.

Remarque Les requêtes enregistrées comportent un intervalle de temps fixe et ne sont pas mises à jour. En enregistrant une requête, vous prenez un snapshot des messages de journaux disponibles dans l'intervalle de temps au moment de l'enregistrement.

La requête est ajoutée à la liste Requêtes favorites.

Tous les utilisateurs, notamment les administrateurs, disposent d'une liste individuelle de requêtes enregistrées.



Renommer une requête dans vRealize Log Insight

Vous pouvez renommer une requête que vous avez enregistrée dans vRealize Log Insight.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Cliquez sur l'icône Requetes favorites .
- 3 Pointez la requête que vous souhaitez renommer, puis cliquez sur l'icône **Modifier cette requête enregistrée** .
- 4 Tapez un nouveau nom et cliquez sur **Enregistrer**.

Charger une requête dans vRealize Log Insight

Vous pouvez charger des requêtes à partir de requêtes ou de packs de contenu que vous avez enregistrés pour les afficher dans l'onglet **Analyse interactive**.


Les requêtes enregistrées sont séparées des éléments du tableau de bord. Elles ne s'affichent pas sur un tableau de bord personnalisé. Si vous souhaitez afficher une requête enregistrée, vous devez la charger.

Tous les utilisateurs, notamment les administrateurs, disposent d'une liste individuelle de requêtes enregistrées.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Cliquez sur l'icône Requetes favorites .
- 3 Dans la liste Requetes favorites, cliquez sur la requête que vous souhaitez afficher dans l'onglet **Analyse interactive**.

La requête est chargée dans l'onglet **Analyse interactive**. L'intervalle de temps de la requête s'affiche au-dessus de la liste d'événements.

Suivant

Vous pouvez ajouter la requête à un tableau de bord, modifier la granularité du diagramme ou appliquer un filtrage supplémentaire aux résultats de la requête.



Supprimer une requête de vRealize Log Insight

Vous pouvez supprimer des requêtes enregistrées de vRealize Log Insight.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu déroulant à droite du bouton **Rechercher**, sélectionnez **Charger la requête**.
- 3 Cliquez sur l'icône Requetes favorites .
- 4 Dans la liste Requetes favorites, cliquez sur  en regard de la requête à supprimer.
- 5 Cliquez sur **Supprimer** pour confirmer


Partager la requête actuelle

Vous pouvez envoyer à vos homologues un lien vers la requête actuelle.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, effectuez la requête que vous souhaitez partager.
- 2 Cliquez sur  et sélectionnez **Partager la requête**.
vRealize Log Insight crée et affiche une URL raccourcie pour la requête. L'URL est conservée 93 jours après sa dernière utilisation avant d'être supprimée.
- 3 Copiez l'URL et envoyez-la à la personne avec qui vous souhaitez la partager.


Exporter la requête actuelle

Vous pouvez exporter les résultats d'une requête de journal pour les partager avec d'autres systèmes, ou les transférer vers votre contact de support.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, effectuez la requête que vous souhaitez exporter.
- 2 Cliquez sur  et sélectionnez **Exporter des résultats d'événements**.
- 3 Sélectionnez le format d'enregistrement de la requête, puis cliquez sur **Exporter**.

Option	Description
Événements bruts	Sélectionnez cette option pour enregistrer les résultats au format TXT
JSON	Sélectionnez cette option pour enregistrer les résultats au format JSON
XML	Sélectionnez cette option pour enregistrer les résultats au format XML

Prendre un snapshot d'une requête

Vous pouvez prendre un snapshot de votre requête actuelle et l'intervalle de temps dans vRealize Log Insight pour une visualisation rapide ou pour l'enregistrer dans un tableau de bord. Les snapshots peuvent être pris sur la page Analyse interactive.


Un snapshot enregistre les messages disponibles du journal dans l'intervalle de temps au moment où vous prenez le snapshot. Après avoir pris un snapshot, cliquez dessus pour revenir à la requête lorsque vous avez pris le snapshot. Pour enregistrer un ou plusieurs snapshots, ajoutez-les à un tableau de bord existant ou créez-en un.


Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, effectuez la requête que vous souhaitez enregistrer comme snapshot.
- 2 Cliquez sur l'icône Snapshot.
Le snapshot s'affiche au bas de l'écran.
- 3 (Facultatif) Modifiez la requête et prenez d'autres snapshots.
Les snapshots s'affichent au bas de l'écran.

- 4 (Facultatif) Au bas de l'écran, cliquez sur  et sélectionnez **Tout enregistrer dans le tableau de bord**.
 - a Sélectionnez un tableau de bord existant ou créez-en un.
 - b Cliquez sur **Ajouter**.

Le snapshot est ajouté au tableau de bord sélectionné ou au nouveau.
- 5 (Facultatif) Pour supprimer le snapshot, cliquez sur le « X » sur un snapshot.
- 6 (Facultatif) Cliquez sur  et sélectionnez **Supprimer tout** pour supprimer les snapshots.

Utilisation de tableaux de bord

Les tableaux de bord dans vRealize Log Insight sont des collections de widgets Diagramme, Tableaux de champ et Liste de requêtes.

Tableaux de bord personnalisés

Les tableaux de bord personnalisés sont créés par les utilisateurs de l'instance actuelle de vRealize Log Insight. Les tableaux de bord personnalisés sont organisés en deux catégories, Mes tableaux de bord et Tableaux de bord partagés. Les tableaux de bord partagés sont visibles par tous les utilisateurs de l'instance de vRealize Log Insight.

Mes tableaux de bord sont propres à un utilisateur.

Les utilisateurs normaux ne peuvent modifier que les tableaux de bord de la section Mes tableaux de bord.

Les utilisateurs Admin peuvent modifier les tableaux de bord de la section Mes tableaux de bord et ceux qu'ils ont créés dans la section Tableaux de bord partagés.

Tableaux de bord de packs de contenu

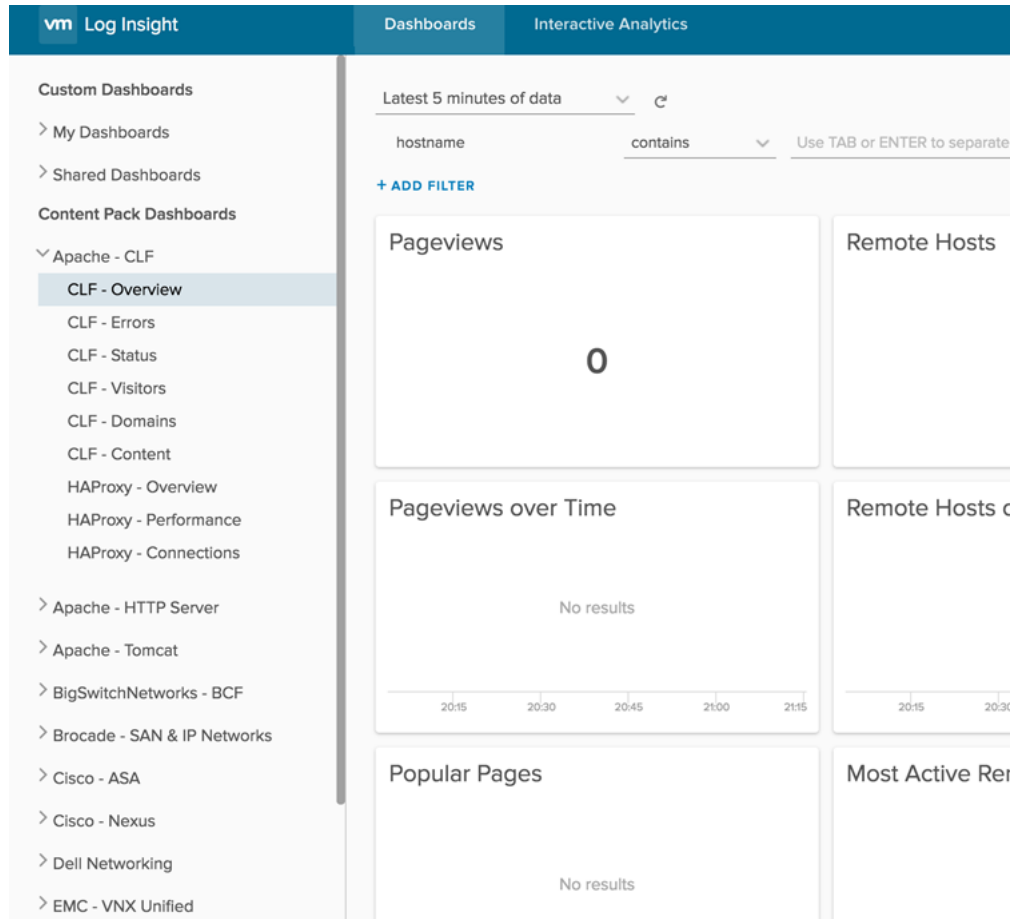
Les tableaux de bord de pack de contenu sont importés avec des packs de contenu et sont visibles par tous les utilisateurs de l'instance de vRealize Log Insight.

Remarque Les tableaux de bord du pack de contenu sont en lecture seule. Vous ne pouvez ni les supprimer ni les renommer. Toutefois, vous pouvez cloner les tableaux de bord du pack de contenu dans votre tableau de bord personnalisé. Vous pouvez cloner les tableaux de bord entiers ou les widgets séparés.

Pour voir les tableaux de bord qui sont disponibles dans votre instance de vRealize Log Insight, cliquez sur **Tableaux de bord** dans le coin supérieur gauche de l'interface utilisateur de vRealize Log Insight. Le volet qui s'affiche à gauche répertorie tous les tableaux de bord auxquels vous avez accès, ceux-ci étant regroupés par tableaux de bord personnalisés et tableaux de bord des packs de contenu. Cliquez sur le

signe > en regard de chaque sous-groupe pour afficher les tableaux de bord associés. Vous pouvez ouvrir un groupe de tableaux de bord à la fois en cliquant sur le signe > en regard du nom du groupe. Cliquez sur le signe > en regard d'un autre nom de groupe pour ouvrir un nouveau groupe et fermer le précédent. Il n'est possible d'ouvrir qu'un seul groupe à la fois.

Pour voir le contenu d'un tableau de bord, cliquez sur le nom du tableau de bord dans la liste à gauche.







Gestion de tableaux de bord

Vous pouvez ajouter, modifier et supprimer des tableaux de bord dans votre espace Tableaux de bord personnalisés.

Les tableaux de bord de pack de contenu ne peuvent pas être modifiés, mais vous pouvez les cloner dans votre espace Tableaux de bord personnalisés et modifier les clones.

Important vRealize Log Insight n'effectue pas de contrôles pour détecter des noms dupliqués pour les tableaux de bord, les requêtes et les alertes que vous enregistrez ou clonez. Le nom d'affichage n'est pas un identificateur unique lorsque vRealize Log Insight enregistre les requêtes. Par conséquent, vous pouvez enregistrer plusieurs diagrammes, alertes et tableaux de bord sous le même nom. Pour améliorer les possibilités de récupération de données, ne dupliquez pas les noms lors de l'enregistrement de diagrammes, d'alertes ou de tableaux de bord.

Tableau 1-8. Utilisation de tableaux de bord personnalisés

Tâche	Procédure
Créer un nouveau tableau de bord personnalisé	Dans l'onglet Tableaux de bord , sélectionnez Mes tableaux de bord , puis cliquez sur Nouveau tableau de bord dans le coin inférieur gauche.
Modifiez le nom d'un tableau de bord personnalisé	Dans l'onglet Tableaux de bord , pointez le nom du tableau de bord, cliquez sur l'icône du menu  et sélectionnez Renommer . Entrez un nouveau nom et cliquez sur Enregistrer .
Supprimer un tableau de bord personnalisé	Dans l'onglet Tableaux de bord , pointez le nom du tableau de bord, cliquez sur l'icône du menu  et sélectionnez Supprimer . Dans la boîte de dialogue de confirmation, sélectionnez Supprimer .
Cloner un tableau de bord à partir d'un pack de contenu dans votre tableau de bord personnalisé	<ol style="list-style-type: none"> 1 Dans l'onglet Tableaux de bord, sélectionnez un pack de contenu et pointez le tableau de bord à cloner. 2 Cliquez sur l'icône de menu  et sélectionnez Cloner dans le menu déroulant. 3 Tapez un nom et cliquez sur Enregistrer. <p>Si vous êtes un utilisateur administrateur, vous pouvez choisir de partager ou non votre tableau de bord avec d'autres utilisateurs.</p>
Ajouter un widget Diagramme à un tableau de bord	<ol style="list-style-type: none"> 1 En haut à gauche de l'onglet Analyse interactive, cliquez sur Ajouter au tableau de bord. Vous pouvez également aller au menu situé à droite du bouton Rechercher et sélectionner Ajouter la requête actuelle au tableau de bord. 2 Tapez un nom, sélectionnez le tableau de bord de destination dans le menu déroulant, sélectionnez le type de widget, ajoutez des informations sur le widget, puis cliquez sur Ajouter.
Ajouter un widget Liste de requêtes au tableau de bord	Reportez-vous à Ajouter un widget Liste de requêtes au tableau de bord .
Ajouter une requête à un widget Liste de requêtes dans un tableau de bord	Reportez-vous à Ajouter une requête à un widget Liste de requêtes dans un tableau de bord .
Ajouter une requête à un widget Tableau de champs dans un tableau de bord	Reportez-vous à Ajouter un widget Tableau de champs à un tableau de bord
Ajouter un widget Types d'événements à un tableau de bord	Ajouter un widget Types d'événements à un tableau de bord
Ajouter un widget Tendances des événements à un tableau de bord	Ajouter un widget Tendances des événements à un tableau de bord
Supprimer un widget d'un tableau de bord	<ol style="list-style-type: none"> 1 Dans l'onglet Tableaux de bord, sélectionnez le tableau de bord personnalisé qui contient le widget que vous souhaitez supprimer. 2 Dans le coin supérieur droit du widget, cliquez sur l'icône Autres actions , puis sélectionnez Supprimer. 3 Dans la boîte de dialogue Supprimer le widget, cliquez sur Supprimer pour confirmer.


Ajouter un widget Liste de requêtes au tableau de bord

Vous pouvez créer des widgets Liste de requêtes afin d'enregistrer les listes de requêtes de recherche de vos tableaux de bord personnalisés.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête que vous souhaitez ajouter au tableau de bord.
- 2 Cliquez sur l'icône **Ajouter la requête actuelle au tableau de bord** .
- 3 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord auquel vous souhaitez ajouter la requête.
- 4 Dans le menu déroulant **Type de widget**, sélectionnez **Liste de requêtes**.
- 5 Dans le menu déroulant **Liste de requêtes**, sélectionnez **Nouvelle liste de requêtes**, tapez un nom pour la liste, puis cliquez sur **Enregistrer**.
- 6 Cliquez sur **Add**.

Le widget Liste de requêtes s'affiche sur le tableau de bord que vous avez spécifié.

Suivant

Vous pouvez ajouter des requêtes au widget Liste de requêtes que vous avez créé. Reportez-vous à [Ajouter une requête à un widget Liste de requêtes dans un tableau de bord](#).

Ajouter une requête à un widget Liste de requêtes dans un tableau de bord


Les widgets Liste de requêtes permettent d'accéder rapidement à une ou plusieurs requêtes enregistrées à partir du tableau de bord.

Vous pouvez modifier les widgets Liste de requêtes personnalisés pour ajouter de nouvelles requêtes.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête que vous souhaitez ajouter au widget Liste de requêtes.
- 2 Cliquez sur l'icône **Ajouter la requête actuelle au tableau de bord** .
- 3 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord qui contient le widget Liste de requêtes.
- 4 Dans le menu déroulant **Type de widget**, sélectionnez **Liste de requêtes**.
- 5 Dans le menu déroulant **Liste de requêtes**, sélectionnez le nom du widget auquel vous souhaitez ajouter la requête, puis cliquez sur **Enregistrer**.
- 6 Cliquez sur **Add**.

vRealize Log Insight ajoute la requête au widget que vous avez sélectionné.

Remarque Les widgets Liste de requêtes utilisent des requêtes de message. Si vous utilisez la même requête de message dans un widget Diagramme et choisissez un champ de regroupement qui n'existe dans aucun des messages, le diagramme n'affiche aucun résultat.


Ajouter un widget Tableau de champs à un tableau de bord

Les widgets Tableau de champs permettent d'accéder à un ou plusieurs champs enregistrés rapidement, à partir du tableau de bord.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête que vous souhaitez ajouter au widget Tableau de champs.
- 2 Cliquez sur l'icône **Ajouter la requête actuelle au tableau de bord** .
- 3 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord auquel vous souhaitez ajouter le tableau de champs.
- 4 Dans le menu déroulant **Type de widget**, sélectionnez **Tableau de champs**.
- 5 Sélectionnez les champs que vous souhaitez inclure dans le tableau de champs.
- 6 Cliquez sur **Add**.

Le widget Tableaux de champs s'affiche sur le tableau de bord que vous avez spécifié.


Ajouter un widget Types d'événements à un tableau de bord

Les widgets Types d'événements fournissent un accès à des groupes de types d'événements, qui sont créés via l'apprentissage automatique pour regrouper les événements semblables.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête que vous souhaitez ajouter au widget.
- 2 Cliquez sur l'icône **Ajouter la requête actuelle au tableau de bord** .
- 3 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord auquel vous souhaitez ajouter le widget.
- 4 Dans le menu déroulant **Type de widget**, sélectionnez Types d'événements.
- 5 Cliquez sur **Add**.

Le widget s'affiche sur le tableau de bord que vous avez spécifié.


Ajouter un widget Tendances des événements à un tableau de bord

Les widgets Tendances des événements fournissent un accès à des informations sur les tendances des événements, qui analysent les tendances sur une période spécifiée.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête que vous souhaitez ajouter au widget.
- 2 Cliquez sur l'icône **Ajouter la requête actuelle au tableau de bord** .
- 3 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord auquel vous souhaitez ajouter le widget.
- 4 Dans le menu déroulant **Type de widget**, sélectionnez Tendances des événements.
- 5 Cliquez sur **Add**.

Le widget s'affiche sur le tableau de bord que vous avez spécifié.

Filtrer à l'aide de valeurs de champs de diagrammes

Vous pouvez utiliser une valeur de champ dans un diagramme comme filtre sur le tableau de bord qui contient le diagramme, sur un autre tableau de bord qui utilise le champ et dans Analyse interactive.

Si vous détectez un problème sur une valeur de champ, dans un diagramme, vous pouvez rapidement utiliser la valeur de champ comme entrée et passer à un autre tableau de bord qui utilise ce champ. Si aucun autre tableau de bord n'utilise ce champ, vous pouvez utiliser la valeur de champ comme filtre sur le même tableau de bord ou l'exécuter dans Analyse interactive.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans le menu déroulant **Tableau de bord**, sélectionnez le tableau de bord qui contient un widget Diagramme.
- 2 Dans le widget Diagramme, pointez les données du diagramme et visualisez les valeurs de champ qui s'affichent sous la forme d'info-bulles.

- 3 Cliquez sur la valeur de champ que vous souhaitez utiliser comme filtre.

Le menu **Ajouter une valeur comme filtre** s'affiche.

- 4 Sélectionnez l'endroit où vous souhaitez utiliser la valeur de champ comme filtre.

Option	Action
Analyse interactive	La page Analyse interactive s'ouvre et affiche les résultats de la requête de diagramme. La valeur de champ que vous avez sélectionnée à l'étape 3 est utilisée comme filtre.
Ce tableau de bord	La valeur de champ que vous avez sélectionnée à l'étape 3 est utilisée comme filtre sur le même tableau de bord.
Autre tableau de bord	La valeur de champ que vous avez sélectionnée à l'étape 3 est utilisée comme filtre sur un autre tableau de bord qui contient le champ.

Utilisation des packs de contenu

Les packs de contenu contiennent des tableaux de bord, des champs extraits, des requêtes enregistrées et des alertes qui sont associés à un produit spécifique ou à un ensemble de journaux.

Pour afficher les packs de contenu qui sont chargés sur votre système, sélectionnez **Packs de contenu** dans le menu déroulant situé dans le coin supérieur droit de l'interface utilisateur de vRealize Log Insight.

Pour voir le contenu d'un pack de contenu, cliquez sur le pack de contenu dans la liste à gauche.

Packs de contenu

La catégorie Packs de contenu contient des ensembles importés de tableaux de bord, de champs extraits, de requêtes et d'alertes. Les packs de contenu Général et VMware - vSphere sont importés par défaut.

Remarque Les tableaux de bord du pack de contenu sont en lecture seule. Vous ne pouvez ni les supprimer ni les renommer. Toutefois, vous pouvez cloner les tableaux de bord du pack de contenu dans votre tableau de bord personnalisé. Vous pouvez cloner les tableaux de bord entiers ou les widgets séparés.

Contenu personnalisé

La catégorie Contenu personnalisé contient des tableaux de bord, des champs extraits et des requêtes créés dans l'instance actuelle de vRealize Log Insight. La section Mon contenu contient le contenu personnalisé de l'utilisateur actuellement connecté. La section Contenu partagé contient le contenu qui est partagé entre tous les utilisateurs de vRealize Log Insight.

Seuls les utilisateurs Admin peuvent partager du contenu avec d'autres utilisateurs. Seuls les utilisateurs Admin peuvent gérer du contenu partagé.

Remarque Vous ne pouvez pas désinstaller du contenu de la section Contenu personnalisé. Si vous souhaitez supprimer des informations enregistrées de la section Contenu personnalisé, vous devez supprimer des éléments individuels, tels que des tableaux de bord, des requêtes, des alertes et des champs.

Installer un pack de contenu à partir du lieu de vente du module de contenu

Vous pouvez installer des packs de contenu à partir du lieu de vente du module de contenu sans quitter l'interface utilisateur de vRealize Log Insight.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight en tant qu'utilisateur disposant de l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host`, où *log-insight-host* est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Cliquez sur **Marketplace** sous **Marketplace du pack de contenu** à gauche.
- 3 Cliquez sur le pack de contenu que vous souhaitez installer.
- 4 Cochez cette case pour accepter les termes des contrats de licence.
- 5 Cliquez sur **Installer**.

Lorsque l'installation est terminée, le pack de contenu s'affiche dans la liste des Packs de contenu installés située à gauche.

Mettre à jour un pack de contenu installé à partir du lieu de vente du module de contenu

Vous pouvez mettre à jour les packs de contenu déjà installés à partir du Marketplace du pack de contenu sans quitter vRealize Log Insight.

Remarque Lorsque les alertes des packs de contenu sont activées, elles sont copiées vers le profil d'un utilisateur. Les utilisateurs peuvent modifier la description ou les conditions de la copie. À partir des définitions d'alerte instanciées dans la version 4.0, la mise à jour d'un pack de contenu et, par extension, de ses définitions d'alerte, actualise ou supprime les copies afin qu'elles correspondent au pack de contenu amélioré. Si vous voulez conserver les modifications utilisateur, exportez-les d'abord dans un pack de contenu, puis réimportez-les dans le profil d'utilisateur après la mise à jour.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight en tant qu'utilisateur disposant de l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host`, où `log-insight-host` est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Dans le menu de gauche, sélectionnez **Mises à jour** pour voir une liste de packs de contenu pour lesquels des mises à jour sont disponibles.
 - Pour mettre à jour un seul pack de contenu, cliquez sur son icône afin d'ouvrir une fenêtre d'information. Cliquez sur **Mettre à jour** pour commencer l'importation. En fonction du pack de contenu, une fenêtre contextuelle avec des instructions supplémentaires peut s'afficher après l'importation. Si elle s'affiche, suivez les étapes de configuration pour terminer la mise à niveau correctement.
 - Pour mettre à jour en silence tous les packs de contenu avec des mises à jour en attente, cliquez sur **Tout mettre à jour**. Lisez les instructions dans la fenêtre contextuelle d'information et cliquez sur **Mettre à jour** pour continuer. Après la mise à niveau, cliquez sur chaque pack de contenu afin de voir les étapes de configuration pour terminer l'importation correctement. Si vous avez exporté un pack de contenu afin de conserver les modifications utilisateur, réimportez-le dans le profil d'utilisateur.

Le pack de contenu mis à jour apparaît dans la liste des packs de contenu installés, sur la gauche.

Importer un pack de contenu

Vous pouvez importer des packs de contenu pour échanger des informations définies par l'utilisateur avec d'autres instances de vRealize Log Insight ou pour mettre à niveau vos packs de contenu anciens vers des versions plus récentes.

Vous pouvez importer uniquement des fichiers de pack de contenu vRealize vRealize Log Insight (VLCP).

Remarque Si vous importez une nouvelle version d'un pack de contenu qui existe déjà et si la nouvelle version contient des définitions de champs modifiées, l'ensemble des diagrammes, des requêtes et des alertes utilisant le champ modifié est mis à jour pour tenir compte de la nouvelle définition. Si des champs qui existent dans la version actuelle du pack de contenu sont manquants dans la nouvelle version que vous importez, vRealize Log Insight crée des copies temporaires de ces champs pour chaque requête, diagramme ou alerte qui utilise un champ supprimé.

Prérequis

- Si vous souhaitez utiliser Installer en tant que pack de contenu comme méthode d'importation, vérifiez que vous êtes connecté à l'interface utilisateur Web vRealize Log Insight en tant qu'utilisateur avec l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host`, où `log-insight-host` est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.
- Si vous souhaitez utiliser Importer dans mon contenu, vous pouvez vous connecter à l'interface utilisateur Web vRealize Log Insight avec n'importe quel niveau d'autorisation.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Dans l'angle inférieur gauche, cliquez sur **Importer un pack de contenu**.
- 3 Sélectionnez la méthode d'importation.

Option	Description
Installer en tant que pack de contenu	<p>Le contenu est importé en tant que pack de contenu en lecture seule, visible par tous les utilisateurs de l'instance de vRealize Log Insight.</p> <p>Remarque Les tableaux de bord du pack de contenu sont en lecture seule. Vous ne pouvez ni les supprimer ni les renommer. Toutefois, vous pouvez cloner les tableaux de bord du pack de contenu dans votre tableau de bord personnalisé. Vous pouvez cloner les tableaux de bord entiers ou les widgets séparés.</p>
Importer dans Mon contenu	<p>Le contenu est importé en tant que contenu personnalisé dans votre espace utilisateur et il n'est visible que par vous. Vous pouvez modifier le contenu importé sans le cloner.</p> <p>Remarque Les métadonnées des packs de contenu, telles que le nom, l'auteur, l'icône, etc., ne sont pas affichées dans ce mode.</p> <p>Une fois importé dans Mon contenu, le pack de contenu ne peut pas être désinstallé en tant que pack. Si vous souhaitez supprimer un pack de contenu de Mon contenu, vous devez supprimer individuellement chacun de ses éléments, tels que des tableaux de bord, des requêtes, des alertes et des champs.</p>

Les utilisateurs normaux peuvent importer des packs de contenu uniquement dans leur propre espace utilisateur.

- 4 Accédez au pack de contenu que vous souhaitez importer et cliquez sur **Ouvrir**.

5 Cliquez sur **Importer**.

Si vous avez sélectionné l'option d'importation en tant que contenu personnalisé, une boîte de dialogue s'affiche pour vous permettre de sélectionner le contenu à importer.

6 (Facultatif) Si vous avez sélectionné l'option d'importation en tant que contenu personnalisé, utilisez les cases à cocher pour sélectionner les éléments à importer, puis cliquez de nouveau sur **Importer**.

Remarque Les champs utilisés dans les requêtes, les diagrammes et les alertes importés sont également importés.

7 (Facultatif) Pour certains packs de contenu, si vous importez le pack de contenu pour la première fois, une fenêtre contextuelle contenant des instructions de configuration s'affiche lorsque l'importation est terminée. Suivez ces instructions pour terminer la configuration du pack de contenu.

8 (Facultatif) Pour certains packs de contenu, si vous importez le pack de contenu pour une mise à niveau, une fenêtre contextuelle contenant des instructions de mise à niveau s'affiche lorsque l'importation est terminée. Suivez ces instructions pour terminer la configuration du pack de contenu.

Le pack de contenu importé est prêt à être utilisé et apparaît dans la liste Packs de contenu ou Contenu personnalisé sur la gauche.

Remarque Les alertes importées sont désactivées par défaut. Reportez-vous à [Activer des requêtes d'alerte](#).

Exporter un pack de contenu


Vous pouvez exporter vos tableaux de bord personnalisés, requêtes enregistrées, alertes et champs extraits en tant que pack de contenu, pour partager du contenu entre des instances de vRealize Log Insight ou avec des utilisateurs de vRealize Log Insight sur la communauté.

Les packs de contenu sont enregistrés dans des fichiers vCenter vRealize Log Insight Content Pack (VLCP).

Tous les champs qui sont utilisés dans des requêtes, des graphiques et des alertes que vous exportez sont inclus dans le pack de contenu exporté.

Si vous exportez du contenu contenant des champs temporaires, vRealize Log Insight crée ces champs dans le pack de contenu pendant l'exportation.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Cliquez sur le pack de contenu que vous souhaitez exporter et sélectionnez **Exporter** dans le menu déroulant  à côté du nom du pack de contenu.

- 3 (Facultatif) Sélectionnez le contenu que vous souhaitez inclure dans le pack de contenu.

Remarque Vous ne pouvez pas désélectionner les champs qui sont utilisés dans les tableaux de bord, les requêtes ou les alertes sélectionnées pour l'exportation.

- 4 Dans les champs de texte à droite, remplissez les métadonnées pour votre pack de contenu.

Option	Description
Nom	Le nom s'affiche lorsque vous importez le pack dans une instance de vRealize Log Insight. Le nom du fichier de pack de contenu est dérivé de la zone de texte Nom . Le format recommandé est <i>Fournisseur - Produit</i> Par exemple, VMware - vSphere.
Version	Si vous prévoyez de mettre à niveau ce pack de contenu, tapez une version. vRealize Log Insight affiche la version lorsque vous essayez d'installer un pack de contenu qui existe déjà dans la liste des packs de contenu.
Espace de noms	L'espace de noms est un identifiant unique pour le pack de contenu. Utilisez l'affectation de nom DNS inverse, par exemple com.companyname.contentpackname .
Author	Vous pouvez aussi taper votre nom ou le nom de votre société.
Site Web	Vous pouvez éventuellement indiquer un lien vers le site Web associé au pack de contenu. Tous les utilisateurs qui peuvent voir le pack de contenu peuvent également voir le lien du site Web.
Description	Vous pouvez également fournir des informations sur le contenu et l'objectif du pack.
Icône	Vous pouvez éventuellement rechercher une icône à afficher à côté du nom du pack de contenu. Remarque Le format du fichier de l'icône doit être PNG ou JPG et sera réduit à une taille de 144 par 144 pixels.

Remarque Ces données ne sont visibles que si vous importez le pack de contenu en utilisant l'option **Installer comme pack de contenu**. Vous ne pouvez pas voir ces informations si vous choisissez d'importer le pack de contenu en tant que contenu personnalisé.

- 5 Cliquez sur **Exporter**, accédez à l'emplacement d'enregistrement du fichier et cliquez sur **Enregistrer**.

Le fichier VLCP exporté est téléchargé vers l'emplacement sélectionné.

Afficher des détails sur des éléments de pack de contenu

Vous pouvez ouvrir les requêtes qui constituent les tableaux de bord ou ouvrir les définitions de champs, de requêtes et d'alertes, directement à partir de la vue Packs de contenu.

Vous pouvez souhaiter utiliser les définitions des éléments d'un pack de contenu comme modèles pour vos définitions personnalisées.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Sélectionnez le pack de contenu qui contient l'élément que vous souhaitez réviser.
- 3 Cliquez sur le bouton correspondant au type d'élément que vous souhaitez réviser.
Par exemple, cliquez sur **Alertes** pour voir toutes les alertes que le pack de contenu contient.
- 4 Dans la liste d'éléments, cliquez sur le nom de l'élément que vous souhaitez réviser.

La page **Analyse interactive** s'ouvre et affiche la requête correspondant à l'élément sélectionné.

Suivant

Vous pouvez modifier la requête ou la définition de l'élément du pack de contenu, et l'enregistrer dans votre contenu personnalisé.

Désinstaller un pack de contenu

Vous pouvez désinstaller des packs de contenu. Désinstaller des packs de contenu supprime les tableaux de bord personnalisés, les requêtes enregistrées, les alertes et les champs extraits.


Les packs de contenu sont enregistrés dans des fichiers vCenter vRealize Log Insight Content Pack (VLCP).

Lorsque vous désinstallez un pack de contenu, celui-ci devient définitivement indisponible pour tous les utilisateurs. Créez tout d'abord une copie de sauvegarde en exportant le pack de contenu en tant que fichier VLCP. Reportez-vous à [Exporter un pack de contenu](#).

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight en tant qu'utilisateur disposant de l'autorisation **Modifier le compte Admin**. Le format de l'URL est `https://log-insight-host`, où *log-insight-host* est l'adresse IP ou le nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Dans le menu déroulant dans le coin supérieur droit, sélectionnez **Packs de contenu**.
- 2 Cliquez sur le pack de contenu que vous souhaitez désinstaller et sélectionnez **Désinstaller** dans le menu déroulant  à côté du nom du pack de contenu.
- 3 Cliquez sur **Désinstaller**.

Le pack de contenu est supprimé de la liste des packs de contenu installés.

Création de packs de contenu

Tout utilisateur de Log Insight peut créer un pack de contenu pour un usage privé ou public.

Les packs de contenu sont des plug-ins en lecture seule de vRealize Log Insight qui fournissent des connaissances prédéfinies sur des types d'événements spécifiques, par exemple des messages de journaux. Un pack de contenu a pour objet de fournir des connaissances sur un ensemble spécifique d'événements dans un format facilement compréhensible par les administrateurs, les ingénieurs, les équipes de surveillance et la direction de l'entreprise.

Les packs de contenu fournissent des informations sur l'état de santé d'un produit ou d'une application. En outre, un pack de contenu vous permet de mieux comprendre le fonctionnement d'un produit ou d'une application.

Vous pouvez enregistrer les informations d'un pack de contenu en utilisant les pages Tableaux de bord ou Analyse interactive de vRealize Log Insight. Les informations d'un pack de contenu incluent notamment les éléments suivants :

- Requêtes : un pack de contenu contient généralement au moins trois requêtes et trois widgets de diagramme pour chaque tableau de bord, ce qui donne plus de neuf requêtes au total
- Champs : un pack de contenu doit comporter au moins vingt champs extraits
- Agrégations
- Alertes : chaque pack de contenu contient au moins cinq alertes
- Tableaux de bord : chaque pack de contenu comporte au moins trois tableaux de bord
- Filtres de tableau de bord - reportez-vous à [Recherche et filtrage d'événements de journaux](#)
- Visualisations - reportez-vous à [Utilisation du diagramme Analyse interactive pour analyser des journaux](#)

Par défaut, vRealize Log Insight est livré avec le pack de contenu VMware - vSphere. Vous pouvez importer des packs de contenu supplémentaires si nécessaire.

Termes des packs de contenu

Le workflow de création de packs de contenu repose sur plusieurs termes et concepts. Vous devez vous familiariser avec ceux-ci pour créer et maintenir efficacement les packs de contenu.

Instance

Seuls les administrateurs de vRealize Log Insight peuvent importer un fichier de pack de contenu sous la forme d'un pack de contenu. Si un pack de contenu est importé sous la forme d'un pack de contenu, il ne peut pas être modifié.

Tous les utilisateurs peuvent importer un fichier de pack de contenu dans un espace utilisateur. Si vous importez un fichier de pack de contenu dans un espace utilisateur, l'opération importe sélectivement les objets sous Mon contenu. Lorsque vous importez un pack de contenu dans un espace utilisateur, vous pouvez modifier les packs de contenu dans une instance de vRealize Log Insight. Si vous souhaitez publier ou modifier un pack de contenu, vous avez besoin d'un pack de contenu exporté.

Utilisateur

Les packs de contenu sont en partie créés à partir du contenu enregistré sous Tableaux de bord personnalisés, également nommé espace utilisateur, ou plus spécifiquement Mes tableaux de bord ou Tableaux de bord partagés dans la page Tableaux de bord. Bien que les objets d'un tableau de bord personnalisé puissent être exportés sélectivement, il est recommandé que chaque pack de contenu individuel soit créé par une entité utilisateur distincte dans vRealize Log Insight pour garantir un espace utilisateur propre pour chaque pack de contenu.

Pour plus d'informations sur la création d'utilisateurs dans vRealize Log Insight, reportez-vous au *Guide d'administration de VMware vRealize Log Insight*.

Employez un utilisateur auteur de pack de contenu distinct dans vRealize Log Insight pour chaque pack de contenu que vous créez.

Événements

Il est essentiel de collecter des événements pertinents avant de tenter de créer un pack de contenu afin de s'assurer qu'un pack de contenu couvre tous les événements pertinents d'un produit ou d'une application. Pour collecter des événements pertinents, il convient de s'adresser aux équipes d'assurance qualité et de support, car celles-ci ont généralement accès aux événements courants et les connaissent bien.

Les tentatives de génération d'événements pendant la création d'un pack de contenu entraînent une perte de temps et risquent d'ignorer des événements importants. Si les équipes de contrôle qualité et de support ne peuvent pas fournir d'événements, vous pouvez les simuler et les utiliser à la place si des événements de produits ou d'applications sont connus et documentés.

Une fois que vous avez collecté les journaux appropriés, ils doivent être ingérés dans vRealize Log Insight.

Auteurs

Les auteurs d'un pack de contenu doivent avoir les qualifications suivantes :

- Expérience d'utilisation de VMware vRealize Log Insight.
- Connaissances pratiques et concrètes d'utilisation du produit ou de l'application.
- Capacité de générer des expressions régulières optimisées.
- Expérience de débogage de problèmes multiples dans des produits ou des applications à l'aide de journaux.
- Antécédents de support impliquant la résolution d'une multitude de problèmes.
- Antécédents d'administrateur système avec une expérience de syslog.

Workflow

L'approche recommandée pour la création de packs de contenu consiste à ouvrir la page Analyse interactive et à effectuer des requêtes sur des types spécifiques d'événements comme des erreurs ou des avertissements. Examinez les résultats des requêtes, puis analysez et extrayez les champs qui vous semblent appropriés. Une fois que vous connaissez les différents types d'événements et les informations utiles qu'ils contiennent, construisez et enregistrez des requêtes pertinentes adaptées. Pour les requêtes qui mettent en évidence un problème nécessitant une intervention rapide, créez et enregistrez des alertes. Lors de l'enregistrement de requêtes, supprimez-les de la liste de résultats en utilisant un filtre pour identifier d'autres événements pouvant constituer d'éventuels candidats à l'enregistrement de nouvelles requêtes. Une fois que vous avez enregistré toutes les requêtes pertinentes, organisez-les et affichez-les d'une manière logique dans la page Tableaux de bord.

Requêtes

Les requêtes dans vRealize Log Insight peuvent récupérer et résumer des événements.

Vous pouvez créer et enregistrer des requêtes à partir de la page Analyse interactive. Une requête est composée d'un ou plusieurs des éléments suivants :

Mots clés	Correspondances alphanumériques, de traits d'union et/ou de tirets de soulignement complètes ou en texte intégral.
Caractères génériques	Correspondances alphanumériques, de traits d'union et/ou de tirets de soulignement complètes ou en texte intégral.
Expressions régulières	Correspondance de modèles de chaînes sophistiqués basée sur des expressions régulières Java.
Opérations sur des champs	Correspondances de mots clés, d'expressions régulières et de modèles appliquées à des champs extraits.
Agrégations	Fonctions appliquées à un ou plusieurs sous-groupes des résultats.

vRealize Log Insight prend en charge les types de requêtes suivants :

- Message. Requête composée de mots clés, d'expressions régulières et/ou d'opérations de champ.
- Expression régulière ou champ. Requête composée de mots clés et/ou d'expressions régulières.
- Agrégation. Requête composée d'une fonction, d'un ou plusieurs regroupements et d'un nombre quelconque de champs.

Vous pouvez définir des alertes personnalisées dans vRealize Log Insight et les déclencher à partir de requêtes planifiées de n'importe quel type.

Recommandations liées à la création de requêtes de message

Concepts de base pour la création de requêtes de message.

Vous pouvez entrer des requêtes de message à l'aide de la barre de recherche ou en entrant des filtres.

Utilisez la barre de recherche pour affiner les résultats des événements dans une instance vRealize Log Insight. Bien que vous puissiez utiliser un filtre à la place de la barre de recherche, il est souvent plus facile de comprendre une requête qui utilise la barre de recherche qu'un filtre équivalent. Il convient d'utiliser la barre de recherche plutôt qu'un filtre équivalent lorsque cela est possible.

Un filtre permet de créer des requêtes à l'aide d'une expression régulière, d'un champ, d'une opération logique OU, ou d'une combinaison de requêtes à barre de recherche et à filtres.

Lorsque vous créez des requêtes en utilisant la barre de recherche et des filtres, les recommandations suivantes s'appliquent :

- Assurez-vous que les requêtes ne sont pas spécifiques de l'environnement. Les packs de contenu publics doivent être génériques et applicables à tout environnement et ne reposent donc pas sur des informations propres à l'environnement. Exemples d'informations spécifiques de l'environnement : source, nom d'hôte et éventuellement installation si l'installation utilise *local*.*.
- Lors de la construction d'une requête, utilisez si possible des mots clés, lorsque les mots clés ne suffisent pas, utilisez des caractères génériques et lorsque les caractères génériques ne suffisent pas, utilisez des expressions régulières. Les requêtes à mots clés constituent les requêtes les moins gourmandes en ressources. Les caractères génériques représentent une version simplifiée de l'expression régulière et constituent le deuxième type de requête le moins gourmand en ressources. Les expressions régulières sont les plus gourmandes en ressources.
- Fournissez autant de mots clés que possible lors de l'utilisation d'expressions régulières ou de champs. Si une expression régulière inclut un opérateur logique OU, par exemple *cecil|ce/a*, n'incluez pas de mots clés. vRealize Log Insight est optimisé pour effectuer des requêtes à mots clés avant d'utiliser des expressions régulières afin de minimiser la charge des expressions régulières.

Requêtes de champs

Les champs constituent une méthode puissante pour ajouter une structure à des événements non structurés et permettent la manipulation de représentations textuelles et visuelles des données.

Les champs constituent l'un des éléments les plus importants d'un pack de contenu, car ils peuvent être utilisés de différentes manières, notamment dans des agrégations et des filtres. Les agrégations vous permettent d'appliquer des fonctions et des regroupements à des champs. Les filtres permettent d'effectuer des opérations sur des champs.

Vous devez extraire une partie d'un message de journal qui peut être applicable à une requête ou une agrégation. Les champs sont un type de requête à expression régulière et sont utiles pour la mise en correspondance de modèles complexes, ils vous permettent d'éviter de devoir connaître, mémoriser ou apprendre des expressions régulières compliquées.

Valeur contextuelle du champ	Définition
Expression rationnelle avant la valeur	Incluez autant de mots clés que possible. Si ce champ est vide ou ne contient que des caractères spéciaux, l'expression rationnelle après la valeur doit inclure des mots clés.
Expression rationnelle après la valeur	Incluez autant de mots clés que possible. Si ce champ est vide ou ne contient que des caractères spéciaux, l'expression rationnelle avant la valeur doit inclure des mots clés.

Valeur contextuelle du champ	Définition
Nom	Utilisez uniquement des caractères alphanumériques. Vérifiez que tous les caractères sont minuscules et utilisez des tirets de soulignement plutôt que des espaces, car cela améliore la visibilité des champs. Gardez à l'esprit que les noms des champs de pack de contenu et des champs d'utilisateur peuvent être les mêmes, bien qu'un espace de noms sera indiqué entre parenthèses à droite des noms de champs de pack de contenu. Utilisez un préfixe à abréviation devant les champs de pack de contenu, par exemple vmw_, pour éviter toute confusion.
Termes de la recherche par mot-clé	Un ou plusieurs mots-clés, séparés par des espaces, qui s'affichent à l'intérieur des événements contenant le champ.
Filtre	Un champ statique, opérateur, et une valeur potentielle qui s'affichent à l'intérieur des événements contenant le champ. Il est courant d'utiliser ceci conjointement avec l'agent vRealize Log Insight et les balises des événements qui ne contiennent pas de mots-clés.
Informations (bouton « i »)	Utilisé pour fournir des informations sur le champ y compris sa signification, quelles valeurs potentielles pourraient être renvoyées et éventuellement un mappage convivial des valeurs avec les informations compréhensibles par l'être humain.

Meilleures pratiques

Outre les divers composants qui constituent un champ, plusieurs recommandations s'appliquent.

- Créez des champs uniquement pour des modèles d'expression régulières. Si un champ peut faire l'objet de requêtes à mots clés, ou ne pourra renvoyer qu'une valeur unique, utilisez des requêtes à mots clés plutôt qu'un champ prédéfini. Si un champ renverra uniquement deux valeurs, envisagez de construire des requêtes individuelles plutôt que d'extraire un champ. Les champs servent à ajouter de la structure à des données non structurées et à permettre d'effectuer une requête sur des parties spécifiques d'un événement.
- Créez uniquement des champs pour des modèles d'expression régulière qui renvoient une partie de l'ensemble des événements. Les champs qui correspondront à la plupart des événements et/ou renverront un très grand nombre de résultats ne conviennent pas à l'extraction de champ. L'expression régulière devra être appliquée à grand nombre d'événements, ce qui entraînera une opération gourmande en ressources. Si possible, ajoutez des mots clés pour réduire le nombre de résultats renvoyés et optimiser la requête.
- Si un champ contient des mots clés dans une syntaxe d'expression régulière, ajoutez de tels mots clés en tant que filtre sans syntaxe d'expression régulière. Par exemple, si la valeur ou le contexte d'un champ contient des mots clés dans une syntaxe d'expression régulière, par exemple *ceci|cela*, ajoutez les mots-clés sous forme de filtre textuel pour optimiser la requête comme dans **texte contient ceci, cela**.
- L'utilisation du contexte supplémentaire avec un ou plusieurs mots-clés est recommandée pour des expressions régulières complexes dans le contexte avant ou après.
- Ajoutez le contexte supplémentaire à tous les champs extraits afin d'optimiser la performance des requêtes.

Champs temporaires

Un champ temporaire fait partie d'une requête mais n'est pas enregistré globalement dans une instance de vRealize Log Insight ou comme partie intégrante d'un pack de contenu installé.

vRealize Log Insight réduit les risques de créer un champ temporaire en actualisant automatiquement la requête qui repose sur un champ modifié.

Remarque Si vous supprimez un champ dont dépend une requête enregistrée, la requête enregistrée contient un champ temporaire.

Vous pouvez voir les champs temporaires lorsque vous exécutez une requête enregistrée dans la page Analyse interactive et l'espace de noms Temporary figure à droite du nom d'un champ utilisé dans la requête enregistrée.

Les requêtes doivent contenir un ou plusieurs champs. Pour les requêtes enregistrées dans vRealize Log Insight, la définition de champ utilisée lors de l'enregistrement d'une requête sera modifiée si le champ est modifié. Les modifications de champ incluent notamment les éléments suivants

- Modification de la valeur du champ
- Modification de l'expression rationnelle avant la valeur et de l'expression rationnelle après la valeur du champ
- Modification du nom du champ
- Suppression du champ

Lorsque vous exportez un pack de contenu, vRealize Log Insight convertit tous les champs temporaires en champs de pack de contenu. Si vous voyez un champ temporaire dans un pack de contenu, vous avez peut-être ouvert un pack de contenu d'une version de produit précédente qui est exportée avec des champs temporaires ou le pack de contenu est modifié manuellement.

Si un champ temporaire existe avec le même nom qu'un champ extrait existant, il s'affiche en terminant par {n}. Par exemple, si un champ est appelé product_test_field, product_test_field {2} pourrait être également visible lors de l'exportation. Si vous observez ce comportement, un champ temporaire existe. Pour résoudre ce problème, choisissez l'option **Tout désélectionner** au bas de la boîte de dialogue d'exportation et sélectionnez chaque tableau de bord ou alerte jusqu'à ce que le ou les champs à extraire avec la terminaison {n} soient cochés. Allez dans ces tableaux de bord ou alertes et modifiez chaque requête. Lorsque vous trouvez une requête utilisant le champ extrait, modifiez le filtre ou l'agrégation pour utiliser le champ sans la terminaison {n}, exécutez la requête puis enregistrez-la. Après avoir terminé ces étapes pour toutes les requêtes utilisant un champ se terminant par {n}, celui-ci ne s'affiche plus lors de l'exportation.

Requêtes d'agrégation

vRealize Log Insight vous permet de manipuler la représentation visuelle d'événements à l'aide de requêtes d'agrégation.

Les requêtes d'agrégation comportent les deux attributs suivants :

- Fonctions

■ Regroupements

Une requête d'agrégation nécessite une fonction et au moins un regroupement. Les regroupements constituent une partie importante des packs de contenu. Les fonctions et les regroupements ont une incidence sur le mode d'affichage des diagrammes.

Les affichages de diagramme sont limités aux 2 000 résultats les plus récents.

Diagrammes à barres

Par défaut, le diagramme d'aperçu dans la page Analyse interactive de vRealize Log Insight affiche un nombre d'événements dans le temps. Si vous utilisez la fonction nombre avec le regroupement de séries chronologiques, vRealize Log Insight crée un diagramme à barres.

Si vous utilisez la fonction nombre avec un regroupement de champ unique à la place d'un regroupement de séries chronologiques, vRealize Log Insight crée des diagrammes à barres dont les quantités sont répertoriées de la plus élevée à la plus faible.

Diagrammes linéaires

Toutes les fonctions, à l'exception de la fonction nombre, sont mathématiques. Elles nécessitent un champ sur lequel vous appliquez l'équation. Lors de l'exécution d'une fonction mathématique sur un champ et un regroupement par séries chronologiques, vRealize Log Insight crée un diagramme linéaire.

Diagrammes empilés

Par défaut, le diagramme d'aperçu dans la page Analyse interactive de vRealize Log Insight affiche un nombre d'événements dans le temps. Si vous ajoutez un champ au regroupement de séries chronologiques, vRealize Log Insight crée un diagramme empilé.

Si vous utilisez un regroupement par séries chronologiques, plus un champ, et si vous utilisez n'importe quelle fonction à l'exception de nombre, vRealize Log Insight crée un diagramme linéaire empilé. Les diagrammes empilés sont très utiles lorsqu'il s'agit de rechercher des anomalies sur un objet.

Vous devez décider du type de diagramme empilé à utiliser, en fonction du nombre d'objets que la requête d'agrégation peut renvoyer. L'affichage d'un plus grand nombre d'objets nécessite des ressources supplémentaires pour analyser et afficher les informations. En outre, le nombre de couleurs est fixe et la distinction entre les objets peut devenir difficile selon le nombre d'objets renvoyés. En général, les recommandations suivantes s'appliquent

- Si le nombre d'objets renvoyés dans chaque barre est inférieur à dix, il est probablement préférable d'utiliser des diagrammes empilés.
- Si le nombre d'objets renvoyés dans chaque barre est compris entre dix et vingt, les diagrammes empilés peuvent convenir. Vous devez déterminer la manière de représenter visuellement les diagrammes dans un pack de contenu.
- Si le nombre d'objets renvoyés dans chaque barre est ou peut être supérieur à vingt, il convient d'éviter les diagrammes empilés.

Diagrammes multicolores

Si vous créez un regroupement en utilisant plusieurs champs et des séries chronologiques, vRealize Log Insight crée un diagramme multicolore. Le diagramme comporte deux couleurs en alternance. Chaque changement de couleur marque un nouvel intervalle de temps. Dans la mesure où les diagrammes multicolores peuvent être difficiles à interpréter, il convient d'en tenir compte lors du choix de la valeur d'un tel diagramme avant de l'inclure dans un pack de contenu.

Lorsque que vous effectuez un regroupement par plusieurs champs, envisagez l'utilisation de séries non chronologiques. La suppression des séries chronologiques simplifie l'interprétation du diagramme à barres.

Si plusieurs champs sont importants dans un intervalle de temps donné, vous pouvez créer plusieurs diagrammes pour chaque champ individuellement sur l'intervalle de temps. Vous pouvez alors afficher les diagrammes dans la même colonne qu'un groupe de tableaux de bord d'un pack de contenu.

Autres diagrammes

Plusieurs autres types de diagrammes sont disponibles, notamment des diagrammes à secteurs, à bulles et comparatif. Pour utiliser ces diagrammes, un type de requête spécifique est requis. Si l'option de ces diagrammes est disponible, vous possédez déjà la requête appropriée. Si cette option n'est pas disponible, survolez le nom du diagramme à utiliser. Un message contextuel décrit le type de requête requis pour le type de diagramme.

Requêtes de message

Lors de la construction d'une requête d'agrégation, la requête de message doit uniquement renvoyer les résultats pertinents pour la requête d'agrégation. Cela simplifie l'analyse et garantit que seuls les résultats pertinents s'affichent dans les champs. Pour garantir que la requête de message renvoie les mêmes résultats que la requête d'agrégation, vous devez ajouter des filtres à l'aide de l'opérateur *existe* pour chaque champ qui est utilisé dans la requête d'agrégation.

Modification du type de diagramme

Pour modifier le type de diagramme d'un widget sur un tableau de bord, cliquez sur l'icône roue dentée du widget et sélectionnez **Modifier le type de diagramme**. Pour modifier un type de widget, enregistrez un nouveau widget et supprimez l'ancien.

Alertes

Les alertes offrent un moyen de déclencher une réaction lorsqu'un certain type d'événement se produit.

vRealize Log Insight prend en charge deux types d'alertes

- E-mail
- vRealize Operations Manager

Vous pouvez enregistrer des alertes uniquement dans un espace utilisateur. Par défaut, toutes les alertes de pack de contenu sont désactivées. Si vous créez une alerte activée et l'exportez en tant que partie intégrante d'un pack de contenu, l'alerte sera désactivée dans ce pack de contenu.

Les packs de contenu ne contiennent pas de paramètres d'e-mail et de vRealize Operations Manager. Vous ne pouvez pas ajouter ces paramètres à un pack de contenu.

Seuils

Les seuils définissent une limite pour le nombre d'alertes déclenchées.

Il est important de comprendre le fonctionnement des seuils pour vous assurer que, si elle est activée, une alerte de pack ne spamme pas involontairement un utilisateur. Lorsque vous envisagez d'utiliser un seuil, vous devez vous poser deux questions.

- À quelle fréquence faut-il déclencher l'alerte ? Log Insight utilise des fréquences prédéfinies. Les alertes ne se déclencheront qu'une seule fois pour une fenêtre de seuil donnée.
- À quelle fréquence un état d'alerte est-il contrôlé ? Une alerte est déclenchée par une requête. Les alertes, tout comme les requêtes, ne sont pas gérées en temps réel dans la version actuelle. Pour chaque fenêtre de seuil, une fréquence de requêtes prédéterminée est allouée. La modification du seuil modifie l'heure de la requête.

Regroupements

Lorsque vous créez une alerte par e-mail, il est important de grouper selon un champ qui identifie la source de l'alerte.

L'e-mail envoyé par l'alerte contient un tableau des résultats pour une requête d'agrégation particulière. La page Analyse interactive affiche une représentation visuelle de la requête.

En l'absence d'un identifiant unique sur la base duquel effectuer le regroupement, vous ne pouvez pas savoir si le résultat obtenu est pertinent pour un ou plusieurs systèmes de votre environnement. Vous devez baser le regroupement sur le champ de nom d'hôte, par sur le champ de source. Vous pouvez également ajouter tout champ permettant de déterminer l'origine unique de l'événement.

Recommandations concernant les tableaux de bord

Les tableaux de bord font partie des packs de contenu. Certaines recommandations s'appliquent lors de la création de tableaux de bord.

Lors de la création de tableaux de bord, les recommandations suivantes s'appliquent

- Les packs de contenu contiennent généralement un minimum de trois tableaux de bord. Il convient de commencer par des tableaux de bord d'aperçu pour fournir des informations de haut niveau sur les événements d'un produit ou d'une application particulière. Outre les tableaux de bord d'aperçu, des tableaux de bord doivent être créés en fonction de regroupements logiques d'événements. Les regroupements logiques sont propres aux produits ou aux applications, mais certaines approches courantes sont liées aux performances, aux erreurs et à l'audit. Il est également courant de créer des

tableaux de bord pour un composant, par exemple un disque et un contrôleur. Il convient de noter que l'approche composant n'est efficace que si les requêtes peuvent être construites de manière à envoyer les résultats à partir de composants spécifiques. Si cela est impossible, l'approche logique est recommandée.

- Lorsque vous nommez des tableaux de bord, choisissez un titre générique et évitez d'ajouter des noms spécifiques de produits ou d'applications sauf s'ils sont utilisés d'une manière propre à un composant. Par exemple, le pack de contenu VMware - vSphere contient un groupe de tableaux de bord nommé ESX/ESXi plutôt que VMware ESX/ESXi.
- Des tableaux de bord doivent contenir un minimum de trois widgets de tableau de bord et un maximum de six widgets de tableau de bord. Avec moins de trois widgets de tableau de bord, la quantité de connaissances pouvant être obtenue par les tableaux de bord est minimale. En outre, s'il dispose de nombreux tableaux de bord et d'un nombre limité de widgets de tableau de bord, un utilisateur doit sans cesse basculer entre les différentes pages et ne bénéficie pas d'un accès cohérent aux informations.

À l'inverse, l'utilisation de plus de six widgets de tableaux de bord pour des tableaux de bord peut avoir un impact négatif. La trop grande quantité d'informations ainsi obtenue peut être déroutante. Un grand nombre de widgets entraîne une utilisation intensive de ressources système, car chaque widget est une requête exécutée sur le système.

Lorsque vous incluez plus de six widgets de tableau de bord dans des tableaux de bord, vous devez séparer les informations et créer plusieurs tableaux de bord. Si un widget de tableau de bord s'applique à un ou plusieurs tableaux de bord, créez le widget dans chaque tableau de bord applicable.

Filtres de tableau de bord

Les filtres de tableau de bord peuvent être utilisés pour explorer des événements spécifiques. Les filtres fonctionnent comme les filtres sur la page Analytique interactive et utilisent les champs à explorer. Chaque tableau de bord doit comprendre au moins un filtre de tableau de bord, généralement avec le champ de nom d'hôte, mais jusqu'à cinq champs peuvent être ajoutés à chaque tableau de bord.

Le champ ajouté doit être utilisé par la majorité des widgets dans un tableau de bord donné de sorte que si le filtre de tableau de bord est utilisé, la plupart des widgets renvoient des résultats. Les exemples de filtres de tableau de bord peuvent inclure un champ de gravité, un champ d'utilisateur voire un champ de composant.

Remarque Le champ et l'opérateur utilisés par le filtre de tableau de bord seront enregistrés dans un pack de contenu exporté. Toute valeur utilisée par un filtre de tableau de bord ne sera pas enregistrée lors de l'exportation car il est probable que la valeur soit propre à un environnement et pas générique à tous les événements.

Widgets Tableau de bord

Les widgets Tableau de bord vous aident à visualiser les informations.

Il existe plusieurs types de widgets dans vRealize Log Insight que vous pouvez ajouter à un tableau de bord. Ces widgets sont les suivants :

- Un widget Diagramme qui contient une représentation visuelle d'événements avec un lien vers une requête enregistrée.
- Un widget Liste de requêtes qui contient des liens de titres vers des requêtes enregistrées.
- Un widget Tableau de champs qui contient les événements où chaque champ représente une colonne.
- Un widget Tableau de types d'événements simplifié qui contient des événements semblables combinés dans des groupes uniques.
- Un widget Tableau de tendances des événements simplifié qui indique une liste de types d'événements trouvés dans la requête, triés par nombre d'occurrences. Il s'agit d'une méthode rapide pour voir les types d'événements qui se produisent très souvent dans une requête.

Diagramme

Un widget Diagramme de tableau de bord contient une représentation visuelle d'événements. Vous pouvez représenter un diagramme sous forme de diagramme à barres ou de diagramme linéaire, et l'afficher en mode empilé dans les deux cas.

Il y a plusieurs manières de représenter des diagrammes :

- Les diagrammes peuvent contenir beaucoup d'informations. Évitez d'inclure plus de deux widgets de diagramme sur une ligne. Dans de rares cas, trois widgets de diagramme peuvent être utilisés efficacement, mais il est fortement déconseillé d'en inclure plus de trois. Pour déterminer si des widgets de diagramme sont lisibles ou non, assurez-vous d'employer la résolution minimale prise en charge par vRealize Log Insight, à savoir 1 024 x 768 pixels.
- Si une ligne, à l'exception de la dernière, contient un seul widget de diagramme, attribuez toute la largeur de la ligne à celui-ci.
- Pour nommer un widget de diagramme, utilisez un titre descriptif et évitez les noms de champs indéchiffrables. Par exemple, un champ extrait se nomme `vmw_error_message`. Plutôt que de nommer un diagramme Nombre de `vmw_error_message`, nommez-le Nombre de messages d'erreur.
- Vous pouvez enregistrer des diagrammes similaires et les empiler dans la même colonne d'un groupe de tableaux de bord à des fins de comparaison visuelle. Par exemple :
 - Moyenne X d'événements dans le temps + Maximum X d'événements dans le temps. En raison des différentes fonctions utilisées, l'axe Y des diagrammes peut présenter une échelle différente.
 - Nombre d'événements dans le temps groupés par X + Nombre d'événements dans le temps groupés par Y.

Liste de requêtes

Un widget Liste de requêtes de tableau de bord contient un ou plusieurs liens vers des requêtes prédéfinies.

Vous pouvez utiliser des widgets Liste de requêtes pour les raisons suivantes

- Lorsqu'un widget Diagramme ne fournit pas de valeur significative, alors que la requête sous-jacente en fournit.
- Pour enregistrer des requêtes complexes comme celles utilisant des expressions régulières.
- Pour utiliser différentes agrégations sur la même requête sous-jacente dans un groupe de tableaux de bord.

Tableau de champs

Un tableau de champs qui content les événements où chaque champ représente une colonne.

Un widget de tableau de champs de tableau de bord contient les derniers événements de la requête donnée dans un format tabulaire où chaque champ représente une colonne.

Vous pouvez utiliser un widget de tableau de champ pour les raisons suivantes.

- Pour visualiser les derniers événements de la requête donnée. Ceci peut être utile pour la gestion des changements ou pour des raisons de sécurité.
- Pour ne visualiser que les champs intéressants d'une enquête donnée. Ceci peut-être utile pour limiter la sortie de l'événement.

Erreur d'importation de pack de contenu

Lorsque vous importez un pack de contenu, vous pouvez obtenir des avertissements ou des messages d'erreur.

Mise à niveau

Vous pouvez obtenir un message de mise à niveau. Cela signifie qu'un autre pack de contenu installé sur le système utilise le même espace de noms. Dans ce cas, vous pouvez mettre à niveau et remplacer le pack de contenu existant, ou annuler le processus de mise à niveau et conserver le pack de contenu existant.

Format non valide

Vous pouvez obtenir un message indiquant que le format n'est pas valide. Cela signifie que le fichier VLCP est modifié manuellement et contient des erreurs de syntaxe Les erreurs de syntaxe doivent être corrigées avant l'importation du pack de contenu.

Version plus récente

Ce type de message indique que le pack de contenu est créé et est pris en charge uniquement sur une version plus récente de Log Insight. Sur les versions du produit postérieures à Log Insight 1.5, ce type de message signifie que le fichier VLCP est modifié manuellement.

Version non reconnue

Lorsque le fichier VLCP est modifié manuellement et contient des erreurs de syntaxe, vous pouvez voir ce type de message. Vous devez corriger les erreurs de syntaxe avant de tenter d'importer le pack de contenu.

Remarque Vous ne devez pas modifier manuellement les fichiers VLCP. Il est donc difficile de localiser et de corriger des erreurs.

Exigences de publication des packs de contenu

Lorsque vous créez un pack de contenu et souhaitez le publier, assurez-vous que les packs de contenu répondent aux exigences de publication de base.

Vous devez vérifier les exigences de packs de contenu et les exigences de publication.

Exigences des packs de contenu

Les packs de contenu doivent satisfaire certaines exigences en matière de contenu, de qualité et de normes.

Les exigences de contenu incluent notamment les éléments suivants :

- Minimum de trois tableaux de bord
- Minimum de un, de préférence trois, et jusqu'à cinq filtres par tableau de bord
- Minimum de trois widgets par tableau de bord
- Maximum de six widgets par tableau de bord
- Maximum de trois widgets de tableau de bord par ligne
- Minimum de cinq alertes
- Minimum de vingt champs extraits

Les exigences de qualité pour un pack de contenu sont les suivantes

- Chaque requête comporte au moins un mot clé en texte intégral et idéalement trois mots clés ou plus
- Les requêtes ne sont pas basées sur des attributs propres à l'environnement tels que source, nom d'hôte ou *local**
- Chaque champ comporte au moins un mot clé en texte intégral et idéalement trois mots clés ou plus
- Les champs sont spécifiques des produits/applications et ne renverront pas de résultats pour les journaux d'autres produits/applications
- Chaque widget Tableau de bord doit contenir des informations/liens sur ce que le diagramme affiche et pourquoi ce contenu est important

Les normes de création de packs de contenu respectent les règles suivantes

Partie du pack de contenu	Format
Format du nom du pack de contenu	<i>Société - Produit</i>
Format d'espace de noms de pack de contenu (le pack de contenu doit être exporté avec l'espace de noms)	<i>Ext.Domaine.Produit</i>
Format de champ extrait	<i>Préfixe_Champ_Nom</i> où Préfixe est le nom ou l'abréviation de la société.

Exigences de publication

Avant de publier un pack de contenu, vérifiez qu'il répond aux exigences de publication. Utilisez l'éditeur du pack de contenu dans le Centre des développeurs pour obtenir les recommandations sur le pack de contenu et pour charger une version à examiner sur VMware.

<https://developercenter.vmware.com/web/loginsight>

Exigence de publication	Description
Format de fichier de pack de contenu	Fichier VLCP.
Événements	Événements appropriés nécessaires pour valider un pack de contenu.
Présentation	Présentation de un à deux paragraphes du pack de contenu.
Points importants	Trois points importants, montrant la valeur du pack de contenu.
Description	Description de deux à trois paragraphes du pack de contenu et sa valeur.
Spécifications techniques	Décrivez la configuration minimale requise y compris les versions et la configuration du produit et de Log Insight. En outre, indiquez toutes les instructions nécessaires pour configurer le produit à consigner dans Log Insight et remplissez le pack de contenu.
Captures d'écran	Au moins trois captures d'écran affichant le pack de contenu avec les données réelles.
Vidéo (Facultative)	Exemple de l'apport en termes de valeur du pack de contenu.
Livre blanc (Facultatif)	Comment configurer le produit ou l'application pour transférer des journaux vers vRealize Log Insight.

Envoyer un pack de contenu

Envoyez le pack de contenu que vous avez créé sur VMware Solutions Exchange.

Prérequis

- Vérifiez que votre pack de contenu répond aux [Exigences de publication des packs de contenu](#).
- Si vous n'avez pas de compte sur <http://solutionexchange.vmware.com>, cliquez sur **Register** et sélectionnez **Partner**. Remplissez le formulaire de demande d'inscription de partenaire et envoyez-le. Vous recevrez un e-mail de notification si votre demande de connexion est approuvée.

Procédure

- 1 Rendez-vous sur <http://solutionexchange.vmware.com> et cliquez sur **Log In Now** dans le coin supérieur droit de la page.
- 2 Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Log In Now**.

3 Cliquez sur **Administration**, puis choisissez **Manage Solutions** pour ajouter ou modifier une solution.

4 Cliquez sur **Add Solution** et fournissez les informations requises.

Utilisez le bouton **Save Draft** fréquemment pour éviter de perdre votre travail.

5 Cliquez sur **Submit for Approval**.

Votre solution est envoyée à l'équipe VMware Solution Exchange Alliance pour révision et approbation.

Vous recevrez un e-mail indiquant l'état d'approbation de votre solution.

Suivant

Pour plus d'informations sur le remplissage d'une liste de solutions, cliquez sur le lien **Partner Corner** en haut de la page. Si vous ne trouvez pas les informations dont vous avez besoin, contactez VSXAlliance@vmware.com pour poser vos questions.

Requêtes d'alerte dans vRealize Log Insight

Vous pouvez configurer vRealize Log Insight pour exécuter des requêtes spécifiques à des intervalles planifiés.

Si le nombre d'événements qui correspondent à la requête dépasse les seuils que vous avez définis, vRealize Log Insight peut envoyer des notifications par e-mail ou Webhook et déclencher des événements de notification dans vRealize Operations Manager.

Pour afficher la liste des alertes disponibles, accédez à la page Analyse interactive et sélectionnez **Gérer les alertes...** dans le menu déroulant **Créer et gérer des alertes...** en regard du champ **Rechercher**. L'état de chaque alerte s'affiche sous le nom de l'alerte.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

Types d'alertes que vous pouvez créer dans vRealize Log Insight

Vous pouvez contrôler les intervalles d'exécution des requêtes d'alerte et les conditions lors desquelles vRealize Log Insight envoie des notifications d'alerte en sélectionnant l'un des types d'alerte.

Alerte pour toute correspondance

La requête d'alerte s'exécute automatiquement toutes les cinq minutes. Une notification est déclenchée lorsqu'au moins un événement au cours des 5 dernières minutes correspond à la requête.

Alerte basée sur le type d'événement

La requête d'alerte s'exécute automatiquement toutes les cinq minutes. Une notification est déclenchée lorsqu'un type d'événement spécifié est vu.

Alerte basée sur un nombre d'événements dans une période personnalisée

Les intervalles de requêtes d'alerte dépendent de vos paramètres. Une notification est déclenchée conformément à vos paramètres lorsque plus ou moins de X événements correspondants se sont produits au cours des Y dernières minutes.

Si ce type d'alerte est déclenché, il est répété pendant la durée de sa période pour empêcher que des alertes dupliquées ne soient générées pour le même ensemble d'événements. Si vous souhaitez activer une alerte pendant qu'elle est répétée, vous pouvez la désactiver, puis la réactiver.

Alertes basées sur des requêtes d'agrégation

L'alerte de requête d'agrégation déclenche une notification si une valeur dans une fonction d'un regroupement dépasse une valeur définie. Vous pouvez voir cela sur un diagramme, dans lequel au moins une barre se situe au-dessus ou en dessous du seuil que vous avez défini dans la période que vous avez spécifiée.

Ce type d'alerte peut être défini pour les diagrammes qui ne détectent pas le **Nombre d'événements dans le temps**.

Alertes de pack de contenu

Les packs de contenu peuvent contenir des requêtes d'alerte. Le pack de contenu vSphere qui est inclus dans vRealize Log Insight par défaut contient plusieurs requêtes d'alerte prédéfinies. Elles peuvent déclencher des alertes si un hôte ESXi cesse d'envoyer des données syslog, si vRealize Log Insight ne peut plus collecter de données d'événements, de tâches et d'alarmes à partir d'une instance de vCenter Server, ou lorsqu'un état d'alarme passe au rouge. Vous pouvez utiliser ces requêtes d'alerte comme modèles pour créer des alertes spécifiques de votre environnement.

Toutes les alertes de pack de contenu sont désactivées par défaut.

L'activation de l'alerte **vCenter Server : ESX/ESXi a arrêté la journalisation** est recommandée, car certaines versions d'hôtes ESXi peuvent arrêter l'envoi de données syslog lorsque vous redémarrez vRealize Log Insight. Cette alerte surveille l'événement vCenter Server `esx.problem.vmsyslogd.remote.failure` pour détecter si un hôte ESXi a arrêté d'envoyer des flux syslog. Pour plus de détails sur les problèmes et solutions syslog, reportez-vous à [Un hôte VMware ESXi 5.x arrête d'envoyer des journaux syslog à un serveur distant \(2003127\)](#).

Vous pouvez ajouter le filtre suivant à la requête d'alerte et l'enregistrer sous une nouvelle alerte pour détecter uniquement les hôtes ESXi qui cessent d'envoyer des flux à votre instance de vRealize Log Insight : **vc_remote_host (VMware - vSphere) contient log-insight-hostname**.

Les requêtes d'alerte de pack de contenu sont en lecture seule. Pour enregistrer les modifications apportées à une alerte de pack de contenu, vous devez enregistrer l'alerte dans votre contenu personnalisé.

■ [Ajouter une requête d'alerte pour envoyer des notifications par e-mail](#)

Vous pouvez configurer des requêtes d'alerte dans vRealize Log Insight pour envoyer des notifications par e-mail lorsque des données spécifiques figurent dans les journaux.

- [À propos de l'utilisation de webhooks pour envoyer des alertes à des produits tiers](#)

Vous pouvez envoyer des alertes utilisateur vRealize Log Insight à des produits tiers en utilisant des webhooks.

- [Afficher des requêtes d'alerte](#)

Vous pouvez afficher les requêtes d'alerte que vous avez créées et vérifier si les notifications pour ces alertes sont activées.

- [Modifier des requêtes d'alerte](#)

Vous pouvez modifier le déclencheur de requêtes d'alerte, activer ou désactiver les notifications qu'une requête envoie, ou modifier la méthode de notification (e-mail, Webhook ou envoi à vRealize Operations Manager).

- [Activer des requêtes d'alerte](#)

Lorsqu'une requête d'alerte est désactivée, vRealize Log Insight n'envoie pas de notifications par e-mail ou Webhook et ne déclenche pas d'événements de notification vRealize Operations Manager.

- [Supprimer des requêtes d'alerte](#)

Vous pouvez supprimer des requêtes d'alerte lorsque vous n'en avez plus besoin.


Ajouter une requête d'alerte pour envoyer des notifications par e-mail

Vous pouvez configurer des requêtes d'alerte dans vRealize Log Insight pour envoyer des notifications par e-mail lorsque des données spécifiques figurent dans les journaux.

Prérequis

- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez qu'un administrateur a configuré SMTP pour activer les notifications par e-mail. Reportez-vous à [Configurer le serveur SMTP pour Log Insight](#).

Procédure

- 1 Dans l'onglet **Analyse interactive**, exécutez la requête pour laquelle vous souhaitez envoyer des notifications.
- 2 Dans le menu **Créer ou gérer des alertes** à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Créer une alerte à partir d'une requête**.
- 3 Dans la boîte de dialogue Ajouter une alerte, tapez un nom pour l'alerte et fournissez une brève description significative de l'événement qui déclenche cette alerte.

Le nom et la description de l'alerte sont inclus dans l'e-mail envoyé par vRealize Log Insight.

- 4 Cochez la case **E-mail** et tapez l'adresse e-mail à laquelle vous souhaitez que vRealize Log Insight envoie les notifications.

Utilisez des virgules pour séparer plusieurs adresses.

- 5 Définissez le seuil d'alerte.

Type d'alerte	Sélection
Toutes les correspondances	Sélectionnez l'option sur toutes les correspondances . Les requêtes s'exécutent toutes les 5 minutes.
Basée sur le type d'événement	Sélectionnez l'option Lorsqu'un nouveau type d'événement est vu . Les requêtes s'exécutent toutes les 5 minutes.
À partir du nombre d'événements sur une période donnée	Sélectionnez la troisième option et utilisez les menus déroulants pour définir les paramètres. Les requêtes s'exécutent en fonction de ce que vous avez sélectionné dans le menu déroulant.
À partir des valeurs du diagramme	Sélectionnez la quatrième option et utilisez les menus déroulants pour configurer les paramètres. Remarque Ce type d'alerte est disponible uniquement si vous avez sélectionné des événements de groupe en fonction d'au moins un champ. Vous ne pouvez pas créer ce type d'alerte pour les diagrammes n'affichant que des données selon un ordre chronologique. Les requêtes s'exécutent en fonction de ce que vous avez sélectionné dans le deuxième menu déroulant.

La ligne orange dans l'aperçu du graphique indique le seuil actuel.

- 6 Cliquez sur **Enregistrer**.

Suivant

Vous pouvez activer, désactiver ou supprimer les alertes que vous avez enregistrées.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

À propos de l'utilisation de webhooks pour envoyer des alertes à des produits tiers

Vous pouvez envoyer des alertes utilisateur vRealize Log Insight à des produits tiers en utilisant des webhooks.

vRealize Log Insight utilise des webhooks pour envoyer des alertes sur HTTP POST à d'autres applications. vRealize Log Insight envoie un webhook dans son propre format propriétaire, mais les solutions tierces attendent des webhooks entrants dans leur propre format propriétaire. Pour utiliser les informations envoyées avec des webhooks vRealize Log Insight, l'application tierce doit prendre en charge nativement le format de vRealize Log Insight ou vous devez créer un mappage entre les formats de vRealize Log Insight et le format utilisé par le produit tiers avec un shim. Le shim traduit, ou mappe, le format de vRealize Log Insight en un format différent.

Les notifications système, les alertes créées avec des requêtes de message et les alertes créées avec des requêtes agrégées disposent chacune de leur propre format webhook.

L'authentification de base HTTP est prise en charge. Incorporer des informations d'identification dans l'url en utilisant le formulaire `{{https://username:password@hostname/path}}`

Vous devez être un administrateur vRealize Log Insight pour créer des notifications système.


Ajouter une requête d'alerte pour envoyer des notifications Webhook

Vous pouvez configurer des requêtes d'alerte dans vRealize Log Insight pour envoyer des notifications Webhook à un serveur Web distant en présence de données spécifiques dans les journaux. Webhooks fournit des notifications d'événement sur HTTP POST.

Prérequis

- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez qu'un serveur Web a été configuré pour recevoir des notifications Webhook.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu **Créer ou gérer des alertes** à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Créer une alerte à partir d'une requête**.
- 3 Dans la boîte de dialogue Ajouter une alerte, tapez un nom pour l'alerte et fournissez une brève description significative de l'événement qui déclenche cette alerte.

Le nom et la description de l'alerte sont inclus dans la notification envoyée par vRealize Log Insight.
- 4 Cochez la case **Webhooks** et entrez l'URL à laquelle vous souhaitez que vRealize Log Insight envoie les notifications.
- 5 Définissez le seuil d'alerte.

Type d'alerte	Sélection
Toutes les correspondances	Sélectionnez l'option sur toutes les correspondances . Les requêtes s'exécutent toutes les 5 minutes.
Basée sur le type d'événement	Sélectionnez l'option Lorsqu'un nouveau type d'événement est vu . Les requêtes s'exécutent toutes les 5 minutes.

Type d'alerte	Sélection
À partir du nombre d'événements sur une période donnée	<p>Sélectionnez la troisième option et utilisez les menus déroulants pour définir les paramètres.</p> <p>Les requêtes s'exécutent en fonction de ce que vous avez sélectionné dans le menu déroulant.</p>
À partir des valeurs du diagramme	<p>Sélectionnez la quatrième option et utilisez les menus déroulants pour configurer les paramètres.</p> <p>Remarque Ce type d'alerte est disponible uniquement si vous avez sélectionné des événements de groupe en fonction d'au moins un champ. Vous ne pouvez pas créer ce type d'alerte pour les diagrammes n'affichant que des données selon un ordre chronologique.</p> <p>Les requêtes s'exécutent en fonction de ce que vous avez sélectionné dans le deuxième menu déroulant.</p>

La ligne orange dans l'aperçu du graphique indique le seuil actuel.

6 Cliquez sur **Enregistrer**.

Suivant

Vous pouvez activer, désactiver ou supprimer les alertes que vous avez enregistrées.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

À propos de l'écriture de shims de traduction pour les alertes de vRealize Log Insight

Les shims sont utilisés pour mapper des formats de webhook variables.

vRealize Log Insight envoie un webhook dans son propre format propriétaire, et les solutions tierces attendent des webhooks entrants dans leur propre format propriétaire. Cela signifie que la solution tierce doit prendre en charge nativement le format de vRealize Log Insight ou un shim entre vRealize Log Insight et la solution tierce est nécessaire pour traduire le format de vRealize Log Insight en format tiers.

Les figures suivantes indiquent une requête d'alerte utilisateur et le webhook qui est généré pour elle. Vous pouvez utiliser ces informations pour mieux comprendre le mappage requis pour les shims pris en charge.

Figure 1-1. Requête d'alerte définie par l'utilisateur

Count of events + over time grouped by hostname Apply Reset

appname contains vpqa

+ Add Filter X Clear All Filters

Figure 1-2. Sortie de webhook pour la requête d'agrégation d'alerte utilisateur

```
{
  "AlertType":1,
  "AlertName":"ESXi Vpqa Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"2016-06-24T15:42:42.055Z esx01 Vpqa: [4845FB90 verbose 'VpqaHalCnxHostagent' opID=WFU-
dcfc2d3a] [WaitForUpdatesDone] Starting next WaitForUpdates() call to hostd",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"hostname",
          "content":"esx01"
        },
        {
          "name":"appname",
          "content":"vpqa"
        }
      ]
    },
    {
      "text":"2016-06-24T15:42:42.055Z esx02 Vpqa: [4845FB90 verbose 'vpqavpqaInvtVm' opID=WFU-
dcfc2d3a] [VpqaInvtVmChangeListener] Guest DiskInfo Changed",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"hostname",
          "content":"esx02"
        },
        {
          "name":"appname",
          "content":"vpqa"
        }
      ]
    }
  ],
  "HasMoreResults":false,
  "Url":"https://10.11.12.13/s/8pgzq6",
}
```

```

    "EditUrl":"https://10.11.12.13/s/56monr",
    "Info":"This is an alert for all the 'ESXi Vpxa' messages",
    "NumHits":2
  }

```

Format de webhook pour les requêtes de message d'alerte utilisateur

Le format utilisé par un webhook vRealize Log Insight dépend du type de requête à partir de laquelle il est créé. Les notifications système, les requêtes de message d'alerte utilisateur et les alertes générées à partir des requêtes utilisateur agrégées disposent chacune d'un format de webhook différent.

Lorsque vous envoyez une alerte générée par une requête de message d'alerte utilisateur à un programme tiers, vous devez écrire un shim pour rendre les informations de vRealize Log Insight compréhensibles par les formats du programme tiers.

Format de webhook de message d'alerte utilisateur

L'exemple suivant montre le format d'un webhook de vRealize Log Insight pour une requête de message d'alerte utilisateur.

```

{
  "AlertType":1,
  "AlertName":"Hello World Alert",
  "SearchPeriod":300000,
  "HitCount":0.0,
  "HitOperator":2,
  "messages":[
    {
      "text":"hello world 1",
      "timestamp":1451940578545,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1"
        },
        {
          "name":"Field_2",
          "content":"Content 2"
        }
      ]
    },
    {
      "text":"hello world 2",
      "timestamp":1451940561008,
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1_2"
        },
        {
          "name":"Field_2",
          "content":"Content 2_2"
        }
      ]
    }
  ]
}

```

```

    }
  ],
  "HasMoreResults":false,
  "Url":"https://10.11.12.13/s/8pgzq6",
  "EditUrl":"https://10.11.12.13/s/56monr",
  "Info":"This is an alert for all the 'Hello World' messages",
  "NumHits":2
}

```

Format de webhook pour une requête d'agrégation d'alerte utilisateur

Le format utilisé par un webhook vRealize Log Insight dépend du type de requête à partir de laquelle il est créé. Les notifications système, les requêtes de message d'alerte utilisateur et les alertes générées à partir des requêtes utilisateur agrégées disposent chacune d'un format de webhook différent.

Lorsque vous envoyez une notification système à un programme tiers, vous devez écrire un shim pour rendre les informations de vRealize Log Insight compréhensibles par les formats du programme tiers.

Format de webhook pour les requêtes d'agrégation d'alerte utilisateur

```

{
  "AlertType":2,
  "AlertName":"field_1 aggregated alert",
  "SearchPeriod":300000,
  "HitCount":2.0,
  "HitOperator":2,
  "messages":[
    {
      "fields":[
        {
          "name":"Field_1",
          "content":"Content 1"
        }
      ]
    }
  ],
  "HasMoreResults":false,
  "Url":"https://10.11.12.13/s/r25g3s",
  "EditUrl":"https://10.11.12.13/s/n3gsed",
  "Info":null,
  "NumHits":1
}

```

Afficher des requêtes d'alerte


Vous pouvez afficher les requêtes d'alerte que vous avez créées et vérifier si les notifications pour ces alertes sont activées.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Gérer les alertes**.

Vous voyez une liste de toutes vos requêtes d'alerte. L'état des notifications d'alerte s'affiche sous le nom de l'alerte.

Suivant

Vous pouvez cliquer sur des requêtes d'alerte dans la liste pour modifier leurs paramètres ou supprimer les requêtes dont vous n'avez plus besoin.

Les requêtes d'alerte de pack de contenu sont en lecture seule. Pour enregistrer les modifications apportées à une alerte de pack de contenu, vous devez enregistrer l'alerte dans votre contenu personnalisé.

Modifier des requêtes d'alerte

Vous pouvez modifier le déclencheur de requêtes d'alerte, activer ou désactiver les notifications qu'une requête envoie, ou modifier la méthode de notification (e-mail, Webhook ou envoi à vRealize Operations Manager).

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

Les requêtes d'alerte de pack de contenu sont en lecture seule. Pour enregistrer les modifications apportées à une alerte de pack de contenu, vous devez enregistrer l'alerte dans votre contenu personnalisé.


Vous pouvez appliquer vos modifications à une ou plusieurs alertes en même temps.

Prérequis

- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez qu'un administrateur a configuré SMTP pour activer les notifications par e-mail. Reportez-vous à [Configurer le serveur SMTP pour Log Insight](#).
- Vérifiez qu'un administrateur a configuré la connexion entre vRealize Log Insight et vRealize Operations Manager pour activer l'intégration des alertes. Voir [Configurer Log Insight pour envoyer des événements de notification à vRealize Operations Manager](#).

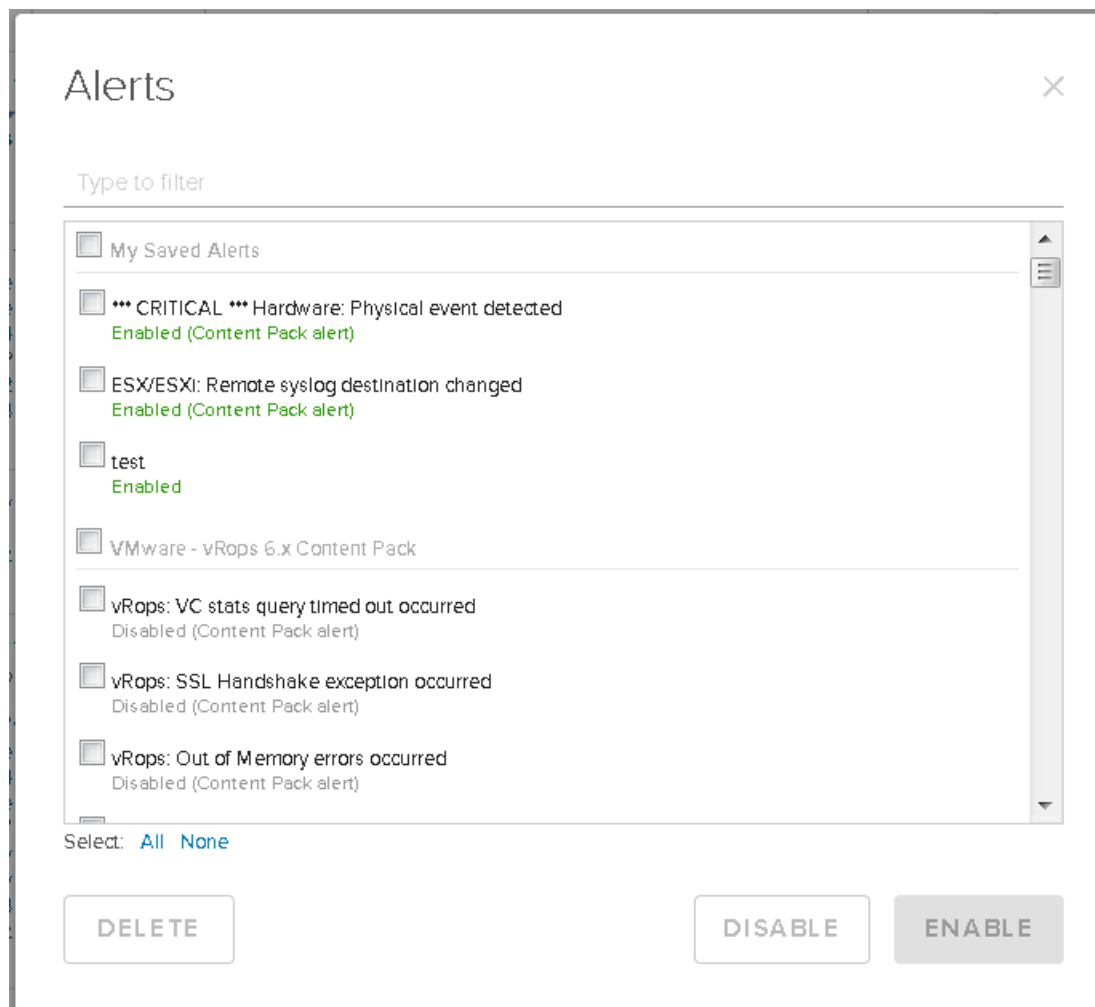
- Si vous utilisez des Webhooks, vérifiez qu'un serveur Web a été configuré pour recevoir des notifications Webhook.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu **Créer ou gérer des alertes** à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Gérer les alertes**.
- 3 Dans la liste Alertes, sélectionnez une ou plusieurs requêtes d'alerte que vous voulez modifier, puis apportez les modifications nécessaires aux paramètres de la requête.

Vous pouvez rechercher des requêtes en entrant une chaîne sous forme de filtre. Les requêtes sont étiquetées comme étant activées ou désactivées et s'il s'agit d'une requête Pack de contenu.

Remarque Si vous désactivez toutes les options de notification, la requête d'alerte est désactivée.



4 Enregistrez vos modifications.

Option	Description
Enregistrer	Ce bouton s'affiche lorsque vous modifiez vos propres alertes.
Enregistrer dans Mes alertes.	Ce bouton s'affiche lorsque vous modifiez une alerte partagée ou une alerte de pack de contenu. L'alerte d'origine reste inchangée, mais vous enregistrez une copie de l'alerte dans votre contenu personnalisé.

Activer des requêtes d'alerte

Lorsqu'une requête d'alerte est désactivée, vRealize Log Insight n'envoie pas de notifications par e-mail ou Webhook et ne déclenche pas d'événements de notification vRealize Operations Manager.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

Une requête d'alerte est désactivée dans les conditions suivantes.


- Si vous désactivez toutes les options de notification dans la boîte de dialogue Modifier l'alerte.
- Si l'alerte fait partie d'un pack de contenu.

Les requêtes d'alerte de pack de contenu sont en lecture seule. Pour enregistrer les modifications apportées à une alerte de pack de contenu, vous devez enregistrer l'alerte dans votre contenu personnalisé.

Prérequis

- Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.
- Vérifiez qu'un administrateur a configuré SMTP pour activer les notifications par e-mail. Reportez-vous à [Configurer le serveur SMTP pour Log Insight](#).
- Vérifiez qu'un administrateur a configuré la connexion entre vRealize Log Insight et vRealize Operations Manager pour activer l'intégration des alertes. Voir [Configurer Log Insight pour envoyer des événements de notification à vRealize Operations Manager](#).

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu **Créer ou gérer des alertes** à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Gérer les alertes**.
- 3 Dans la liste Alertes, cliquez sur une ou plusieurs requêtes d'alerte que vous souhaitez activer.

- 4 Sélectionnez les options de notification que vous souhaitez activer, puis fournissez les paramètres requis.

Option	Description
E-mail	Entrez au moins une adresse e-mail dans la zone de texte. Utilisez des virgules pour séparer plusieurs adresses.
Webhook	Entrez l'URL à laquelle vous souhaitez que vRealize Log Insight envoie les notifications.
Envoyez vers vRealize Operations Manager	Sélectionnez une ressource vRealize Operations Manager à associer aux événements de notification, puis sélectionnez le niveau de criticité des événements.

- 5 Enregistrez vos modifications.

Option	Description
Enregistrer	Ce bouton s'affiche lorsque vous modifiez vos propres alertes.
Enregistrer dans Mes alertes.	Ce bouton s'affiche lorsque vous modifiez une alerte partagée ou une alerte de pack de contenu. L'alerte d'origine reste inchangée, mais vous enregistrez une copie de l'alerte dans votre contenu personnalisé.

Lorsque la requête d'alerte renvoie des résultats correspondant aux critères d'alerte, vRealize Log Insight envoie des notifications correspondant à votre configuration.

Exemple : Activer une alerte à partir du pack de contenu VMware - vSphere

Le pack de contenu VMware - vSphere contient plusieurs requêtes d'alerte prédéfinies, notamment l'alerte **vCenter Server : ESX/ESXi a arrêté la journalisation**.

L'activation de l'alerte **vCenter Server : ESX/ESXi a arrêté la journalisation** est recommandée, car certaines versions d'hôtes ESXi peuvent arrêter l'envoi de données syslog lorsque vous redémarrez vRealize Log Insight. Cette alerte surveille l'événement vCenter Server `esx.problem.vmsyslogd.remote.failure` pour détecter si un hôte ESXi a arrêté d'envoyer des flux syslog.

- 1 Dans l'onglet **Analyse interactive**, développez le menu déroulant à droite du bouton **Rechercher**, puis sélectionnez **Gérer les alertes**.
- 2 Sous Pack de contenu VMware - vSphere, cliquez sur **vCenter Server: ESX/ESXi a arrêté la journalisation**.
- 3 Activez les notifications par e-mail, les notifications Webhook ou les événements de notification de vRealize Operations Manager.
- 4 Cliquez sur **Enregistrer dans Mes alertes**.

Pour détecter uniquement les hôtes ESXi qui arrêtent d'envoyer des flux à votre instance de vRealize Log Insight, vous pouvez ajouter le filtre suivant à votre requête d'alerte : **vc_remote_host (VMware - vSphere) contient <log-insight-hostname>**, et enregistrer la nouvelle requête dans vos alertes.

Pour plus de détails sur les problèmes et solutions Syslog, consultez l'article de la base de connaissances Un hôte VMware ESXi 5.x arrête d'envoyer des journaux Syslog à un serveur distant (2003127) à l'adresse <https://kb.vmware.com/kb/2003127>.

Supprimer des requêtes d'alerte



Vous pouvez supprimer des requêtes d'alerte lorsque vous n'en avez plus besoin.

Remarque Les requêtes d'alerte sont spécifiques à l'utilisateur. Vous pouvez gérer vos propres alertes uniquement.

Prérequis

Vérifiez que vous êtes connecté à l'interface utilisateur Web de vRealize Log Insight. Le format de l'URL est `https://log_insight-host`, où `log_insight-host` correspond à l'adresse IP ou au nom d'hôte du dispositif virtuel vRealize Log Insight.

Procédure

- 1 Accédez à l'onglet **Analyse interactive**.
- 2 Dans le menu à droite du bouton **Rechercher**, cliquez sur  et sélectionnez **Gérer les alertes**.
- 3 Sélectionnez une ou plusieurs alertes que vous souhaitez supprimer, puis cliquez sur **Supprimer** ou sur l'icône de suppression .
- 4 Dans la boîte de dialogue **Supprimer l'alerte**, sélectionnez **Supprimer** pour confirmer l'action.