

Application IBM QRadar User Behavior Analytics (UBA)  
Version 3.2.0

*Guide d'utilisation*



**Important**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 211.

Certaines illustrations de ce manuel ne sont pas disponibles en français à la date d'édition.

Le présent document s'applique à IBM QRadar Security Intelligence Platform V7.2.8 et aux versions ultérieures de ce produit tant qu'il n'est pas remplacé par une nouvelle édition.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France  
Direction Qualité  
17, avenue de l'Europe  
92275 Bois-Colombes Cedex*

© Copyright IBM France 2019. Tous droits réservés.

© **Copyright IBM Corporation 2016, 2019.**

---

# Table des matières

<b>Avis aux lecteurs canadiens</b> . . . . .	<b>ix</b>
<b>1 User Behavior Analytics for QRadar</b> . . . . .	<b>1</b>
Nouveautés de l'application User Behavior Analytics . . . . .	2
Problèmes connus . . . . .	7
Présentation du processus . . . . .	8
Tutoriels et démonstrations vidéo . . . . .	9
Tableau de bord UBA et informations détaillées sur les utilisateurs . . . . .	9
Examen d'utilisateurs dans QRadar Advisor with Watson . . . . .	14
Conditions préalables à l'installation de l'application User Behavior Analytics . . . . .	14
Navigateurs pris en charge pour l'application User Behavior Analytics . . . . .	15
Types de sources de journaux liés à l'application User Behavior Analytics . . . . .	16
<b>2 Installation et désinstallation</b> . . . . .	<b>17</b>
Installation de l'application User Behavior Analytics . . . . .	17
Désinstallation de l'application User Behavior Analytics . . . . .	18
<b>3 Mise à niveau</b> . . . . .	<b>21</b>
Mise à niveau de l'application User Behavior Analytics . . . . .	21
<b>4 Configuration</b> . . . . .	<b>23</b>
Configuration de l'application User Behavior Analytics . . . . .	23
Configuration de l'application Reference Data Import - LDAP . . . . .	23
Configuration des paramètres UBA . . . . .	28
Configuration du jeton d'autorisation dans les paramètres QRadar . . . . .	28
Configuration des paramètres des packages de contenu . . . . .	29
Configuration des paramètres d'application . . . . .	30
Configuration de l'importation des données utilisateur et de la coalescence utilisateur . . . . .	32
Configuration des attributs à afficher . . . . .	34
<b>5 Administration</b> . . . . .	<b>37</b>
Gestion des droits de l'application UBA de QRadar . . . . .	37
Création de listes de surveillance . . . . .	37
Affichage de la liste blanche pour les utilisateurs de confiance . . . . .	39
Gestion des outils de surveillance du réseau . . . . .	39
Gestion des programmes restreints . . . . .	40
Ajout de sources de journaux au groupe de sources de journaux de confiance . . . . .	41
Comptes dormants . . . . .	41
<b>6 Réglage</b> . . . . .	<b>43</b>
Activation des index pour l'amélioration des performances . . . . .	43
Intégration de contenu QRadar (nouveau ou existant) à l'application UBA . . . . .	44
Ensembles de référence . . . . .	45
<b>7 Règles et réglages pour l'application UBA</b> . . . . .	<b>47</b>
Accès et authentification . . . . .	47
UBA : Tentatives d'authentification par force brute . . . . .	47
UBA : Accès d'un utilisateur standard à un actif destiné uniquement aux administrateurs . . . . .	49
UBA : Accès d'un utilisateur à haut risque à une ressource critique . . . . .	51
UBA : Echec de connexion de plusieurs comptes VPN à partir d'une adresse IP unique . . . . .	52
UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP . . . . .	53
UBA : Répétition d'accès non autorisés . . . . .	53
UBA : Accès non autorisé . . . . .	55
UBA : Accès Unix/Linux avec un compte de service ou de machine . . . . .	56

UBA : Accès utilisateur - Echec de l'accès à des ressources critiques . . . . .	57
UBA : Accès utilisateur - Premier accès à des ressources critiques . . . . .	58
UBA : Accès utilisateur depuis plusieurs hôtes . . . . .	60
UBA : Accès utilisateur au serveur interne à partir d'un serveur intermédiaire . . . . .	61
UBA : Anomalie lors de la connexion utilisateur . . . . .	63
UBA : Utilisateur accédant à un compte à partir d'une source anonyme . . . . .	63
UBA : Accès utilisateur à des heures inhabituelles . . . . .	65
UBA : Accès au VPN par un compte de service ou de machine . . . . .	66
UBA : Partage d'un certificat VPN . . . . .	67
UBA : Accès Windows avec un compte de service ou de machine . . . . .	68
Comptes et privilèges . . . . .	69
UBA : Compte, groupe ou privilège ajouté . . . . .	69
UBA : Compte, groupe ou privilège modifié . . . . .	70
UBA : Attaque DoS par suppression de comptes . . . . .	71
UBA : Compte utilisateur créé et supprimé dans une courte période de temps . . . . .	74
UBA : Compte inactif utilisé . . . . .	75
UBA : Tentative d'utilisation d'un compte dormant . . . . .	75
UBA : Compte expiré utilisé . . . . .	77
UBA : Première escalade de privilèges . . . . .	77
UBA : Nouvelle utilisation du compte détectée . . . . .	79
UBA : Activité nécessitant des privilèges suspecte (première utilisation d'un privilège observée) . . . . .	80
UBA : Activité nécessitant des privilèges suspecte (privilège rarement utilisé) . . . . .	82
UBA : Tentative de l'utilisateur d'utiliser un compte suspendu . . . . .	83
UBA : Utilisateur inactif (règle ADE) . . . . .	84
Comportement de navigation . . . . .	85
UBA : Accès à un site web commercial/de services . . . . .	85
UBA : Accès à un site web de communication. . . . .	85
UBA : Accès à un site web de divertissement . . . . .	86
UBA : Accès à un site web de jeux d'argent . . . . .	86
UBA : Accès à un site web d'informatique . . . . .	87
UBA : Accès à un site web de recherche d'emploi . . . . .	87
UBA : Accès à un site web sur le mode de vie . . . . .	88
UBA : Accès à un site web malveillant . . . . .	88
UBA : Accès à un site web de contenu mixte/potentiellement pour adultes . . . . .	89
UBA : Accès à un site web de hameçonnage . . . . .	89
UBA : Accès à un site web pornographique . . . . .	90
UBA : Accès à un site web frauduleux/douteux/illégal . . . . .	90
UBA : Accès à un site web non catégorisé . . . . .	91
UBA : Utilisateur accédant à une URL risquée. . . . .	91
Cloud . . . . .	92
UBA : Accès à la console AWS par un utilisateur non autorisé . . . . .	92
UBA : Utilisateur non standard accédant à des ressources AWS . . . . .	92
Contrôleur de domaine . . . . .	93
UBA : Tentative de récupération de clé principale de secours DPAPI . . . . .	93
UBA : Énumération de comptes Kerberos détectée . . . . .	93
UBA : Plusieurs échecs d'authentification Kerberos pour le même utilisateur . . . . .	94
UBA : Accès non administrateur au contrôleur de domaine . . . . .	94
UBA : Attaque Pass-the-Hash . . . . .	96
UBA : Possible énumération de services d'annuaires . . . . .	96
UBA : Possible énumération des sessions SMB sur un contrôleur de domaine. . . . .	97
UBA : Falsification possible des tickets d'octroi d'autorisations . . . . .	98
UBA : Falsification possible des tickets d'octroi d'autorisations avec un PAC . . . . .	98
UBA : Demande de réplication d'un contrôleur autre que de domaine. . . . .	99
UBA : TGT Ticket Used by Multiple Hosts . . . . .	99
Point d'extrémité . . . . .	100
UBA : Détecter un protocole non sécurisé ou non standard . . . . .	100
UBA : Détecter les sessions SSH persistantes . . . . .	101
UBA : Paramètres Internet modifiés . . . . .	102
UBA : Activité de logiciel malveillant - Registre modifié en vrac . . . . .	103
UBA : Détection de processus Netcat (Linux). . . . .	103
UBA : Détection de processus Netcat (Windows) . . . . .	104

UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Linux) . . . . .	104
UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Windows) . . . . .	105
UBA : Comportement de rançongiciel détecté . . . . .	105
UBA : Utilisation du programme restreinte . . . . .	106
UBA : Utilisateur installant une application suspecte . . . . .	107
UBA : Utilisateur exécutant un nouveau processus . . . . .	107
UBA : Copie miroir d'un volume créée . . . . .	108
Exfiltration . . . . .	109
UBA : Abnormal data volume to external domain (règle ADE) . . . . .	109
UBA : Tentatives de transfert sortant anormales (règle ADE) . . . . .	109
UBA : Transfert sortant volumineux effectué par un utilisateur à haut risque . . . . .	110
UBA : Plusieurs transferts de fichier bloqués suivis d'un transfert de fichier réussi . . . . .	110
UBA : Accès suspects suivis d'une exfiltration de données . . . . .	113
UBA : Anomalies liées aux volumes utilisateur - Détection du trafic vers des domaines externes (règle ADE) . . . . .	113
Géographie . . . . .	114
UBA : Compte erroné créé depuis un nouvel emplacement . . . . .	114
UBA : Compte de cloud erroné créé depuis un nouvel emplacement . . . . .	118
UBA : Accès utilisateur depuis des emplacements différents . . . . .	119
UBA : Accès utilisateur depuis un emplacement interdit . . . . .	120
UBA : Accès utilisateur depuis un emplacement restreint . . . . .	122
UBA : Changement de zone géographique de l'utilisateur . . . . .	123
UBA : Zone géographique de l'utilisateur, Accès depuis des emplacements inhabituels . . . . .	125
Trafic et attaques du réseau . . . . .	126
UBA : Détection d'attaques par refus de service . . . . .	126
UBA : Activité Honeytoken . . . . .	127
UBA : Trafic réseau : surveillance des données acquises et utilisation du programme d'analyse . . . . .	128
UBA : Anomalie de session par adresse IP de destination (règle ADE) . . . . .	129
UBA : User Event Frequency Anomaly Categories (règle ADE) . . . . .	130
UBA : Anomalies liées aux volumes utilisateur - Détection du trafic vers des domaines internes (règle ADE) . . . . .	130
QRadar DNS Analyzer . . . . .	131
UBA : Accès potentiel à un domaine en liste noire . . . . .	131
UBA : Accès potentiel à un domaine DGA . . . . .	131
UBA : Potential Access to Squatting Domain . . . . .	132
UBA : Accès potentiel à un domaine Tunneling . . . . .	132
QRadar Network Insights (QNI) . . . . .	133
UBA : QNI - Accès à un service incorrectement sécurisé - Certificat arrivé à expiration . . . . .	133
UBA : QNI - Accès à un service incorrectement sécurisé - Certificat non valide . . . . .	134
UBA : QNI - Accès à un service incorrectement sécurisé - Longueur de clé publique faible . . . . .	134
UBA : QNI - Accès à un service incorrectement sécurisé - Certificat auto-signé . . . . .	135
UBA : QNI - Transfert en cours d'un contenu confidentiel vers une zone géographique étrangère . . . . .	135
UBA : QNI - Hachage de fichier comportant une menace logicielle observé . . . . .	136
UBA : QNI - Hachage de fichier sur plusieurs hôtes observé . . . . .	137
UBA : QNI - Courrier indésirable/Hameçonnage potentiel détecté pour le destinataire d'un courrier électronique rejeté . . . . .	137
UBA : QNI - Objet de courrier indésirable/hameçonnage potentiel détecté à partir de plusieurs serveurs d'envoi . . . . .	138
Reconnaissance . . . . .	138
UBA : Analyse inhabituelle des serveurs DHCP détectée . . . . .	138
UBA : Analyse inhabituelle des serveurs de base de données détectée . . . . .	139
UBA : Analyse inhabituelle des serveurs DNS détectée . . . . .	139
UBA : Analyse inhabituelle des serveurs FTP détectée . . . . .	140
UBA : Analyse inhabituelle des serveurs de jeu détectée . . . . .	140
UBA : Analyse inhabituelle du protocole ICMP générique détectée . . . . .	140
UBA : Analyse inhabituelle du protocole TCP générique détectée . . . . .	141
UBA : Analyse inhabituelle du protocole UDP générique détectée . . . . .	141
UBA : Analyse inhabituelle des serveurs IRC détectée . . . . .	142
UBA : Analyse inhabituelle des serveurs LDAP détectée . . . . .	142
UBA : Analyse inhabituelle des serveurs de messagerie détectée . . . . .	143
UBA : Analyse inhabituelle des serveurs de messagerie détectée . . . . .	143
UBA : Analyse inhabituelle des serveurs P2P détectée . . . . .	143
UBA : Analyse inhabituelle des serveurs proxy détectée . . . . .	144

UBA : Analyse inhabituelle des serveurs RPC détectée . . . . .	144
UBA : Analyse inhabituelle des serveurs SNMP détectée . . . . .	145
UBA : Analyse inhabituelle des serveurs SSH détectée . . . . .	145
UBA : Analyse inhabituelle des serveurs Web détectée . . . . .	146
UBA : Analyse inhabituelle des serveurs Windows détectée . . . . .	146
Surveillance du système (Sysmon) . . . . .	146
UBA : Outils d'exploitation courants détectés . . . . .	146
UBA : Outils d'exploitation courants détectés (actif) . . . . .	147
UBA : Processus malveillant détecté. . . . .	147
UBA : Accès à un partage réseau. . . . .	148
UBA : Processus créant des unités d'exécution distantes suspectes détectés (actif) . . . . .	149
UBA : Activités suspectes sur des hôtes compromis . . . . .	149
UBA : Activités suspectes sur des hôtes compromis (actifs) . . . . .	150
UBA : Suspicious Administrative Activities Detected . . . . .	150
UBA : Activité d'invite de commande suspecte . . . . .	151
UBA : Entrées suspectes dans le registre système (actif) . . . . .	151
UBA : Charge suspecte des images détectée (actif) . . . . .	152
UBA : Activités suspectes du pipe (actif) . . . . .	152
UBA : Activité PowerShell suspecte . . . . .	153
UBA : Activité PowerShell suspecte (actif). . . . .	153
UBA : Activités suspectes des tâches planifiées . . . . .	154
UBA : Activités suspectes des services . . . . .	154
UBA : Activités suspectes des services (actif). . . . .	155
UBA : Contournement du contrôle d'accès utilisateur détecté (actif) . . . . .	155
Renseignement sur les menaces . . . . .	156
UBA : Abnormal visits to Risky Resources (règle ADE) . . . . .	156
UBA : Indicateurs de compromission pour Locky détectés . . . . .	156
UBA : Indicateurs de compromission pour WannaCry détectés. . . . .	157
UBA : Clés de registre modifiées par un rançongiciel . . . . .	158
UBA : Utilisateur accédant à des ressources risquées . . . . .	158
UBA : Utilisateur qui accède à une adresse IP risquée, Anonymisation . . . . .	159
UBA : Utilisateur qui accède à une adresse IP risquée, Botnets . . . . .	159
UBA : Utilisateur qui accède à une adresse IP risquée, Dynamique . . . . .	160
UBA : Utilisateur qui accède à une adresse IP risquée, Logiciels malveillants . . . . .	161
UBA : Utilisateur accédant à une adresse IP risquée, spam . . . . .	161
<b>8 Application Reference Data Import - LDAP . . . . .</b>	<b>163</b>
Navigateurs pris en charge pour l'application LDAP . . . . .	164
Importation de données d'utilisateurs à partir d'un fichier CSV. . . . .	164
Création d'un jeton de service autorisé . . . . .	165
Ajout d'une autorité de certification racine privée . . . . .	165
Ajout d'une configuration LDAP . . . . .	166
Sélection d'attributs . . . . .	167
Ajout de mappages d'attributs LDAP . . . . .	167
Ajout d'une configuration de données de référence. . . . .	168
Configuration de l'interrogation . . . . .	169
Vérification que les données sont ajoutées à la collection de données de référence . . . . .	170
Création d'une règle répondant aux mises à jour de données LDAP . . . . .	170
<b>9 Application Machine Learning Analytics . . . . .</b>	<b>175</b>
Problèmes connus de Machine Learning Analytics . . . . .	175
Conditions préalables à l'installation de l'application Machine Learning Analytics . . . . .	176
Installation de l'application Machine Learning Analytics . . . . .	176
Mise à niveau de l'application Machine Learning Analytics . . . . .	177
Configuration des paramètres Machine Learning Analytics . . . . .	178
Configuration de l'analyse <i>Activité totale</i> . . . . .	178
Configuration de l'analyse <i>Tentatives de transfert sortant anormales</i> . . . . .	180
Configuration de l'analyse <i>Activité par catégorie</i> . . . . .	182
Configuration de l'analyse <i>Degré d'exposition au risque</i> . . . . .	184
Configuration de l'analyse <i>Volume anormal de données circulant vers des domaines externes.</i> . . . . .	186

Configuration de l'analyse <i>Distribution de l'activité</i> . . . . .	188
Configuration de l'analyse <i>Groupe d'homologues défini</i> . . . . .	190
Configuration de l'analyse <i>Groupe d'homologues enregistré</i> . . . . .	192
Tableau de bord UBA avec Machine Learning Analytics . . . . .	194
Groupes d'utilisateurs pour l'analyse du groupe d'homologues défini . . . . .	201
Désinstallation de l'application Machine Learning Analytics . . . . .	202
<b>10 Identification et résolution des problèmes et support . . . . .</b>	<b>205</b>
Page Aide et assistance d'UBA . . . . .	205
Demandes de service . . . . .	206
Le statut de l'application Machine Learning affiche un avertissement dans le tableau de bord . . . . .	206
Le statut de l'application Machine Learning n'affiche pas de progression de l'ingestion des données . . . . .	206
Statut d'erreur pour l'application ML . . . . .	207
Extraction des fichiers journaux UBA et Machine Learning . . . . .	208
<b>Remarques . . . . .</b>	<b>211</b>
Marques . . . . .	212
Dispositions applicables à la documentation du produit . . . . .	213
Déclaration IBM de confidentialité sur Internet . . . . .	213
Règlement général sur la protection des données . . . . .	214



---

## Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

### Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

### Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

### Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

### OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

### Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Post)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

## Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

## Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

---

# 1 User Behavior Analytics for QRadar

L'application User Behavior Analytics for QRadar vous permet de déterminer les profils de risque des utilisateurs au sein de votre réseau et de prendre les mesures nécessaires lorsqu'une alerte signale un comportement à risque.

L'application User Behavior Analytics for QRadar (UBA) est un outil de détection des menaces internes à votre organisation. Bâtie sur l'infrastructure des applis QRadar, elle tire parti des données existantes de votre environnement QRadar pour générer de nouvelles perspectives sur les utilisateurs et les risques. UBA ajoute deux fonctions majeures à QRadar : le profilage du risque et l'identité unifiée pour les utilisateurs.

Le profilage du risque est réalisé par l'affectation d'un niveau de risque à différents cas d'utilisation de sécurité. Il peut s'agir, par exemple, de simples règles et de contrôles visant à détecter les accès aux sites web sur liste noire ou d'analyses plus avancées exploitant l'apprentissage machine. Un niveau de risque est affecté à chaque cas d'utilisation en fonction de la gravité de l'incident détecté et de la fiabilité de cette détection. Pour générer ces informations et profiler les utilisateurs et le risque qu'ils représentent, UBA utilise les données d'événements et de flux existantes, recueillies au sein de votre système QRadar. Elle analyse trois types de trafic : 1. Trafic en lien avec les accès, l'authentification et les changements de compte. 2. Comportement de l'utilisateur sur le réseau - équipements tels que proxys, pare-feux, IPS et VPN. 3. Journaux des points d'extrémité et des applications, tels que ceux des systèmes Windows ou Linux et des applications SAAS. Les trois types de trafic enrichissent la base de données d'UBA et lui permettent d'analyser davantage de cas d'utilisation pour profiler le risque.

L'unification de l'identité des utilisateurs est accomplie par la combinaison des comptes disparates de chaque utilisateur dans QRadar. En important les données d'un annuaire Active Directory ou LDAP ou d'un fichier CSV, vous pouvez apprendre à UBA à identifier quels comptes appartiennent à tel ou tel utilisateur. C'est ce qui permet d'attribuer un niveau de risque au trafic généré par différents noms d'utilisateur.

L'application ML (Machine Learning) est un outil complémentaire qui étend l'application UBA. Elle autorise une analyse et une identification plus détaillée des cas d'utilisation, avec le profilage et le regroupement des données de séries temporelles. Elle s'installe à partir de l'application UBA, sur la page de paramètres Machine Learning. ML ajoute davantage de visualisations à UBA en montrant les comportements qu'elle a appris (modèles), les comportements du moment et les alertes. Elle utilise jusqu'à quatre semaines de données historiques collectées dans QRadar pour établir un modèle prédictif et la référence (ou ligne de base) d'un comportement considéré comme normal pour un utilisateur.

Pour plus d'informations sur l'utilisation de l'application Reference Data Import - LDAP, consultez 8, «Application Reference Data Import - LDAP», à la page 163.

Pour plus d'informations sur l'utilisation de l'application Machine Learning Analytics, consultez 9, «Application Machine Learning Analytics», à la page 175.

**Avertissement :** Vous devez installer IBM® QRadar version 7.2.8 ou une version ultérieure avant d'installer l'application QRadar UBA.

## Concepts associés:

7, «Règles et réglages pour l'application UBA», à la page 47

L'application User Behavior Analytics (UBA) d'IBM QRadar prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

«Configuration de l'application User Behavior Analytics», à la page 23

Avant d'utiliser l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer des

paramètres de configuration supplémentaires.

8, «Application Reference Data Import - LDAP», à la page 163

L'application Reference Data Import - LDAP permet de collecter les informations d'identité contextuelle de plusieurs sources LDAP dans QRadar Console.

9, «Application Machine Learning Analytics», à la page 175

L'application Machine Learning Analytics (ML) étend les fonctions de votre système QRadar et de l'application QRadar User Behavior Analytics (UBA) en ajoutant des scénarios d'utilisation pour Machine Learning Analytics. Les scénarios d'utilisation Machine Learning Analytics vous permettent d'avoir une vision plus précise du comportement utilisateur concernant la modélisation prédictive. Grâce à l'application ML, votre système peut détecter plus facilement le comportement attendu des utilisateurs au sein de votre réseau.

#### **Tâches associées:**

«Installation de l'application User Behavior Analytics», à la page 17

Utilisez l'outil Gestion des extensions d'IBM QRadar pour charger et installer directement votre archive d'application dans QRadar Console.

«Mise à niveau de l'application User Behavior Analytics», à la page 21

L'outil Gestion des extensions d'IBM QRadar vous permet de mettre à niveau votre application.

---

## **Nouveautés de l'application User Behavior Analytics**

Découvrez les nouveautés de chaque édition de l'application User Behavior Analytics (UBA).

### **Nouveautés de la version 3.2.0**

- Les utilisateurs avec des comptes dormants sont désormais identifiés sur le tableau de bord ainsi que sur les pages de profil de l'utilisateur. Pour plus d'informations, consultez «Comptes dormants», à la page 41.
- Possibilité de créer des listes de surveillance des comptes de services en fonction d'une propriété d'utilisateur manquante. Pour plus d'informations, consultez «Création de listes de surveillance», à la page 37.
- L'application LDAP évolue pour vous permettre de sélectionner les attributs LDAP à utiliser dans UBA. Notez que lorsque vous configurez LDAP, vous devez désormais sélectionner une clé externe dans la section Mappage d'attributs. Pour plus d'informations, consultez «Configuration de l'application Reference Data Import - LDAP», à la page 23.
- Ajout de la possibilité d'importer des informations d'utilisateurs d'un fichier CSV. Pour plus d'informations, consultez «Importation de données d'utilisateurs à partir d'un fichier CSV», à la page 164.
- Ajout du cas d'utilisation UBA : Accès utilisateur depuis plusieurs hôtes. Pour plus d'informations, consultez «UBA : Accès utilisateur depuis plusieurs hôtes», à la page 60.
- Ajout du cas d'utilisation UBA : Possible énumération de services d'annuaires. Pour plus d'informations, consultez «UBA : Possible énumération de services d'annuaires», à la page 96.
- Ajout du cas d'utilisation UBA : Possible énumération des sessions SMB sur un contrôleur de domaine. Pour plus d'informations, consultez «UBA : Possible énumération des sessions SMB sur un contrôleur de domaine.», à la page 97.
- Ajout du cas d'utilisation UBA : Accès suspects suivis d'une exfiltration de données. Pour plus d'informations, consultez «UBA : Accès suspects suivis d'une exfiltration de données», à la page 113.
- Ajout du cas d'utilisation UBA : Tentative d'utilisation d'un compte dormant. Pour plus d'informations, consultez «UBA : Tentative d'utilisation d'un compte dormant», à la page 75.

### **Nouveautés de la version 3.1.0**

- Vous pouvez à présent personnaliser l'affichage des métriques dans la ligne de temps des activités de l'utilisateur et voir les données dont ces métriques sont constituées.
- Ajout de la possibilité de fixer un seuil de risque dynamique.

- Deux nouvelles catégories de cas d'utilisation sont ajoutées à la page Règles et réglages : Cloud et Contrôleur de domaine. Pour plus d'informations, consultez 7, «Règles et réglages pour l'application UBA», à la page 47.
- Ajout du cas d'utilisation UBA : Utilisateur non standard accédant à des ressources AWS. Pour plus d'informations, consultez «UBA : Utilisateur non standard accédant à des ressources AWS», à la page 92.
- Ajout du cas d'utilisation UBA : Accès à la console AWS par un utilisateur non autorisé. Pour plus d'informations, consultez «UBA : Accès à la console AWS par un utilisateur non autorisé», à la page 92.
- Ajout du cas d'utilisation UBA : Demande de réplication d'un contrôleur autre que de domaine. Pour plus d'informations, voir «UBA : Demande de réplication d'un contrôleur autre que de domaine», à la page 99.
- Ajout du cas d'utilisation UBA : Enumération de comptes Kerberos détectée. Pour plus d'informations, consultez «UBA : Enumération de comptes Kerberos détectée», à la page 93.
- Ajout du cas d'utilisation UBA : Falsification possible des tickets d'octroi d'autorisations avec un PAC. Pour plus d'informations, consultez «UBA : Falsification possible des tickets d'octroi d'autorisations avec un PAC», à la page 98.
- Ajout du cas d'utilisation UBA : Tentative de récupération de clé principale de secours DPAPI. Pour plus d'informations, consultez «UBA : Tentative de récupération de clé principale de secours DPAPI», à la page 93.
- Ajout du cas d'utilisation UBA : Attaque DoS par suppression de comptes. Pour plus d'informations, consultez «UBA : Attaque DoS par suppression de comptes», à la page 71.
- Ajout du cas d'utilisation UBA : Plusieurs transferts de fichier bloqués suivis d'un transfert de fichier réussi. Pour plus d'informations, consultez «UBA : Plusieurs transferts de fichier bloqués suivis d'un transfert de fichier réussi», à la page 110.

### **Nouveautés de la version 3.0.1**

- Ajout d'un scénario d'utilisation pour la prise en charge de la détection DNS Tunneling par l'application IBM QRadar DNS Analyzer. Pour plus d'informations, voir «UBA : Accès potentiel à un domaine Tunneling», à la page 132.
- Correction d'un problème qui pourrait empêcher la possibilité de verser des utilisateurs à partir d'une table de référence.

### **Nouveautés de la version 3.0.0**

- Vous pouvez désormais créer et gérer des listes de surveillance de manière à pouvoir surveiller des groupes d'utilisateurs personnalisés. Pour plus d'informations, «Création de listes de surveillance», à la page 37.
- Vous pouvez maintenant afficher, filtrer, et régler des scénarios d'utilisation UBA à partir de la nouvelle page Règles et réglages. Pour plus d'informations, voir 7, «Règles et réglages pour l'application UBA», à la page 47.
- Dans la ligne de temps des activités de l'utilisateur, les événements à risque et les métriques sont désormais visibles par session d'activité. Pour plus d'informations, consultez «Tableau de bord UBA et informations détaillées sur les utilisateurs», à la page 9.
- Ajout d'une analyse Machine Learning qui détecte tout volume anormal de données circulant vers des domaines externes. Pour plus d'informations, consultez «Configuration de l'analyse *Volume anormal de données circulant vers des domaines externes*», à la page 186.
- Ajout d'un scénario d'utilisation UBA : Transfert sortant volumineux effectué par un utilisateur à haut risque. Pour plus d'informations, consultez «UBA : Transfert sortant volumineux effectué par un utilisateur à haut risque», à la page 110.
- Ajout d'un scénario d'utilisation UBA : Activité Honeytoken. Pour plus d'informations, consultez «UBA : Activité Honeytoken», à la page 127.

- Ajout d'un scénario d'utilisation UBA : Tentatives d'authentification par force brute. Pour plus d'informations, consultez «UBA : Tentatives d'authentification par force brute», à la page 47.
- Ajout d'un scénario d'utilisation UBA : Compte utilisateur créé et supprimé dans une courte période de temps. Pour plus d'informations, consultez «UBA : Compte utilisateur créé et supprimé dans une courte période de temps», à la page 74.
- Ajout d'un scénario d'utilisation UBA : Accès d'un utilisateur à haut risque à une ressource critique. Pour plus d'informations, consultez «UBA : Accès d'un utilisateur à haut risque à une ressource critique», à la page 51.
- Ajout d'un scénario d'utilisation : Compte erroné créé depuis un nouvel emplacement. Pour plus d'informations, consultez «UBA : Compte erroné créé depuis un nouvel emplacement», à la page 114.
- Ajout d'un scénario d'utilisation UBA : Compte de cloud erroné créé depuis un nouvel emplacement. Pour plus d'informations, consultez «UBA : Compte de cloud erroné créé depuis un nouvel emplacement», à la page 118.

## Nouveautés de la version 2.8.0

- Il est désormais possible de filtrer avec des requêtes AQL entrées dans le champ **Filtre de recherche avancée** vous configurez les paramètres des analyses Machine Learning. Pour plus d'informations, consultez «Configuration des paramètres Machine Learning Analytics», à la page 178.
- Les statistiques Utilisateurs découverts à partir d'événements et Utilisateurs importés depuis le répertoire sont désormais visibles sur le tableau de bord. Pour plus d'informations, voir «Tableau de bord UBA et informations détaillées sur les utilisateurs», à la page 9.
- Vous pouvez maintenant spécifier les utilisateurs que vous voulez suivre avec Machine Learning. Pour plus d'informations, voir «Tableau de bord UBA et informations détaillées sur les utilisateurs», à la page 9
- Vous pouvez maintenant choisir d'afficher ou non le graphique de chaque analyse Machine Learning. Pour plus d'informations, consultez «Configuration des paramètres Machine Learning Analytics», à la page 178.
- Vous pouvez maintenant choisir s'il faut ou non installer ou mettre à niveau les packages de contenu UBA (règles QRadar, propriétés personnalisées et données de référence pour les cas d'utilisation). Pour plus d'informations, consultez «Configuration des paramètres des packages de contenu», à la page 29.
- Une analyse Machine Learning a été ajoutée, que vous pouvez activer pour détecter les tentatives de transfert sortant anormal. Pour plus d'informations, voir «Configuration de l'analyse *Tentatives de transfert sortant anormales*», à la page 180.
- Des configurations mémoire ont été ajoutées dans les paramètres Machine Learning pour permettre la surveillance d'un nombre accru d'utilisateurs lorsque vous exécutez UBA avec Machine Learning sur un noeud d'application.
- Un ensemble de référence a été ajouté pour permettre l'identification des utilisateurs à haut risque. Pour plus d'informations, consultez «Ensembles de référence», à la page 45.
- Des cas d'utilisation ont été ajoutés pour les catégories suivantes d'accès à un site web : site web commercial/de services, site web sur un mode de vie, site web non catégorisé. Pour plus d'informations, consultez «Comportement de navigation», à la page 85.
- Ajout du cas d'utilisation UBA : Accès à un partage réseau. Pour plus d'informations, consultez «UBA : Accès à un partage réseau», à la page 148.
- Ajout du cas d'utilisation UBA : Accès non administrateur au contrôleur de domaine. Pour plus d'informations, consultez «UBA : Accès non administrateur au contrôleur de domaine», à la page 94.
- Ajout du cas d'utilisation UBA : Accès utilisateur depuis un emplacement interdit. Pour plus d'informations, consultez «UBA : Accès utilisateur depuis un emplacement interdit», à la page 120.
- Ajout du cas d'utilisation UBA : Accès utilisateur depuis un emplacement restreint. Pour plus d'informations, consultez «UBA : Utilisation du programme restreinte», à la page 106

- Ajout du cas d'utilisation UBA : Plusieurs échecs d'authentification Kerberos pour le même utilisateur. Pour plus d'informations, consultez «UBA : Plusieurs échecs d'authentification Kerberos pour le même utilisateur», à la page 94.
- Ajout du cas d'utilisation UBA : TGT Ticket Used by Multiple Hosts. Pour plus d'informations, voir «UBA : TGT Ticket Used by Multiple Hosts», à la page 99

## Nouveautés de la version 2.7.0

**Avertissement :** Si vous effectuez une mise à niveau vers la version 2.7.0, vous devez appliquer les instructions de la note technique suivante : <http://www.ibm.com/support/docview.wss?uid=swg22005489>.

La version 2.7.0 de l'application User Behavior Analytics inclut les nouvelles fonctions suivantes :

- Vous pouvez désormais examiner les utilisateurs dans l'application QRadar Advisor with Watson. Remarque : QRadar Advisor with Watson V1.13.0 doit être installé. Pour plus d'informations, voir «Examen d'utilisateurs dans QRadar Advisor with Watson», à la page 14.
- Vous pouvez désormais générer un rapport de conformité RGPD (Règlement général sur la protection des données) pour un utilisateur et arrêter le suivi d'un utilisateur.
- Vous pouvez désormais marquer le statut d'examen d'un utilisateur et afficher tous les utilisateurs en cours d'examen à partir du tableau de bord **Analyse utilisateur**.
- Vous pouvez désormais définir si vous souhaitez afficher les indicateurs de pays et de région pour les adresses IP.
- Ajout de la prise en charge des événements d'accès au domaine générés par l'application IBM QRadar DNS Analyzer. Pour plus d'informations, voir «QRadar DNS Analyzer», à la page 131.
- Ajout de 19 scénarios d'utilisation d'analyse inhabituelle. Pour plus d'informations, voir «Reconnaissance», à la page 138.
- Ajout de 3 scénarios d'utilisation d'application suspecte. Pour plus d'informations, voir «Point d'extrémité», à la page 100.
- Ajout de 10 scénarios d'utilisation de navigation à risque. Pour plus d'informations, consultez «Comportement de navigation», à la page 85.
- Ajout de 13 scénarios d'utilisation de surveillance de système (Sysmon). Pour plus d'informations, voir «Surveillance du système (Sysmon)», à la page 146.

## Nouveautés de la version 2.6.0

**Avertissement :** Si vous effectuez une mise à niveau vers la version 2.6.0, vous devez suivre les instructions de la note technique suivante : <http://www.ibm.com/support/docview.wss?uid=swg22005489>.

La version 2.6.0 de l'application User Behavior Analytics inclut les nouvelles fonctions suivantes :

- Extension de l'application Machine Learning Analytics (ML) pour analyser les anomalies en fonction des groupes d'homologues définis dans LDAP et Active Directory.
- L'analyse Groupe d'homologues pour l'application ML a été renommée Groupe d'homologues enregistré.
- Ajout du scénario d'utilisation UBA : Process Executed Outside Gold Disk Whitelist (Windows / Linux)
- Ajout du scénario d'utilisation UBA : Comportement de rançongiciel détecté
- Ajout du scénario d'utilisation UBA : Détection de processus Netcat (Windows / Linux)
- Ajout du scénario d'utilisation UBA : Echec de connexion de plusieurs comptes VPN à partir d'une adresse IP unique
- Ajout du scénario d'utilisation UBA : Copie miroir d'un volume créée

- Ajout du scénario d'utilisation UBA : Détecter un protocole non sécurisé ou non standard
- Ajout du scénario d'utilisation UBA : Activité de logiciel malveillant - Registre modifié en vrac
- Ajout du scénario d'utilisation UBA : Paramètres Internet modifiés
- Ajout du scénario d'utilisation UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP
- Ajout du scénario d'utilisation UBA : Activité PowerShell suspecte (actif)
- Ajout du scénario d'utilisation UBA : Activité PowerShell suspecte
- Ajout du scénario d'utilisation UBA : Suspicious Command shell Activity
- Ajout du scénario d'utilisation UBA : Processus malveillant détecté

## Nouveautés de la version 2.5.0

**Avvertissement :** Si vous effectuez une mise à niveau vers la version 2.5.0, vous devez suivre les instructions de la note technique suivante : <http://www.ibm.com/support/docview.wss?uid=swg22005489>.

La version 2.5.0 de l'application User Behavior Analytics inclut les améliorations suivantes :

- Ajout de la possibilité d'examiner rapidement le comportement risqué d'un utilisateur avec l'afficheur d'événements contextuels en ligne. Pour plus d'informations, voir «Tableau de bord UBA et informations détaillées sur les utilisateurs», à la page 9.
- Ajout d'une page Aide et assistance, contenant des liens vers la documentation, les didacticiels et les informations d'assistance et permettant d'accéder aux fonctions d'administration. Pour plus d'informations, voir «Page Aide et assistance d'UBA», à la page 205.
- Augmentation de la précision et de l'évolutivité de Machine Learning et amélioration des messages dans la section Statut des modèles Machine Learning du tableau de bord. Pour plus d'informations, voir «Tableau de bord UBA avec Machine Learning Analytics», à la page 194.
- Ajout du scénario d'utilisation UBA : Utilisateur exécutant un nouveau processus. Pour plus d'informations, voir «UBA : Utilisateur exécutant un nouveau processus», à la page 107.
- Ajout du scénario d'utilisation UBA : Utilisateur installant une application suspecte. Pour plus d'informations, voir «UBA : Utilisateur installant une application suspecte», à la page 107.
- Ajout du scénario d'utilisation UBA : Unix/Linux System Accessed With Service or Machine Account. Pour plus d'informations, voir «UBA : Accès Unix/Linux avec un compte de service ou de machine», à la page 56.
- Ajout du scénario d'utilisation UBA : Accès utilisateur au serveur interne à partir d'un serveur intermédiaire. Pour plus d'informations, voir «UBA : Accès utilisateur au serveur interne à partir d'un serveur intermédiaire», à la page 61.
- Ajout du scénario d'utilisation UBA : Accès d'un utilisateur standard à un actif destiné uniquement aux administrateurs. Pour plus d'informations, voir «UBA : Accès d'un utilisateur standard à un actif destiné uniquement aux administrateurs», à la page 49.

## Nouveautés de la version 2.4.0

**Avvertissement :** Si vous effectuez une mise à niveau vers la version 2.4.0, vous devez suivre les instructions de la note technique suivante : <http://www.ibm.com/support/docview.wss?uid=swg22005489>.

La version 2.4.0 de l'application User Behavior Analytics inclut les améliorations suivantes :

- Affichage du statut d'extraction LDAP dans l'application LDAP.
- Importation de 400 000 utilisateurs au maximum par l'application LDAP. Avant de changer la configuration, voir la section Problèmes connus.
- Rationalisation et simplification de l'intégration et du mappage des données LDAP/AD.
- Possibilité de mapper un nombre illimité d'alias à un ID utilisateur principal.

- Ajout de paramètres de configuration de mémoire dans Paramètres Machine Learning pour la prise en charge d'utilisateurs supplémentaires lorsque vous exécutez Machine Learning sur un noeud d'application.
- Ajout d'une enquête de satisfaction.
- Ajout du scénario d'utilisation UBA: Windows access with Service or Machine Account. Pour plus d'informations, voir «UBA : Accès Windows avec un compte de service ou de machine», à la page 68
- Ajout du scénario d'utilisation UBA: D/DoS Attack Detected. Pour plus d'informations, voir «UBA : Détection d'attaques par refus de service», à la page 126
- Ajout du scénario d'utilisation UBA: Detect Persistent SSH session. Pour plus d'informations, voir «UBA : Détecter les sessions SSH persistantes», à la page 101
- Ajout du scénario d'utilisation UBA: Abnormal data volume to external domain. Pour plus d'informations, voir «UBA : Abnormal data volume to external domain (règle ADE)», à la page 109
- Ajout du scénario d'utilisation UBA: Abnormal Outbound Attempts. Pour plus d'informations, voir «UBA : Tentatives de transfert sortant anormales (règle ADE)», à la page 109

---

## Problèmes connus

L'application User Behavior Analytics inclut des informations pour la mise à niveau ainsi que des problèmes connus.

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

### Problèmes connus pour la version 3.2.0

Les problèmes ci-dessous ont été détectés dans l'application User Behavior Analytics.

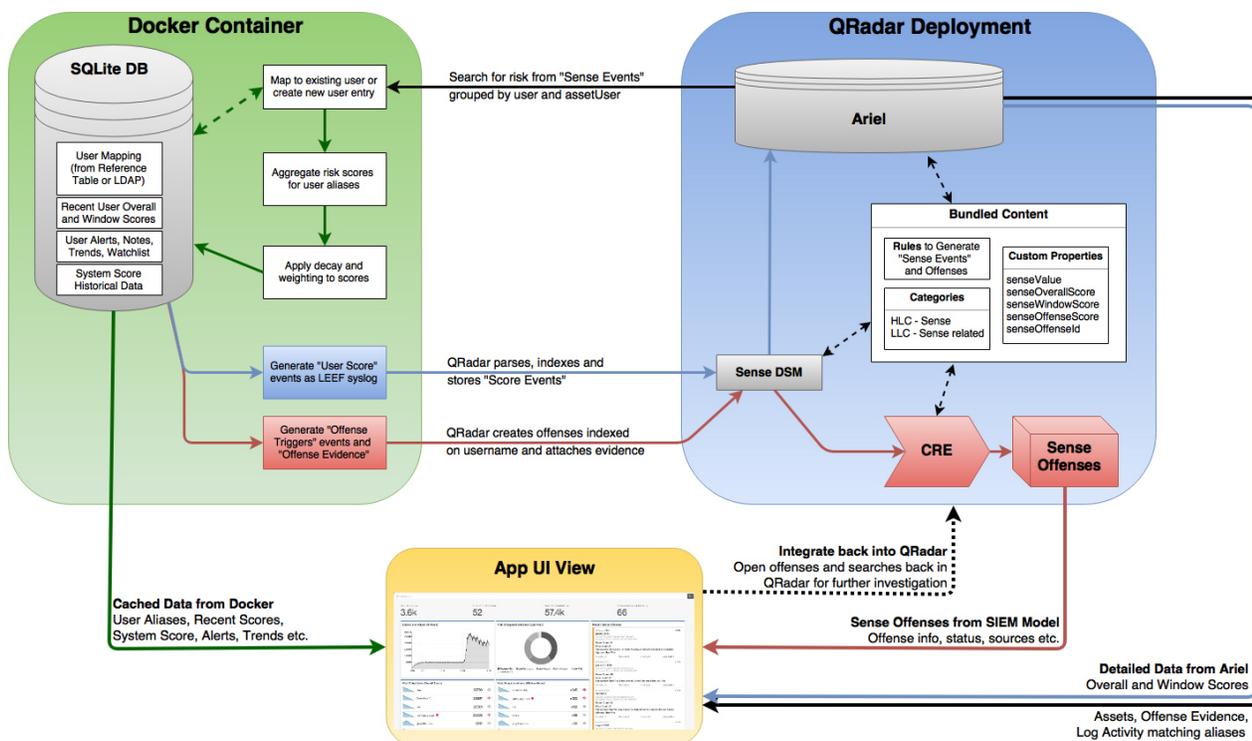
- La coalescence utilisateur depuis une table de référence produit des informations utilisateur incomplètes dans les enregistrements utilisateur UBA si vous exécutez QRadar 7.2.8 Correctif 13, QRadar 7.2.8 Correctif 13 IF1, QRadar 7.3.1 Correctif 3 ou QRadar 7.3.1 Correctif 4. Le problème est résolu dans la version 7.3.1 Correctif 4 IF1. Voir l'APAR IJ06032 pour plus d'informations.
- Si vous effectuez une mise à niveau de l'application UBA et recevez une erreur d'exception Notification QRadar indiquant qu'un ensemble de règles n'a pas pu se charger, vous pouvez l'ignorer et continuer. Si l'erreur persiste, contactez le service clients IBM.
- En raison de problèmes connus dans QRadar version 7.2.8 Correctif 12 et QRadar version 7.3.1 Correctif 3, vous devez effectuer une mise à niveau vers QRadar version 7.2.8 Correctif 13 et QRadar version 7.3.1 Correctif 4.
- Après le passage de l'application à la version 3.2.0, l'affichage du graphique de distribution d'activité de Machine Learning sur la page Détails de l'utilisateur peut prendre une journée.
- Lorsque vous affichez la page de profil d'un utilisateur, le bouton **Ajouter à la liste blanche** peut ne pas s'afficher. Dans ce cas, vous pouvez actualiser la page pour résoudre le problème.
- L'importation de plus de 100 000 utilisateurs dans LDAP for UBA peut affecter considérablement le système QRadar et l'installation de l'application UBA. Le problème est causé par un problème connu, décrit dans l'APAR IV98655. Il n'est pas recommandé d'importer plus de 200 000 utilisateurs sauf si vous utilisez QRadar 7.3.0 ou version ultérieure sur une console 128 Go.
- Dans de rares instances de QRadar version 7.2.8 et version 7.3.0, un problème peut survenir avec un jeton SEC récemment créé. En effet, le jeton SEC peut sembler fonctionner correctement puis devenir non valide ultérieurement. Pour résoudre ce problème, effectuez une des actions suivantes :
  - Redémarrez le service Apache Tomcat à partir d'une ligne de commande sur QRadar Console.
  - Déployez une action à partir de l'onglet Admin dans QRadar.
- Sur le graphique Score système, lorsque la plage de dates fait plus d'un jour et que la date de fin coïncide avec la journée en cours, les 8 premiers points de données indiquent 0 seconde.

- Des chaînes en anglais ou du texte corrompu s'affichent dans certaines parties de l'interface utilisateur lors de l'utilisation de QRadar version 7.2.8 dans certains environnements locaux.

## Présentation du processus

L'application User Behavior Analytics est utilisée avec votre système QRadar pour collecter des données sur les utilisateurs de votre réseau.

## Mode de fonctionnement d'UBA



1. Les journaux envoient des données à QRadar.
2. Les règles spécifiques à UBA recherchent certains événements (en fonction des règles UBA activées) et déclenchent un nouvel événement Sense lu par l'application UBA.
3. Pour les règles UBA, il est nécessaire que les événements aient un nom d'utilisateur et fassent l'objet d'autres tests (consultez les règles pour connaître leurs exigences).
4. UBA extrait le nom d'utilisateur et la valeur *senseValue* de l'événement Sense puis augmente le *score de risque* de cet utilisateur en fonction de la valeur *senseValue*.
5. Lorsque le *score de risque* d'un utilisateur est supérieur au seuil défini sur la page Paramètres UBA, UBA envoie un événement qui déclenche la règle "UBA : Create Offense" et une infraction est créée pour cet utilisateur.

## Score de risque

Un score de risque est la somme de tous les événements de risque détectés par les règles UBA. Plus le score est élevé, plus il est probable qu'un utilisateur interne représente un risque pour la sécurité et justifie un examen plus approfondi de l'activité réseau de cet utilisateur. Le score de risque diminue au fil du temps si aucun nouvel événement ne se produit. La pente de réduction, ou ampleur de la réduction en fonction du temps, est contrôlée par la valeur du paramètre **Réduire le risque avec le facteur indiqué, par heure** sur la page Paramètres UBA.

## Mode d'utilisation des valeurs senseValue pour créer des scores de risque d'utilisateur

Chaque règle et analyse ont une valeur attribuée qui indique la gravité du problème détecté. Dès qu'une action utilisateur provoque le déclenchement d'une règle, cette valeur est ajoutée au score pour l'utilisateur. Plus l'utilisateur "viole" une règle, plus le score est élevé.

### Règles et événements Sense

Les règles, lorsqu'elles sont déclenchées, génèrent des événements Sense permettant de déterminer le score de risque de l'utilisateur.

Vous pouvez mettre à jour des règles existantes dans QRadar pour générer des événements Sense. Pour plus d'informations, voir «Intégration de contenu QRadar (nouveau ou existant) à l'application UBA», à la page 44.

### Machine Learning Analytics et événements Sense

Vous pouvez installer l'application Machine Learning Analytics et activer cette dernière pour identifier un comportement utilisateur anormal. Les analyses, lorsqu'elles sont déclenchées, génèrent des événements Sense qui augmentent également le score de risque d'un utilisateur.

---

## Tutoriels et démonstrations vidéo

Informations supplémentaires sur les applications IBM QRadar User Behavior Analytics (UBA), Reference Data Import - LDAP et Machine Learning Analytics (ML).

### IBM Security Learning Academy

Inscrivez-vous aux cours UBA (User Behavior Analytics) sur le site Web IBM Security Learning Academy.

**Conseil :** Pour pouvoir vous inscrire et accéder aux vidéos, vous devez avoir un compte IBM.

### Tutoriels vidéo sur YouTube

Démonstration de l'application User Behavior Analytics avec Machine Learning V2.0.0 : <https://www.youtube.com/watch?v=RgF1RztR1yg>.

Démonstration de la configuration de l'application Reference Data Import - LDAP : <https://www.youtube.com/watch?v=ER-wYxS6wFk>.

Présentation générale de l'application User Behavior Analytics :

- [https://www.youtube.com/watch?v=bf\\_DODl8Ehs](https://www.youtube.com/watch?v=bf_DODl8Ehs)
- <https://www.youtube.com/watch?v=ARVsuQaSF9E>

---

## Tableau de bord UBA et informations détaillées sur les utilisateurs

L'application User Behavior Analytics (UBA) d'IBM QRadar affiche les données de risque globales associées aux utilisateurs de votre réseau.

### Tableau de bord

Une fois l'application UBA installée et configurée, cliquez sur l'onglet **Analyse utilisateur** pour ouvrir le tableau de bord.

**Remarque :** L'application UBA peut surveiller jusqu'à 400.000 utilisateurs.

Dans la zone **Rechercher un utilisateur**, vous pouvez rechercher des utilisateurs par leur nom, leur adresse e-mail ou leur nom d'utilisateur. Au fur et à mesure de la saisie du nom, l'application affiche les cinq premiers résultats.

Le tableau de bord s'actualise automatiquement toutes les minutes et affiche les données de risque suivantes :

Utilisateurs surveillés	Affiche le nombre total d'utilisateurs que l'application UBA surveille activement.
Utilisateurs à haut risque	Affiche le nombre d'utilisateurs qui dépassent actuellement le score de risque. La valeur servant à déterminer le score de risque est fixée dans les paramètres UBA, par l'option "Seuil de risque pour déclencher des infractions".
Utilisateurs reconnus à partir des événements	Affiche le nombre d'utilisateurs découverts d'après des événements, ce qui exclut les utilisateurs importés.
Utilisateurs importés depuis le répertoire	Affiche le nombre d'utilisateurs qui ont été importés de tables de référence.
Analyse active	<ul style="list-style-type: none"> <li>• Règles UBA : indique le statut des règles. Un statut vert indique que les règles sont installées et actives. Le gris indique que les règles sont désactivées. Le jaune indique que l'installation est en cours.</li> <li>• Règles de flux : indique le statut des règles QNI. Un statut vert indique que les règles sont installées et actives. Le gris indique que les règles QNI ne sont pas installées.</li> <li>• Anomalie comportementale : un statut vert indique que les règles ADE sont installées et actives. Le gris indique que les règles ADE ne sont pas installées.</li> <li>• Machine Learning Analytics : un statut vert indique que l'application Machine Learning Analytics est installée. Le gris indique que l'application Machine Learning Analytics n'est pas installée.</li> </ul>
Utilisateurs surveillés	<p>Affiche les 10 utilisateurs présentant le plus de risques. La première colonne contient le nom d'affichage et la fonction, ainsi que la ville, le cas échéant.</p> <ul style="list-style-type: none"> <li>• Risque récent : Affiche le risque cumulé pour l'utilisateur respectif au cours des 5 dernières minutes.</li> <li>• Score de risque : Affiche un graphique illustrant la tendance de score du risque global de l'utilisateur au cours de la dernière heure et le score de risque en cours. La couleur du graphique indique le niveau de risque global.</li> <li>• Icône Liste de surveillance : Permet d'ajouter l'utilisateur à une liste de surveillance ou de créer une liste de surveillance. Le nombre indique le nombre de listes de surveillance dont l'utilisateur est membre.</li> <li>• Vous pouvez afficher tous les utilisateurs suivis sur la page Recherche.</li> </ul>
Infractions récentes	Infractions Sense les plus récentes par utilisateur.
[Utilisateur] Liste de surveillance	<p>Listes de surveillance que vous avez créées. Vous pouvez créer autant de listes de surveillance que vous le souhaitez et elles s'affichent sur le tableau de bord. Vous pouvez afficher tous les utilisateurs suivis dans la liste de surveillance personnalisée que vous avez créée sur la page <b>Recherche</b>.</p> <p><b>Conseil :</b> Pour ajouter un utilisateur à une liste de surveillance, cliquez sur l'icône</p> <p><b>Liste de surveillance</b>   0 . Le nombre indique le nombre de listes de surveillance dont l'utilisateur est membre.</p>
Score système	Accumulation globale du score du risque pour tous les utilisateurs à un moment donné. Cliquez sur l'icône <b>Calendrier</b> pour indiquer une plage de dates supérieure à une journée. La durée maximale que vous pouvez sélectionner est de 30 jours à tout moment au cours de la dernière année.

Répartition des catégories de risque	Catégories de risque de niveau élevé au cours de la dernière heure. Cliquez sur le graphique pour afficher les sous-catégories puis cliquez pour afficher un écran des événements.
Utilisateurs avec comptes dormants	Liste de surveillance des utilisateurs repérés comme ayant des comptes dormants (ou inactifs). Cette liste est générée automatiquement. Disponible dans les versions 3.2.0 et ultérieures.
Examens en cours	Utilisateurs actuellement en cours d'examen. Cochez la case <b>Mes examens</b> pour afficher uniquement les examens que vous avez lancés. Disponible dans les versions 2.7.0 et ultérieures.
Statut des modèles Machine Learning	Le statut de Machine Learning Analytics est visible si l'application Machine Learning est installée. Pour plus d'informations, voir «Tableau de bord UBA avec Machine Learning Analytics», à la page 194.

## Page Détails de l'utilisateur

Vous pouvez cliquer sur un nom d'utilisateur n'importe où dans l'application afin d'afficher des détails sur l'utilisateur sélectionné.

Vous pouvez en savoir plus sur les activités de l'utilisateur grâce au volet *Afficheur d'événements*. Le volet Afficheur d'événements contient des informations sur une activité sélectionnée ou un moment. Si vous cliquez sur le volet *Afficheur d'événements*, des informations supplémentaires, comme des événements syslog et des informations de contenu, s'affichent. Le volet Afficheur d'événements est disponible pour tous les graphiques en anneau et linéaires de la page Détails de l'utilisateur.

La page Détails de l'utilisateur inclut les informations utilisateur suivantes :

- Affiche le nom et les alias de l'utilisateur sélectionné, ainsi que tous détails complémentaires tirés des attributs importés de LDAP.
- Dans les versions 3.2.0 et ultérieures, il est possible de voir l'état (dormant, actif, jamais utilisé) de tous les comptes qui se trouvent être associés à l'utilisateur.
- Si QRadar Advisor with Watson V1.13.0 (ou version ultérieure) est installé, vous pouvez rechercher des informations sur l'utilisateur. Vous devez avoir les privilèges d'administrateur QRadar. Cliquez sur l'icône **Rechercher dans Watson**. (Disponible dans la version 2.7.0 ou ultérieure.)
- Pour lancer un examen de l'utilisateur, cliquez sur l'icône **Commencer l'examen** . Une fois, l'examen terminé, cliquez sur l'icône **Terminer l'examen**. (Disponible dans la version 2.7.0 ou ultérieure.)
- Pour ajouter un utilisateur à une liste de surveillance ou créer une liste de surveillance, cliquez sur

l'icône **Liste de surveillance** .

La liste **Options avancées** inclut les actions suivantes :

<b>Ajouter une alerte personnalisée</b>	Vous pouvez définir une alerte personnalisée qui s'affiche par nom d'utilisateur. Cliquez sur <b>Ajouter une alerte personnalisée</b> , entrez un message d'alerte, puis cliquez sur <b>Définir</b> . Pour retirer l'alerte personnalisée pour l'utilisateur sélectionné, cliquez sur <b>Supprimer une alerte personnalisée</b> .
<b>Ajouter à la liste blanche</b>	Vous devez avoir les privilèges d'administrateur QRadar. Vous pouvez ajouter l'utilisateur sélectionné à la liste blanche afin qu'il ne génère aucun score de risque ou aucune infraction. Pour supprimer l'utilisateur sélectionné de la liste blanche, cliquez sur <b>Sur liste blanche</b> . Pour consulter la liste complète des utilisateurs ayant été ajoutés à la liste blanche, voir «Affichage de la liste blanche pour les utilisateurs de confiance», à la page 39.

<b>Générer un rapport conforme au RGPD pour l'utilisateur</b>	Vous pouvez générer un rapport de conformité RGPD (Règlement général sur la protection des données) pour l'utilisateur. <b>Important :</b> Effectuez cette action avant de cliquer sur <b>Supprimer l'utilisateur et arrêter de le suivre</b> .
<b>Supprimer l'utilisateur et arrêter de le suivre</b>	Vous devez avoir les privilèges d'administrateur QRadar. Vous pouvez cliquer sur <b>Supprimer l'utilisateur et arrêter de le suivre</b> pour vous conformer à la réglementation RGPD (Règlement général sur la protection des données). Sélectionnez <b>Oui</b> pour supprimer l'utilisateur et arrêter de le suivre de manière définitive. Pour commencer à suivre à nouveau l'utilisateur, supprimez ses alias dans l'ensemble de référence <b>UBA : Users Not Tracked</b> . Pour afficher tous les alias de l'utilisateur, téléchargez le rapport RGPD avant de supprimer l'utilisateur.
<b>Toujours suivre avec Machine Learning</b>	Vous devez avoir les privilèges d'administrateur QRadar. Cliquez sur <b>Toujours suivre avec Machine Learning</b> si vous voulez ajouter l'utilisateur à l'ensemble de référence <b>UBA : ML Always Tracked Watchlist</b> . En ajoutant l'utilisateur à cet ensemble de référence, vous avez toutes les chances que cet utilisateur soit inclus dans un modèle d'apprentissage automatique (ML). Pour plus d'informations sur les ensembles de référence dans UBA, consultez «Ensembles de référence», à la page 45. Pour retirer l'utilisateur sélectionné de l'ensemble de référence, cliquez sur <b>Suivi avec Machine Learning</b> . <b>Remarque :</b> Disponible dans la version 2.8.0 ou ultérieure et seulement si Machine Learning est installée et si vous avez les privilèges d'administrateur QRadar.

Vous pouvez consulter les informations suivantes sur l'utilisateur sélectionné :

Score de risque global	Le graphique de score de risque global présente les tendances du risque pour l'utilisateur.
Ligne de temps	Le graphique de la ligne de temps affiche les Événements à risque et les Événements utilisateur. Les événements à risque sont des événements de risque qui contribuent au score du risque. Les événements de utilisateur sont des événements non à risque. L'axe des Y représente le nombre d'événements et l'axe des X le temps. Vous pouvez cliquer sur une activité du diagramme pour ouvrir le volet Afficheur d'événements qui répertorie les événements du journal de prise en charge associés à l'activité de l'utilisateur. Cliquez sur un événement pour afficher des détails supplémentaires sur les événements syslog et les informations de contenu. <ul style="list-style-type: none"> <li>• Dans la version 2.8.0 et les versions antérieures, vous pouvez cliquer sur <b>Grouper par activité</b> ou sur <b>Grouper par heure</b> pour afficher une liste des activités de l'utilisateur, puis filtrer par colonne du diagramme et effectuer une recherche.</li> <li>• A partir de la version 3.0.0 et dans les versions suivantes, l'activité au fil du temps est regroupée par sessions et jours. Les sessions sont définies dans la section Paramètres de l'application de la page <b>Paramètres UBA</b>. Les couleurs représentent le niveau de risque global d'une session. Cliquez sur l'icône <b>Calendrier</b> pour indiquer la plage de dates (1 à 14 jours).</li> <li>• Dans les versions 3.1.0 et ultérieures, vous pouvez personnaliser les métriques affichées sur la ligne de temps en cliquant sur l'icône <b>Métriques</b>. Vous pouvez ajouter les catégories que vous souhaitez voir et retirer celles que vous ne souhaitez pas voir. Les données visibles dans la section Exemples de métriques de l'écran Métriques ne représentent pas de vraies valeurs. <b>Remarque :</b> Les mêmes données sont affichées pour "Événements à risque" et "Cas d'utilisation" lorsque "Événements à risque" est le nombre total d'événements pour les cas d'utilisation indiqués. Les mêmes données sont affichées pour "Catégories d'URL" et "URL" lorsque "URL" est le nombre total d'événements pour les catégories d'URL indiquées. Les mêmes données sont affichées pour "ID d'événements" et "Événements" lorsque "Événements" est le nombre total d'événements pour les ID d'événements indiqués.</li> </ul>
Infractions récentes	Affiche les infractions de type utilisateur où le nom d'utilisateur correspond à un des alias de l'utilisateur sélectionné. Les cinq dernières infractions sont affichées. Cliquez sur une infraction pour ouvrir l'onglet <b>Infractions</b> dans QRadar.

Répartition des catégories de risque	Affiche les catégories de risque de l'utilisateur sélectionné au cours de la dernière heure.
Ajouter des remarques	<p>Cliquez sur l'icône <b>Ajouter</b>  afin d'ajouter des remarques pour l'utilisateur sélectionné. Les remarques sont supprimées automatiquement après une période de conservation de 30 jours.</p> <p><b>Conseil :</b> Pour enregistrer la remarque de manière indéfinie, marquez-la comme étant importante en cliquant sur l'icône représentant un <b>drapeau</b>.</p>

Les graphiques suivants sont affichés sur la page Détails de l'utilisateur si l'application Machine Learning est installée et si les analyses correspondantes sont activées. Pour plus d'informations, voir «Tableau de bord UBA avec Machine Learning Analytics», à la page 194.

Activité totale	Affiche, heure par heure, le nombre d'activités réelles et apprises des utilisateurs au cours de la journée.
Activité utilisateur par catégorie	Affiche les schémas comportementaux des activités utilisateur réelles et attendues par catégorie de niveau supérieur.
Degré d'exposition au risque	S'affiche lorsque le score de risque d'un utilisateur est différent du schéma de score de risque attendu.
Tentatives de transfert sortant anormales	Montre la part d'utilisation de trafic sortant par chaque utilisateur et les alertes pour comportement anormal. Notez que le graphique de cette analyse n'est pas activé par défaut. L'analyse Tentatives de transfert sortant anormales est visible sur le tableau de bord seulement si l'application Machine Learning est installée, si l'analyse est activée et si l'option <b>Afficher le graphique sur la page Détails de l'utilisateur</b> est sélectionnée dans les paramètres Machine Learning. Disponible dans la version 2.8.0 ou ultérieure.
Volume anormal de données circulant vers des domaines externes	Montre l'utilisation des données de domaines externes pour chaque utilisateur et les alertes pour comportement anormal. L'analyse Volume anormal de données circulant vers des domaines externes est visible sur le tableau de bord seulement si l'application Machine Learning est installée, si l'analyse est activée et si l'option <b>Afficher le graphique sur la page Détails de l'utilisateur</b> est sélectionnée dans les paramètres Machine Learning. Disponible dans la version 3.0.0 ou les versions suivantes.
Distribution de l'activité	Affiche les clusters de comportement dynamique pour tous les utilisateurs surveillés par l'application Machine Learning. Disponible dans la version 2.2.0 ou ultérieure.
Groupe d'homologues enregistré	Présente dans quelle mesure l'utilisateur diffère du groupe d'homologues déduit dans lequel il était supposé être. Disponible dans la version 2.2.0 ou ultérieure.
Groupe d'homologues défini	Affiche l'écart entre l'activité d'un utilisateur (en termes d'événements) et celle de son groupe d'homologues défini. Disponible dans la version 2.6.0 ou ultérieure.

Pour retourner au tableau de bord principal, cliquez sur **Tableau de bord**.

#### Concepts associés:

«Tableau de bord UBA avec Machine Learning Analytics», à la page 194

L'application IBM QRadar User Behavior Analytics (UBA) avec Machine Learning Analytics inclut le statut Machine Learning Analytics ainsi que des détails supplémentaires relatifs à l'utilisateur sélectionné.

«Comptes dormants», à la page 41

Vous pouvez voir les utilisateurs de votre système qui ont des comptes dormants, des comptes actifs ou des comptes qui n'ont jamais servi.

#### Tâches associées:

«Création de listes de surveillance», à la page 37

Vous pouvez ajouter un utilisateur à une liste de surveillance nouvelle ou existante.

«Affichage de la liste blanche pour les utilisateurs de confiance», à la page 39

Vous pouvez consulter la liste des utilisateurs de confiance (liste blanche) dans la liste de gestion de

l'ensemble de références.

«Ajout de sources de journaux au groupe de sources de journaux de confiance», à la page 41  
Si vous ne souhaitez pas que certaines sources de journaux fassent l'objet d'une surveillance et d'un rapport par l'application UBA, vous pouvez les ajouter à **UBA : Trusted Log Source Group**. L'ajout de sources de journaux au groupe empêche leur surveillance par l'application UBA.

«Installation de l'application Machine Learning Analytics», à la page 176  
Installez l'application Machine Learning Analytics après l'installation de l'application UBA à partir de l'outil Extension Manager.

«Examen d'utilisateurs dans QRadar Advisor with Watson»  
Vous pouvez sélectionner des utilisateurs dans l'application User Behavior Analytics (UBA) et les transférer dans QRadar Advisor with Watson afin qu'ils soient examinés.

---

## Examen d'utilisateurs dans QRadar Advisor with Watson

Vous pouvez sélectionner des utilisateurs dans l'application User Behavior Analytics (UBA) et les transférer dans QRadar Advisor with Watson afin qu'ils soient examinés.

### Avant de commencer

- L'application User Behavior Analytics (UBA) version 2.7.0 ou ultérieure doit être installée et configurée avec des données utilisateur.
- Vous devez avoir des privilèges admin.
- QRadar Advisor with Watson version 1.13.0 ou ultérieure doit être installé.

Pour plus d'informations, voir <https://developer.ibm.com/qradar/advisor>.

### Pourquoi et quand exécuter cette tâche

**Remarque :** Cette fonction est disponible uniquement dans User Behavior Analytics V2.7.0 et versions ultérieures et dans QRadar Advisor with Watson V1.13.0 et versions ultérieures.

### Procédure

1. Cliquez sur **Analyse utilisateur** pour ouvrir le Tableau de bord UBA.
2. Sélectionnez ou recherchez un utilisateur pour ouvrir la page Détails de l'utilisateur.
3. Cliquez sur l'icône **Rechercher dans Watson**. Lorsque l'icône s'arrête de tourner, vous pouvez consulter vos résultats dans l'application QRadar Advisor with Watson.
4. Sur la page Présentation de l'incident de l'onglet **Watson**, sélectionnez l'examen d'utilisateur. Les examens d'utilisateur sont marqués par une icône indiquant que l'examen a été démarré à partir

d'UBA  .

---

## Conditions préalables à l'installation de l'application User Behavior Analytics

Avant d'installer l'application User Behavior Analytics (UBA), vérifiez que les conditions préalables sont respectées.

- Vérifiez qu'IBM Security QRadar V7.2.8 ou version ultérieure est installé.  
Pour la meilleure expérience possible, mettez à jour votre système QRadar vers les versions suivantes :
  - QRadar 7.2.8 correctif 13 (7.2.8.20180529210357) ou version ultérieure
  - QRadar 7.3.1 correctif 6 (7.3.1.20180912181210) ou version ultérieure
- Installez les packages de contenu à partir d'IBM App Exchange
- Ajoutez IBM Sense DSM pour User Behavior Analytics (UBA).

## Dépendances vis-à-vis du contenu

Plusieurs règles sont conçues pour alimenter UBA avec les événements d'autres applications. Pour fonctionner correctement, ces règles nécessitent que le contenu des autres applications soit installé.

Pour plus d'informations sur le contenu UBA et les applications requises, consultez le tableau suivant.

Contenu UBA	Applications requises
«QRadar DNS Analyzer», à la page 131	IBM QRadar DNS Analyzer
UBA QRadar Network Insights	QRadar Network Insights Content v7.2.8 QRadar Network Insights Content for V7.3.0+
Reconnaissance	IBM Security Reconnaissance Content
Surveillance du système (Sysmon)	IBM QRadar Content for Sysmon

**Remarque :** Si vous éditez ces règles, il est possible qu'elles ne fonctionnent plus comme prévu.

## Installation manuelle d'IBM Sense

L'application User Behavior Analytics (UBA) utilise IBM Sense DSM pour ajouter des scores de risque utilisateur et des infractions dans QRadar. Vous pouvez installer DSM par le biais des mises à jour automatiques ou effectuer un chargement vers QRadar et l'installer manuellement.

**Remarque :** Si votre système n'est pas connecté à Internet, vous devrez peut-être installer RPM DSM manuellement.

**Restriction :** La désinstallation d'un module de support de périphérique (DSM) n'est pas prise en charge dans QRadar.

1. Téléchargez le fichier DSM RPM à partir du site Web de support IBM.
  - Pour QRadar version 7.2.8 : DSM-IBMSense-7.2-20180814101121.noarch.rpm
  - Pour QRadar versions 7.3.0 et ultérieures : DSM-IBMSense-7.3-20180814141146.noarch.rpm
2. Copiez le fichier RPM sur votre console QRadar Console.
3. Utilisez SSH pour vous connecter à l'hôte QRadar en tant qu'utilisateur root.
4. Accédez au répertoire contenant le fichier téléchargé.
5. Entrez la commande suivante :  
`rpm -Uvh <nom-fichier_rpm>`
6. Dans les paramètres **Admin**, cliquez sur **Déployer les modifications**.
7. Dans les paramètres **Admin**, sélectionnez **Avancé** > **Redémarrer le serveur Web**.

---

## Navigateurs pris en charge pour l'application User Behavior Analytics

Pour que les produits IBM Security QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Le tableau ci-après répertorie les versions prises en charge des navigateurs Web.

Navigateur Web	Versions prises en charge
Mozilla Firefox	45.2 Extended Support Release
Google Chrome	Dernière version

**Remarque :** Pour optimiser votre expérience UBA, effectuez une des actions suivantes :

- Désactivez le logiciel de blocage d'incrustation pour votre navigateur.
- Configurez votre navigateur de telle sorte qu'il autorise des exceptions pour les fenêtres pop-up en provenance de l'adresse IP de QRadar Console.

---

## Types de sources de journaux liés à l'application User Behavior Analytics

Les applications User Behavior Analytics (UBA) et ML peuvent accepter et analyser des événements à partir de certaines sources de journaux.

En général, les application UBA et ML nécessitent que des sources de journaux fournissent un nom d'utilisateur. Pour UBA, s'il n'y a pas de nom d'utilisateur, cochez la case **Rechercher des actifs pour un nom d'utilisateur, lorsque celui-ci n'est pas disponible dans les données d'événement ou de flux** dans les paramètres UBA afin qu'UBA puisse tenter de rechercher l'utilisateur dans la table des actifs. Si aucun utilisateur ne peut être déterminé, UBA ne traite pas l'événement.

Pour plus de détails sur des scénarios d'utilisation spécifiques et les types de source de journaux correspondants, voir 7, «Règles et réglages pour l'application UBA», à la page 47.

### Tâches associées:

«Configuration des paramètres UBA», à la page 28

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres de l'application UBA.

---

## 2 Installation et désinstallation

---

### Installation de l'application User Behavior Analytics

Utilisez l'outil Gestion des extensions d'IBM QRadar pour charger et installer directement votre archive d'application dans QRadar Console.

#### Avant de commencer

Effectuez la procédure «Conditions préalables à l'installation de l'application User Behavior Analytics», à la page 14.

**Important :** Avant d'installer l'application, assurez-vous qu'IBM QRadar remplit les conditions de mémoire (RAM) minimum. L'application UBA nécessite 1 Go de mémoire libre dans le pool de mémoire réservé aux applications. Elle ne sera pas installée si le pool réservé aux applications n'a pas suffisamment de mémoire libre.

#### Pourquoi et quand exécuter cette tâche

L'installation a changé à compter de l'introduction de la V2.8.0. Les packages de contenu UBA, qui comprennent les règles de déclenchement des infractions, sont à présent installés sous forme d'extensions séparées. Ils sont installés par défaut. Si vous choisissez de créer vos propres règles personnalisées pour le déclenchement des infractions, vous pouvez changer le réglage de l'option **Installer et mettre à niveau les packages de contenu UBA** (cochée par défaut) lorsque vous configurez les paramètres UBA.

**Avertissement :** Une fois l'application installée, vous devez :

- activer les index
- déployer la configuration complète.
- vider le cache de votre navigateur et actualiser la fenêtre du navigateur.
- configurer les droits pour les utilisateur ayant besoin de consulter l'onglet Analyse utilisateur. Les droits suivants doivent être affectés à chaque rôle utilisateur ayant besoin d'accéder à l'application :
  - Analyse utilisateur
  - Infractions
  - Activité du journal

Une fois que vous avez téléchargé votre application depuis IBM Security App Exchange, utilisez l'outil Gestion des extensions d'IBM QRadar pour effectuer l'installation sur QRadar Console.

#### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Configuration système > Gestion des extensions**.
3. Dans la fenêtre Gestion des extensions, cliquez sur **Ajouter** et sélectionnez l'archive de l'application UBA que vous voulez télécharger vers la console.
4. Cochez la case **Installer immédiatement** et cliquez sur **Ajouter**.
5. A l'invite, sélectionnez **Remplacer**.

**Important :** Vous devrez peut-être patienter plusieurs minutes avant que votre application devienne active. Une fois l'application UBA installée, les packages de contenu sont installés en arrière-plan. Il est donc possible que le contenu ne soit pas visible immédiatement dans QRadar.

6. Dans les paramètres **Admin**, cliquez sur **Configuration système** > **Gestion de l'index** puis activez les index suivants :
  - Catégorie de niveau supérieur
  - Catégorie de niveau inférieur
  - Nom d'utilisateur
  - senseValue
7. Dans les paramètres **Admin**, cliquez sur **Avancé** > **Déployer la configuration entière**.

**Remarque :** Les packages de contenu suivants sont installés une fois l'application UBA installée et configurée.

- User Behavior Analytics Access and Authentication Content
- User Behavior Analytics Accounts and Privileges Content
- User Behavior Analytics Browsing Behavior Content
- User Behavior Analytics DNS Analyzer Content
- User Behavior Analytics Endpoint Content
- User Behavior Analytics Exfiltration Content
- User Behavior Analytics Geography Content
- User Behavior Analytics Network Traffic and Attacks Content
- User Behavior Analytics QRadar Network Insights Content
- User Behavior Analytics Reconnaissance Content
- User Behavior Analytics Sysmon Content
- User Behavior Analytics Threat Intelligence Content

## Que faire ensuite

- Une fois l'installation terminée, videz le cache de votre navigateur et actualisez la fenêtre de navigateur avant d'utiliser l'application.
- Gérez les droits pour les rôles utilisateur de l'application UBA.

### Tâches associées:

«Activation des index pour l'amélioration des performances», à la page 43

Pour améliorer les performances de votre application IBM QRadar User Behavior Analytics (UBA), activez les index dans IBM QRadar.

«Gestion des droits de l'application UBA de QRadar», à la page 37

Les administrateurs utilisent la fonction User Role Management fournie dans IBM QRadar pour configurer et gérer les comptes utilisateurs. En tant qu'administrateur, vous devez activer les droits Analyse utilisateur, Infractions et Activité du journal pour chaque rôle d'utilisateur autorisé à utiliser l'application UBA de QRadar.

---

## Désinstallation de l'application User Behavior Analytics

L'outil Gestion des extensions d'IBM QRadar vous permet de désinstaller votre application dans QRadar Console.

### Avant de commencer

Si l'application Machine Learning Analytics (ML) est installée, vous devez la désinstaller à partir de la page Paramètres Machine Learning avant de désinstaller l'application UBA à partir de la fenêtre Gestion des extensions. Si vous ne retirez pas l'application ML avant de désinstaller UBA, vous devez la

retirer à partir de l'interface de la documentation d'API interactive.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Gestion des extensions**.
3. Sous l'onglet **INSTALLÉ** de la fenêtre Gestion des extensions, sélectionnez l'application User Behavior Analytics et cliquez sur **Désinstaller**.

Lorsque vous désinstallez une application, elle est retirée du système. Si vous souhaitez la réinstaller, vous devez l'ajouter à nouveau.
4. A compter de la version 2.8.0, les packages de contenu suivants sont installés lorsque vous configurez l'application UBA. Pour supprimer entièrement l'application, vous devez désinstaller chaque package de contenu.
  - User Behavior Analytics Access and Authentication Content
  - User Behavior Analytics Accounts and Privileges Content
  - User Behavior Analytics Browsing Behavior Content
  - User Behavior Analytics DNS Analyzer Content
  - User Behavior Analytics Endpoint Content
  - User Behavior Analytics Exfiltration Content
  - User Behavior Analytics Geography Content
  - User Behavior Analytics Network Traffic and Attacks Content
  - User Behavior Analytics QRadar Network Insights Content
  - User Behavior Analytics Reconnaissance Content
  - User Behavior Analytics Sysmon Content
  - User Behavior Analytics Threat Intelligence Content



---

## 3 Mise à niveau

---

### Mise à niveau de l'application User Behavior Analytics

L'outil Gestion des extensions d'IBM QRadar vous permet de mettre à niveau votre application.

#### Avant de commencer

**Important :** Les besoins en mémoire ont augmenté à partir de la version 2.8.0. Avant de mettre à niveau l'application, assurez-vous qu'IBM QRadar remplit les conditions de mémoire (RAM) minimum. L'application UBA nécessite 1 Go de mémoire libre dans le pool de mémoire réservé aux applications. Elle ne sera pas mise à niveau si le pool réservé aux applications n'a pas suffisamment de mémoire libre.

Pour la meilleure expérience possible, mettez à jour votre système QRadar vers les versions suivantes :

- QRadar 7.2.8 correctif 13 (7.2.8.20180529210357) ou version ultérieure
- QRadar 7.3.0 correctif 7 (7.3.0.20171205025101) ou version ultérieure
- QRadar 7.3.1 correctif 6 (7.3.1.20180912181210) ou version ultérieure

#### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur **Gestion des extensions**.
3. Dans la fenêtre Gestion des extensions, cliquez sur **Ajouter** et sélectionnez l'archive de l'application UBA que vous voulez charger sur la console.
4. A l'invite, sélectionnez **Remplacer**. Toutes vos données existantes de l'application UBA restent intactes.

**Important :** Vous devrez peut-être patienter plusieurs minutes avant que votre application devienne active. Une fois l'application UBA mise à niveau, les packages de contenu sont mis à niveau en arrière-plan. Il est donc possible que le contenu ne soit pas visible immédiatement dans QRadar.

**Remarque :** Les packages de contenu suivants sont mis à niveau une fois l'application UBA mise à niveau et configurée.

- User Behavior Analytics Access and Authentication Content
- User Behavior Analytics Accounts and Privileges Content
- User Behavior Analytics Browsing Behavior Content
- User Behavior Analytics DNS Analyzer Content
- User Behavior Analytics Endpoint Content
- User Behavior Analytics Exfiltration Content
- User Behavior Analytics Geography Content
- User Behavior Analytics Network Traffic and Attacks Content
- User Behavior Analytics QRadar Network Insights Content
- User Behavior Analytics Reconnaissance Content
- User Behavior Analytics Sysmon Content
- User Behavior Analytics Threat Intelligence Content

## **Que faire ensuite**

Une fois la mise à niveau terminée, videz le cache de votre navigateur et actualisez la fenêtre de navigateur avant d'utiliser l'application.

---

## 4 Configuration

---

### Configuration de l'application User Behavior Analytics

Avant d'utiliser l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer des paramètres de configuration supplémentaires.

Lors de l'installation de l'application UBA, l'application IBM QRadar Reference Data Import LDAP (LDAP) est également installée. Si vous choisissez d'utiliser l'application LDAP, vous devez la configurer avant de configurer l'application UBA. Les données utilisées par l'application UBA proviennent d'une requête LDAP. La requête LDAP extrait la liste des utilisateurs qui est utilisée pour alimenter l'application UBA.

Les applications UBA et LDAP requièrent des jetons d'autorisation séparés. Vous pouvez les créer au moment où vous configurez chaque application.

Effectuez les procédures de configuration suivantes :

- Configurez l'application Reference Data Import - LDAP si vous utilisez LDAP
- Configurez les paramètres UBA pour l'application UBA

### Configuration de l'application Reference Data Import - LDAP

L'installation de l'application User Behavior Analytics (UBA) d'IBM® QRadar® installe également l'application Reference Data Import - LDAP. Vous pouvez utiliser l'application LDAP pour importer des données d'utilisateurs dans une table de référence QRadar à partir d'un serveur LDAP/AD ou d'un fichier CSV. La table de référence est alors consommée par l'application UBA, ou bien elle peut servir aux recherches ou aux règles QRadar.

#### Avant de commencer

**Avertissement :** Si vous avez précédemment installé l'application Reference Data Import - LDAP autonome, elle est remplacée lors de l'installation de l'application UBA. Vos configurations sont ajoutées à la version mise à jour de l'application Reference Data Import - LDAP.

#### Pourquoi et quand exécuter cette tâche

**Remarque :** Assurez-vous d'avoir noté le nom de la table de référence et vérifiez si vous avez affecté un alias personnalisé à des attributs. Lors de la configuration de l'application UBA, sélectionnez la table de référence que vous avez créée dans l'application Reference Data Import - LDAP.

Pour plus d'informations sur l'application Reference Data Import - LDAP, consultez la section suivante du site IBM Knowledge Center : [http://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.2.8/com.ibm.apps.doc/c\\_Qapps\\_LDAP\\_intro.html](http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.apps.doc/c_Qapps_LDAP_intro.html)

#### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Importation des données de référence - LDAP**.

- Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres UBA**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Importation des données de référence - LDAP > Importation des données de référence - LDAP**.
3. Cliquez sur **Configurer** pour créer un jeton de service autorisé pour LDAP. La boîte Configuration d'un jeton de service autorisé s'ouvre.
    - a. Cliquez sur le lien **Gérer les services autorisés**, puis sur **Ajouter un service autorisé**.
    - b. Dans la zone **Nom du service**, entrez LDAP. C'est sous ce nom d'utilisateur que seront exécutées les demandes d'API émises par l'application LDAP.
    - c. Dans la liste **Rôle utilisateur**, sélectionnez le rôle utilisateur **Admin**.
    - d. Dans la liste **Profil de sécurité**, sélectionnez le profil de sécurité à affecter à ce service autorisé. Le profil de sécurité détermine les réseaux et les sources de journaux auxquels peut accéder ce service dans l'interface utilisateur de QRadar.
    - e. Dans la liste **Date d'expiration**, entrez ou sélectionnez la date à laquelle ce service doit expirer. Si une date d'expiration n'est pas requise, sélectionnez **Pas d'expiration**.
    - f. Cliquez sur **Créer un service**.
    - g. Cliquez sur la ligne contenant le service LDAP que vous avez créé, puis sélectionnez et copiez la chaîne de jeton de la zone **Jeton sélectionné** dans la barre de menu.
    - h. Dans la boîte Configurer un jeton de service autorisé, collez la chaîne du jeton de service autorisé dans la zone **Jeton**.
  4. Facultatif : Pour ajouter un fichier d'autorité de certification racine privé, cliquez sur **Parcourir les fichiers**, ouvrez un fichier pris en charge, cliquez sur **Ouvrir**, puis sur **Télécharger**. Le type de fichier .pem est pris en charge.
  5. Cliquez sur **OK**.

**Configure Authorized Service Token**

Enter a valid QRadar authorized service token

Token

[Manage Authorized Services](#)

To add a private root CA, upload a .pem file.

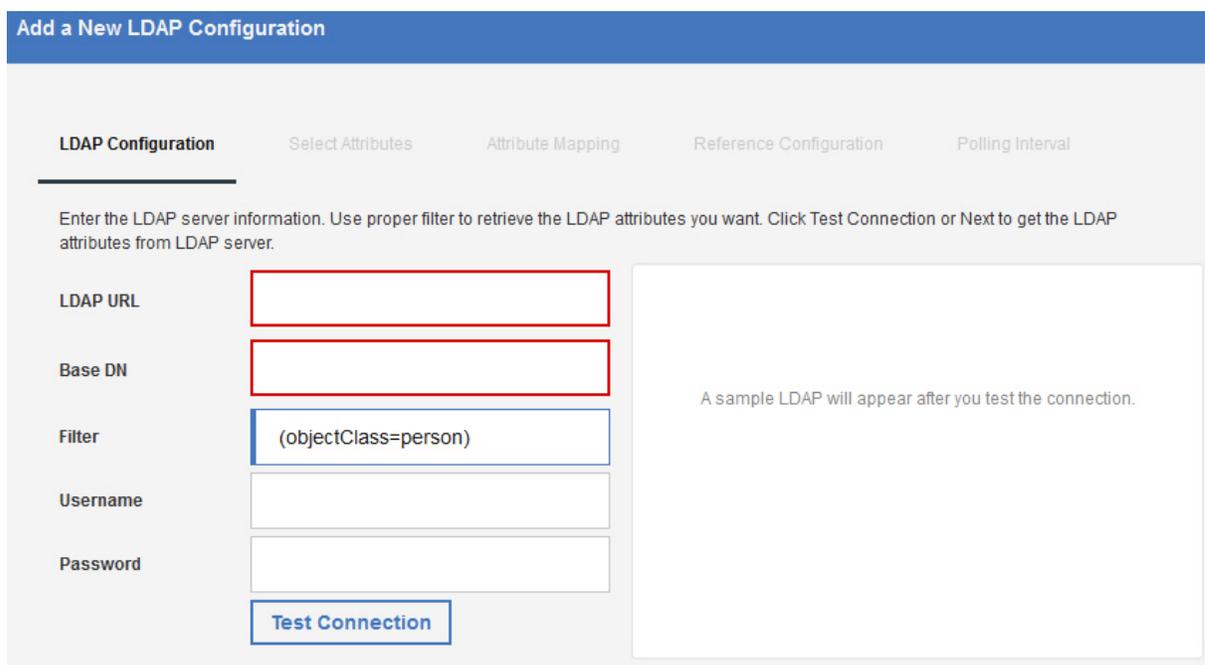
Private Root CA

[Browse files...](#)

[Upload](#)

[Ok](#) [Cancel](#)

6. Dans la fenêtre principale de l'application Importation des données de référence (LDAP), cliquez sur **Ajouter une importation**. La boîte de dialogue de configuration Ajouter une nouvelle configuration LDAP s'affiche.
7. Dans l'onglet **Configuration LDAP**, ajoutez des informations de connexion pour le serveur LDAP. La zone **Filtre** est automatiquement renseignée en fonction de vos attributs Active Directory.
  - a. Entrez une URL qui commence par `ldap://` ou `ldaps://` (pour TLS) dans la zone **URL LDAP**.
  - b. Entrez le point dans l'arborescence de l'annuaire LDAP à partir duquel le serveur doit rechercher des utilisateurs dans la zone **Nom distinctif de base**. Par exemple, si votre serveur LDAP se trouvait dans le domaine `example.com`, vous pouvez utiliser `:dc=example,dc=com`.
  - c. Entrez l'attribut ou les attributs que vous souhaitez utiliser pour trier les données qui sont importées dans la table de référence, dans la zone **Filtre**. Par exemple, `cn=*; uid=*; sn=*`. Les valeurs par défaut suivantes fonctionnent avec Active Directory : `(&(sAMAccountName=*)(samAccountType=805306368))`.
  - d. Entrez le nom d'utilisateur qui est utilisé pour authentifier le serveur LDAP dans la zone **Nom d'utilisateur**.
  - e. Entrez le mot de passe du serveur LDAP dans la zone **Mot de passe**.
8. Cliquez sur **Tester la connexion** ou **Suivant** pour vérifier qu'IBM QRadar peut se connecter au serveur LDAP. Si votre tentative de connexion aboutit, les informations de votre serveur LDAP sont affichées sous l'onglet **Configuration LDAP**.



**Add a New LDAP Configuration**

LDAP Configuration    Select Attributes    Attribute Mapping    Reference Configuration    Polling Interval

Enter the LDAP server information. Use proper filter to retrieve the LDAP attributes you want. Click Test Connection or Next to get the LDAP attributes from LDAP server.

LDAP URL

Base DN

Filter

Username

Password

A sample LDAP will appear after you test the connection.

9. Sous l'onglet **Sélectionner des attributs**, choisissez les attributs que vous voulez extraire du serveur LDAP. Les valeurs par défaut suivantes fonctionnent avec Active Directory : `userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.

LDAP Configuration    **Select Attributes**    Attribute Mapping    Reference Configuration    Polling Interval

Select the attributes to extract from the LDAP server. By default, the attributes are sorted by the Extract column. Suggested attributes are marked with an asterisk (\*).

Search  LDAP attributes discovered: 7

Extract	LDAP Attribute	Sample
<input checked="" type="checkbox"/>	* cn	Zadulemaraedeth <a href="#">more</a>
<input checked="" type="checkbox"/>	gidNumber	6000
<input checked="" type="checkbox"/>	homeDirectory	/home/Zadulemaraedeth <a href="#">more</a>
<input checked="" type="checkbox"/>	loginShell	/bin/bash
<input checked="" type="checkbox"/>	objectClass	account <a href="#">more</a>
<input checked="" type="checkbox"/>	* uid	Zadulemaraedeth <a href="#">more</a>
<input checked="" type="checkbox"/>	uidNumber	81 <a href="#">more</a>

10. Facultatif : Sous l'onglet **Mappage d'attributs**, spécifiez la clé pour la table de référence.

**Conseil :** Vous pouvez créer de nouveaux champs LDAP en cliquant sur **Ajouter** et en combinant deux attributs. Par exemple, vous pouvez utiliser la syntaxe suivante : "Last: {ln}, First: {fn}".

**Conseil :** Si vous souhaitez fusionner des données LDAP provenant de plusieurs sources dans la même table de référence, vous pouvez utiliser des alias personnalisés pour distinguer les attributs LDAP portant le même nom dans les différentes sources.

LDAP Configuration    Select Attributes    **Attribute Mapping**    Reference Configuration    Polling Interval

Set the key for the reference table. The key should uniquely identify the LDAP users. Attributes can also be renamed. **Add**

Optional: New LDAP fields can be created by combining attributes. For example: "{domain}{cn}".

LDAP Attribute ⓘ	Alias ⓘ	Key ⓘ
uid ex: Zadulemaraedeth	TESTING-UID	<input type="radio"/>
objectClass ex: account	OBJECTION	<input type="radio"/>
loginShell ex: /bin/bash	Login	<input type="radio"/>
uidNumber ex: 81	UID	<input type="radio"/>
gidNumber ex: 6000	GIDNum	<input type="radio"/>
homeDirectory ex: /home/Zadulemaraedeth	HomeDir	<input type="radio"/>
cn	Common User Name	<input checked="" type="radio"/>

11. Sous l'onglet **Configuration de référence**, créez une nouvelle mappe de mappes de référence ou indiquez une mappe existante à laquelle vous voulez ajouter les données LDAP.

a. Dans la zone **Table de référence**, entrez le nom d'une nouvelle table de référence. Vous pouvez également ajouter le nom d'une table de référence existante à laquelle ajouter les données LDAP de la liste.

- b. La case à cocher **Générer une mappe d'ensembles** est désactivée par défaut. Si vous l'activez, des données au format d'ensemble de référence sont envoyées afin d'améliorer la recherche QRadar. Cela peut avoir des conséquences sur les performances.
- c. Dans la section **Durée de vie**, définissez la durée pendant laquelle les données doivent demeurer dans la mappe de références des mappes. Par défaut, les données que vous ajoutez n'arrivent jamais à expiration. Lorsque la période de durée de vie est dépassée, un événement *ReferenceDataExpiry* est déclenché.

**Remarque :** Si vous ajoutez des données à une mappe de références de mappes existante, l'application utilise les paramètres de durée de vie d'origine. Ces paramètres ne peuvent pas être remplacés sous l'onglet **Configuration de référence**.

- 12. Sous l'onglet **Interrogation**, définissez la fréquence à laquelle l'application doit interroger votre serveur LDAP.

- a. Dans la zone **Intervalle d'interrogation en minutes**, définissez, en minutes, à quel intervalle vous voulez que l'application interroge votre serveur LDAP.

**Remarque :** La valeur de l'intervalle d'interrogation minimal est 120. Vous pouvez aussi entrer une intervalle d'interrogation égal à zéro. Dans ce cas, vous devrez interroger l'application manuellement à l'aide de l'option d'interrogation affichée dans le flux.

- b. Dans la zone **Limite d'extraction des enregistrements**, entrez le nombre d'enregistrements que le processus d'interrogation doit retourner. Par défaut, 100 000 enregistrements sont renvoyés. Le nombre maximal d'enregistrements pouvant être retournés est 200 000.
- c. Facultatif : La case à cocher **Résultats paginés** est sélectionnée par défaut afin de ne pas limiter le nombre d'enregistrements renvoyés par le serveur LDAP pour chaque interrogation.

**Remarque :** Les résultats paginés ne sont pas pris en charge par tous les serveurs LDAP.

LDAP Configuration    Select Attributes    Attribute Mapping    Reference Configuration    **Polling Interval**

---

Enter a polling interval to retrieve your LDAP data. Enter "0" (zero) for manual polling.

Polling interval in minutes

Record retrieval limit

Paged results

Note: Not all servers support paged results.  
See [RFC2696](#) for details.

13. Cliquez sur **Sauvegarder**.

## Configuration des paramètres UBA

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres de l'application UBA.

### Configuration du jeton d'autorisation dans les paramètres QRadar

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer un jeton d'autorisation dans les paramètres UBA.

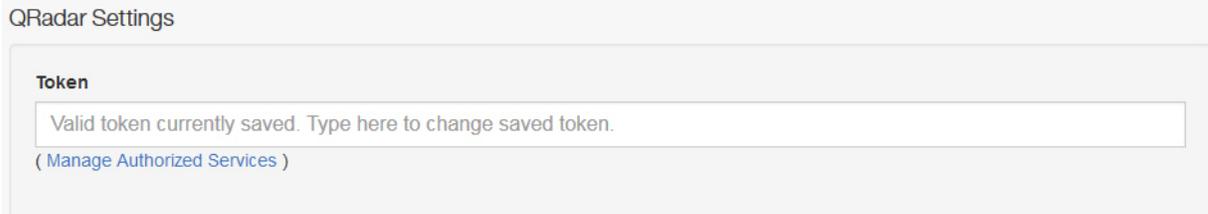
### Pourquoi et quand exécuter cette tâche

**Avertissement :** En raison de leurs capacités d'administration limitées, les administrateurs QRadar on Cloud ne peuvent pas créer de jeton de service autorisé pour les applications QRadar. Si vous êtes un client QRadar on Cloud, contactez le service clients afin qu'il crée pour vous un jeton de service autorisé.

Pour créer un jeton d'autorisation, vous devez effectuer les étapes suivantes. Ne sauvegardez pas la configuration tant que tous les paramètres UBA n'ont pas été configurés.

### Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres UBA**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres UBA**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres UBA**.
- Dans la section Paramètres QRadar, cliquez sur le lien **Gérer les services autorisés**.



4. Cliquez sur **Ajouter un service autorisé**
5. Dans la zone **Nom du service**, entrez UBA.
6. Dans la liste **Rôle utilisateur**, sélectionnez le rôle utilisateur **Admin**.
7. Dans la liste **Profil de sécurité**, sélectionnez le profil de sécurité à affecter à ce service autorisé. Le profil de sécurité détermine les réseaux et les sources de journaux auxquels peut accéder ce service dans l'interface utilisateur de QRadar.
8. Dans la liste **Date d'expiration**, entrez ou sélectionnez la date à laquelle ce service doit expirer. Si une date d'expiration n'est pas requise, sélectionnez **Pas d'expiration**.
9. Cliquez sur **Créer un service**.
10. Cliquez sur la ligne contenant le service UBA que vous avez créé, puis sélectionnez et copiez la chaîne de jeton de la zone **Jeton sélectionné** dans la barre de menu.
11. Retournez à la section Paramètres QRadar et collez la chaîne du jeton de service autorisé dans la zone **Jeton**.

## Que faire ensuite

«Configuration des paramètres des packages de contenu»

## Configuration des paramètres des packages de contenu

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres des packages de contenu.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres UBA**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres UBA**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres UBA**.
3. Dans la section Paramètres des packages de contenu, la case **Installer et mettre à niveau les packages de contenu UBA** est cochée par défaut. Décochez-la et sauvegardez la configuration si vous ne voulez pas installer les packages de contenu UBA. Dans ce cas, vous devrez créer vos propres règles pour déclencher les événements Sense qui envoient des événements à UBA.

**Remarque :** Si vous décochez la case **Installer et mettre à niveau les packages de contenu UBA** et sauvegardez la configuration, puis retournez à la page Paramètres UBA et décidez de cocher à nouveau la case et de sauvegarder la configuration, les packages de contenu seront installés et mis à niveau.

# Content Package Settings

---



## Install and upgrade UBA content packages

Content packages include rules, custom properties, and reference data for use cases.

Important: If the content packages are not installed, you must create your own rules to trigger Sense Events.

## Que faire ensuite

«Configuration des paramètres d'application»

## Configuration des paramètres d'application

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres de l'application UBA.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres UBA**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres UBA**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres UBA**.
3. Dans la section Paramètres de l'application, configurez les paramètres suivants :

Option	Description
<b>Seuil de risque</b>	<p>Indique la valeur maximale du score de risque d'un utilisateur avant le déclenchement d'une infraction pour cet utilisateur. Un <i>score de risque</i> est la somme de tous les événements de risque détectés par les règles UBA.</p> <p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> <li>• <b>Dynamique</b> : La valeur par défaut est 4,0. Plus la valeur est élevée, plus le seuil dynamique sera haut et moins il y aura d'infractions. Vous devez désactiver l'option <b>Générer une infraction pour les utilisateurs à haut risque</b> tant que les réglages n'ont pas été appliqués pendant au moins un jour. La valeur du seuil dynamique est actualisée toutes les heures en fonction de la répartition du score de risque dans le système. Vous pouvez indiquer si vous voulez que le réglage soit basé sur le nombre d'infractions qui pourraient être déclenchées. Consultez les conseils ci-dessous pour plus de détails. <b>Remarque</b> : S'il n'y a pas suffisamment de variété dans les scores, le score de risque est fixé au score de l'utilisateur le plus risqué + 10, ceci afin d'éviter qu'un trop grand nombre d'infractions ne soient générées inutilement.</li> <li>• <b>Statique</b> : La valeur par défaut est 100.000. Par défaut, cette valeur est élevée afin d'éviter que des infractions ne soient déclenchées avant l'analyse de l'environnement. Vous pouvez activer <b>Générer une infraction pour les utilisateurs à haut risque</b> afin qu'une infraction soit ouverte pour les utilisateurs dépassant le seuil de risque. Vous pouvez indiquer si vous voulez que le réglage soit basé sur le nombre d'infractions qui pourraient être déclenchées.</li> </ul> <p><b>Conseil</b> : Pensez à configurer UBA et à conserver la valeur par défaut. Laissez les paramètres s'exécuter pendant au moins un jour afin de voir les types de score renvoyés. Après quelques jours, consultez les résultats sur le tableau de bord afin de déterminer un schéma. Vous pouvez ensuite ajuster le seuil. Par exemple, si un ou deux utilisateurs ont des scores avoisinant 500 mais que la plupart des utilisateurs ont des scores avoisinant 100, indiquez 200 ou 300 comme seuil. Une valeur avoisinant 100 constitue une situation "normale" pour votre environnement. Tout score supérieur peut nécessiter votre attention.</p>
<b>Réduire le risque avec le facteur indiqué, par heure</b>	<p>La dégradation du risque correspond au pourcentage de diminution du score de risque à chaque heure. La valeur par défaut est 0,5.</p> <p><b>Remarque</b> : Plus le nombre est élevé, plus la décroissance du score de risque est rapide et plus le nombre est faible, plus la décroissance du score de risque est lente.</p>
<b>Plage de dates pour les graphiques des détails de l'utilisateur</b>	<p>Plage de date affichée pour les graphiques des détails de l'utilisateur sur la page Détails de l'utilisateur. La valeur par défaut est 1.</p>
<b>Durée du statut d'examen</b>	<p>Il est nécessaire de définir le nombre de jours (1 - 10 000) affecté à un examen.</p>
<b>Intervalle d'inactivité de l'utilisateur</b>	<p>La page Détails de l'utilisateur affiche une ligne de temps avec les activités groupées par session. Si un utilisateur est inactif pendant le laps de temps indiqué dans la zone <b>Intervalle d'inactivité de l'utilisateur</b>, la session se termine. La valeur par défaut est de 15 minutes.</p>
<b>Seuil de compte inactif</b>	<p>Nombre de jours pendant lesquels les utilisateurs peuvent être inactifs avant d'être considérés comme dormants. La valeur par défaut est de 14 jours. Pour plus d'informations, consultez «Comptes dormants», à la page 41.(Disponible dans les versions 3.2.0 et ultérieures.)</p>
<b>Rechercher des actifs pour un nom d'utilisateur, lorsque celui-ci n'est pas disponible dans les données d'événement ou de flux</b>	<p>Sélectionnez la case à cocher pour rechercher des noms d'utilisateur dans la table des actifs. L'application UBA utilise des actifs pour rechercher un utilisateur via une adresse IP lorsque aucun utilisateur n'est répertorié dans un événement.</p> <p><b>Important</b> : Cette fonction peut être à l'origine de problèmes de performances dans l'application UBA et dans votre système QRadar.</p> <p><b>Conseil</b> : Si le seuil de délai d'attente de requête est dépassé, l'application ne renvoie aucune donnée. Si un message d'erreur s'affiche sur le tableau de bord UBA, désélectionnez la case à cocher puis cliquez sur <b>Actualiser</b>.</p>

Option	Description
Afficher les indicateurs de pays/région pour les adresses IP	Désélectionnez cette case à cocher si vous ne souhaitez pas afficher les indicateurs de pays et de région pour les adresses IP.

## Application Settings

**Risk threshold**  Current threshold value is 1330.  
 Dynamic threshold (used as the amount of standard deviation) [ $> 0$ ]

Value

**Generate an offense for high risk users**  
 UBA can open a username type offense for users above the risk threshold.  
 If you enable the setting, **0 offenses** can be generated based on the threshold value you entered.

**Decay risk by this factor per hour [0.01 - 0.99999]**

Factor

**Date range for user detail graphs [1 - 7 Days]**

Days

**Duration of investigation status [1 - 10000 Hours]**

Hours

**User inactivity interval [5 - 120 Minutes]**

Minutes  
 Enter a duration in minutes that defines when a session ends. A session ends when there is no activity seen for the duration specified.

**Dormant accounts threshold [ $\geq 1$  Days]**

Days  
 Enter the number of days that users are inactive before they are considered dormant.

**Search assets for username, when username is not available on event or flow data**  
 Important: Required for flow-based rules. Enabling this setting can affect UBA and QRadar performance.

**Display country/region flags for IP addresses**

### Que faire ensuite

«Configuration de l'importation des données utilisateur et de la coalescence utilisateur»

### Configuration de l'importation des données utilisateur et de la coalescence utilisateur

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous pouvez importer des données utilisateur d'une table de référence.

### Avant de commencer

Effectuez la procédure «Configuration des paramètres d'application», à la page 30.

## Pourquoi et quand exécuter cette tâche

L'importation de données utilisateur et la coalescence utilisateur sont optionnelles.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres UBA**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres UBA**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres UBA**.
3. Dans la section d'importation des données utilisateur, sélectionnez **Table de référence**.
4. Entrez un nombre d'heures afin de déterminer la fréquence à laquelle la table de référence doit effectuer l'ingestion des données.
5. Dans la section de coalescence d'utilisateur, sélectionnez les attributs extraits par votre système QRadar de la table de référence sélectionnée et apparaissant comme nom d'utilisateur. Les scores du risque de ces identificateurs sont ajoutés, et aussi associés, à l'identificateur principal. Ne sélectionnez pas des attributs qui ont partagé des valeurs entre différents utilisateurs. Par exemple, s'il y a trop de personnes du même service, ne sélectionnez pas le nom d'utilisateur "Service". Si vous sélectionnez un attribut partagé, comme "Service" ou "Pays", UBA combine tous les utilisateurs possédant la même valeur de service ou de pays.

## Import User Data

Optional: Select a reference table that contains the user data that you want to import. You can generate the data from the included 'Reference Data Import - LDAP' application or by using external scripts or tools. If no reference table is selected, then all usernames are identified as unique.

### Reference table

50k\_users

50000 unique users in selected table

### Ingest user data from reference table this often [ $\geq$ 2 Hours]

4

Hours

## User Coalescing

Select attributes from the reference table which appear as the property 'Username' on the data processed by your QRadar system. UBA uses the selected attributes to combine activity from different usernames into one user identity. Do not select attributes that have shared values across users. Selecting a shared attribute, such as department or country, causes UBA to combine all users with the same department or country value.

<input type="checkbox"/>	city	Manaus	Shanghai	Rio de Janeiro
<input type="checkbox"/>	country	Brazil	China	Brazil
<input type="checkbox"/>	department	Marketing	Marketing	Sales
<input checked="" type="checkbox"/>	email	testuser-183@example.ibm.com	testuser-182@example.ibm.com	testuser-181@example.ibm.com
<input checked="" type="checkbox"/>	id1	testuser-183	testuser-182	testuser-181
<input checked="" type="checkbox"/>	id2	testuser-183_id2	testuser-182_id2	testuser-181_id2
<input type="checkbox"/>	id3	testuser-183_id3	testuser-182_id3	testuser-181_id3
<input type="checkbox"/>	id4	testuser-183_id4	testuser-182_id4	testuser-181_id4
<input type="checkbox"/>	job_title	Web Designer	Sales Manager	IT Support Specialist
<input checked="" type="checkbox"/>	username	testuser-183	testuser-182	testuser-181

## Que faire ensuite

«Configuration des attributs à afficher»

### Configuration des attributs à afficher

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous pouvez sélectionner des attributs dans la table de référence que vous voulez afficher sur la page Détails de l'utilisateur.

### Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres UBA**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins** > **User Analytics** > **Paramètres UBA**.

- Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres UBA**.
3. Dans la section d'affichage des attributs, sélectionnez les attributs à afficher sur la page Détails de l'utilisateur.

## Display Attributes

Select attributes from the reference table so that they appear on the user profile page. You can select all, some, or none of the display attributes depending on the data in the reference table. "Display Name" is the main username displayed on the UBA dashboard for each user. "Custom Group" can be used to specify another selection attribute (in addition to Job Title or Department) that is obtained from your reference table when you configure the Defined Peer Group analytic in the Machine Learning app.

<b>Display Name</b>	full_name	▼	SAMENAMEEXCEPTCASE-1_id1
<b>Full Name</b>	full_name	▼	SAMENAMEEXCEPTCASE-1_id1
<b>Email</b>	email	▼	SAMENAMEEXCEPTCASE-1_id1@example.ibm.com
<b>Job Title</b>	job_title	▼	Software Engineer
<b>Department</b>	department	▼	Sales
<b>City</b>	city	▼	Monterrey
<b>State/Province</b>	state	▼	Nuevo Leon
<b>Country</b>	country	▼	Mexico
<b>Custom Group</b>	id2	▼	SAMENAMEEXCEPTCASE-1_id2

4. Cliquez sur **Sauvegarder la configuration**.



---

## 5 Administration

---

### Gestion des droits de l'application UBA de QRadar

Les administrateurs utilisent la fonction User Role Management fournie dans IBM QRadar pour configurer et gérer les comptes utilisateurs. En tant qu'administrateur, vous devez activer les droits Analyse utilisateur, Infractions et Activité du journal pour chaque rôle d'utilisateur autorisé à utiliser l'application UBA de QRadar.

#### Pourquoi et quand exécuter cette tâche

Après avoir installé l'application QRadar UBA, les droits **Analyse utilisateur**, **Infractions** et **Activité du journal** doivent être activés pour les rôles utilisateur affectés aux utilisateurs envisageant d'utiliser l'application QRadar UBA.

#### Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Dans la section Configuration du système, cliquez sur **Gestion des utilisateurs**, puis sur l'icône **Rôles utilisateur**.
- Sélectionnez un rôle utilisateur existant ou créez un nouveau rôle.
- Sélectionnez les cases à cocher suivantes pour ajouter les droits au rôle.
  - Analyse utilisateur**
  - Infractions**
  - Activité du journal**
- Cliquez sur **Sauvegarder**.

---

### Création de listes de surveillance

Vous pouvez ajouter un utilisateur à une liste de surveillance nouvelle ou existante.

#### Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un utilisateur à une liste de surveillance nouvelle ou existante à partir du Tableau de bord de l'application UBA, de la page Détails de l'utilisateur ou de la page de Résultats de la recherche. Un utilisateur peut être membre de plusieurs listes de surveillance.

#### Procédure

- Depuis le tableau de bord UBA ou la page Détails de l'utilisateur, cliquez sur l'icône **Liste de surveillance** .
- Dans le menu, sélectionnez **Créer une nouvelle liste de surveillance**. Pour ajouter un utilisateur à une liste de surveillance existante, cliquez sur **Ajouter à votre liste de surveillance**.
- Sous l'onglet **Paramètres généraux**, entrez le nom d'une liste de surveillance.
- Vous pouvez artificiellement accroître ou décroître le score du risque de l'utilisateur en modifiant la valeur de la zone **Evaluer le risque par facteur**. Avec le facteur par défaut '1', le score du risque reste inchangé.

**Remarque :** Si un utilisateur se trouve dans plusieurs listes de surveillance, le facteur d'échelle le plus grand est appliqué.

- Dans la section **Priorité de suivi Machine Learning**, sélectionnez la priorité de suivi des utilisateurs par les analyses Machine Learning.
  - Elevée - Les utilisateurs sont toujours suivis jusqu'au nombre maximum d'utilisateurs par analyse Machine Learning.
  - Normal - Les utilisateurs sont suivis en fonction du risque le plus élevé une fois tous les utilisateurs élevés inclus.
  - Jamais - Les utilisateurs ne sont pas suivis par Machine Learning.
- Cliquez sur **Suivant**.

**Create a watchlist**

**General Settings**   **Membership Settings**

**Name**

Enter a watchlist name.

**Scale risk by factor**

Enter a value in scale factor (0 - 10) to increase or decrease the user's risk.  
For example, if you want to scale down your admin account, set the factor to '0.1'.

0.01

**Machine Learning tracking priority**

Select the priority for how users are added to the ML app.

High

Normal

Never

**Next**   **Cancel**

- Sous l'onglet **Paramètres d'appartenance**, vous pouvez remplir automatiquement la liste de surveillance à partir d'un ensemble de référence et/ou d'une expression régulière.
- Facultatif : Dans la zone **Importer depuis un ensemble de référence QRadar**, recherchez un ensemble de référence ou cliquez pour sélectionner un ensemble de référence de la liste afin d'importer toutes les entrées de cet ensemble de référence. Remarque : La liste peut contenir des ensembles de référence qui n'ont pas de noms d'utilisateur. Après avoir sélectionné un ensemble de référence, cliquez sur le lien pour le consulter.
- Facultatif : Dans la zone **Ajouter depuis les utilisateurs surveillés avec un filtre d'expression régulière**, vous pouvez sélectionner une propriété utilisateur et entrer une expression régulière Python valide pour sélectionner les utilisateurs qui sont déjà présents dans la base de données UBA.
- Dans la zone **Intervalle d'actualisation**, entrez le nombre d'heures définissant la fréquence à laquelle la liste d'utilisateurs doit être mise à jour. Par exemple, si vous entrez 10, la liste d'utilisateurs est mise à jour toutes les 10 heures. Si **Intervalle d'actualisation** est défini sur la valeur 0 (zéro), vous pouvez mettre à jour manuellement la liste de surveillance en cliquant sur **Actualiser**.
- Cliquez sur **Sauvegarder**.

✕

## Create a watchlist

General Settings
Membership Settings

Optional: You can import users with a reference set or regular expression or both.  
 Note: You can also add any user to a watchlist by clicking the Watchlist icon.

**Import from QRadar reference set**  
 Search for or select a reference set from your QRadar system.

**Add from Monitored Users with regex filter**  
 Select a user property and enter a valid Python regular expression.  
 For example, to retrieve all users with engineers in their job title select 'Job title' and enter '\*.Engineer.\*'.  
 You can also enter the '^\$' regular expression to match a missing property. For example, to find service accounts without an email address, select the property 'email' and enter '^\$'.

Select a property ▼

[a-z]+

**Refresh interval**  
 Enter the number of hours between 0 and 24 (0 to disable) for how often users are updated in the watchlist.

24

Save
Cancel

---

## Affichage de la liste blanche pour les utilisateurs de confiance

Vous pouvez consulter la liste des utilisateurs de confiance (liste blanche) dans la liste de gestion de l'ensemble de références.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation ( ) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans la section Configuration du système, cliquez sur **Gestion de l'ensemble de référence**.
3. Dans la fenêtre Gestion de l'ensemble de référence, sélectionnez l'ensemble de références **UBA : Trusted Usernames**.
4. Cliquez sur **Afficher le contenu**.

---

## Gestion des outils de surveillance du réseau

Vous pouvez gérer des outils de surveillance du réseau pour l'application User Behavior Analytics (UBA) d'IBM QRadar.

## Pourquoi et quand exécuter cette tâche

Si vous souhaitez contrôler l'utilisation de programmes de capture, de surveillance ou d'analyse de réseau, vérifiez que ces programmes sont répertoriés dans l'ensemble de références UBA : Network Capture, Monitoring and Analysis Program Filenames. Vous devez ensuite activer la règle **UBA : Network Capture, Monitoring and Analysis Program Filenames**.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans la section Configuration du système, cliquez sur **Gestion de l'ensemble de référence**.
3. Dans la fenêtre Gestion de l'ensemble de référence, sélectionnez l'ensemble de références **UBA : Network Capture, Monitoring and Analysis Program Filenames**.
4. Cliquez sur **Afficher le contenu**.
5. Pour ajouter une application à gérer, cliquez sur **Ajouter** et entrez les valeurs dans la zone.
6. Pour supprimer une application, sélectionnez l'application et cliquez sur **Supprimer**.

### Que faire ensuite

Activez la règle **UBA : Network Capture, Monitoring and Analysis Program Filenames**.

---

## Gestion des programmes restreints

Vous pouvez gérer des programmes restreints pour l'application User Behavior Analytics (UBA) d'IBM QRadar.

## Pourquoi et quand exécuter cette tâche

Si vous avez des applications dont vous souhaitez contrôler l'utilisation, accédez à l'ensemble de références UBA : Restricted Program Filenames et entrez les applications que vous souhaitez contrôler. Vous devez activer la règle UBA : Restricted Program Filenames.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans la section Configuration du système, cliquez sur **Gestion de l'ensemble de référence**.
3. Dans la fenêtre Gestion de l'ensemble de référence, sélectionnez l'ensemble de références **UBA : Restricted Program Filenames**.
4. Cliquez sur **Afficher le contenu**.
5. Pour ajouter une application à gérer, cliquez sur **Ajouter** et entrez les valeurs dans la zone.
6. Pour supprimer une application, sélectionnez l'application et cliquez sur **Supprimer**.

### Que faire ensuite

Activez la règle **UBA : Restricted Program Filenames**.

---

## Ajout de sources de journaux au groupe de sources de journaux de confiance

Si vous ne souhaitez pas que certaines sources de journaux fassent l'objet d'une surveillance et d'un rapport par l'application UBA, vous pouvez les ajouter à **UBA : Trusted Log Source Group**. L'ajout de sources de journaux au groupe empêche leur surveillance par l'application UBA.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Sources de journaux**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres communs de votre source de journaux.
5. Configurez les paramètres spécifiques au protocole de votre source de journaux.
6. Cochez la case **UBA : Trusted Log Source Group**.
7. Cliquez sur **Sauvegarder**.
8. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

---

## Comptes dormants

Vous pouvez voir les utilisateurs de votre système qui ont des comptes dormants, des comptes actifs ou des comptes qui n'ont jamais servi.

### Visualisation des comptes dormants sur la page Détails de l'utilisateur

Dans les versions 3.2.0 et ultérieures, il est possible de voir l'état des comptes associés à l'utilisateur sélectionné sur la page Détails de l'utilisateur.

Etat d'un compte d'utilisateur	Description
Actif	Compte auquel sont reliés des événements que l'application UBA a vus consignés dans une source de journaux QRadar au cours de la période configurée déterminant à partir de quand un compte inactif est considéré comme compte dormant.
Inactif	Compte pour lequel UBA a déjà vu au moins un événement dans le passé, mais n'en a pas vu d'autres au cours de la période configurée déterminant à partir de quand un compte inactif est considéré comme compte dormant.
Jamais utilisé	<p>Compte pour lequel UBA n'a jamais vu d'événement avec ce nom d'utilisateur dans une source de journaux QRadar.</p> <p>Les comptes ayant l'état "Jamais utilisé" peuvent résulter des activités suivantes :</p> <ul style="list-style-type: none"><li>• Comptes n'ayant jamais été consignés par une source de journaux QRadar pour le compte du nom d'utilisateur associé.</li><li>• L'événement s'est produit alors que la version 3.2.0 d'UBA n'était pas encore installée. Notez qu'après l'installation d'UBA, seuls les événements qui se sont produits au cours de la dernière heure sont analysés pour déterminer à quand remonte le dernier accès à un compte. Après cette première analyse, UBA recherche les événements qui se sont produits entre les exécutions de la tâche d'arrière-plan chargée de surveiller l'utilisation des comptes.</li></ul> <p>Notez que les comptes de la catégorie "Jamais utilisé" ont probablement été importés de l'application LDAP.</p>

<b>Test User 1</b>		Active	testuser1
Web Developer			testuser1_admin
Development		Dormant 	testuser1_db
Dallas, TX, US		Never Used	testuser1@exam...
Overall Risk Score		Risk last Interval	
5K 		1K	

## Liste de surveillance Utilisateurs avec comptes dormants

La liste de surveillance Utilisateurs avec comptes dormants est automatiquement générée lorsque l'application UBA récupère les données d'utilisateurs. Elle est visible sur le tableau de bord UBA.

Si vous supprimez cette liste de surveillance, elle n'est pas automatiquement recréeée. Si vous avez besoin de la recréer, sélectionnez l'ensemble de référence **UBA : Dormant Accounts** sous l'onglet **Paramètres d'appartenance** de l'écran Créer une liste de surveillance.

## Configuration du seuil de durée pour les comptes dormants

Le seuil de durée au-delà duquel un compte inactif est considéré comme dormant est, par défaut, de 14 jours. Vous pouvez changer le nombre de jours pendant lesquels les utilisateurs peuvent être inactifs avant d'être considérés comme dormants dans la section Paramètres de l'application de la page Paramètres UBA (**Paramètres d'administrateur > Analyse utilisateur > Paramètres UBA**).

## Réponses aux comptes ou utilisateurs dormants

Vous pouvez générer des réponses aux comptes dormants à partir des règles fournies. Vous pouvez aussi créer des réponses personnalisées en utilisant les événements déclenchés à partir de l'application.

Pour utiliser les règles fournies afin d'augmenter le score d'un utilisateur lorsque celui-ci utilise ou tente d'utiliser un compte dormant, assurez-vous que les règles suivantes soient activées :

- «UBA : Tentative d'utilisation d'un compte dormant», à la page 75
- «UBA : Compte inactif utilisé», à la page 75

Pour créer des réponses personnalisées, vous pouvez utiliser les événements générés suivants dans une règle ou une requête :

- Compte inactif détecté (QID 104000012)
- Compte inactif utilisé (QID 104000013)

### Concepts associés:

«Tableau de bord UBA et informations détaillées sur les utilisateurs», à la page 9

L'application User Behavior Analytics (UBA) d'IBM QRadar affiche les données de risque globales associées aux utilisateurs de votre réseau.

### Tâches associées:

«Configuration des paramètres d'application», à la page 30

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres de l'application UBA.

«Création de listes de surveillance», à la page 37

Vous pouvez ajouter un utilisateur à une liste de surveillance nouvelle ou existante.

---

## 6 Réglage

---

### Activation des index pour l'amélioration des performances

Pour améliorer les performances de votre application IBM QRadar User Behavior Analytics (UBA), activez les index dans IBM QRadar.

#### Pourquoi et quand exécuter cette tâche

Pour améliorer la vitesse des recherches dans IBM QRadar et dans l'application UBA, affinez les données globales en ajoutant les champs indexés suivants à votre requête de recherche :

- Catégorie de niveau supérieur
- Catégorie de niveau inférieur
- senseValue
- senseOverallScore
- Nom d'utilisateur

Pour plus d'informations sur l'indexation, consultez la section suivante dans l'IBM Knowledge Center à l'adresse [https://www.ibm.com/support/knowledgecenter/SS42VS\\_7.3.1/com.ibm.qradar.doc/c\\_qradar\\_adm\\_index\\_mgmt.html](https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_index_mgmt.html).

#### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation (☰) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans la section Configuration système, cliquez sur l'icône **Gestion de l'index**.
3. Dans la page Gestion de l'index, dans la zone de recherche, entrez **Catégorie de niveau supérieur**.
4. Sélectionnez **Catégorie de niveau supérieur**, puis cliquez sur **Activer l'index**.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	High Level Category	63.13%	82.8%	17.2%	17MB	events

5. Cliquez sur **Sauvegarder**.
6. Sélectionnez **Catégorie de niveau inférieur** puis cliquez sur **Activer l'index**.

Enable Index
  Disable Index
 
?

Display: Last 24 Hours | View: All | Database: All | Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

**WARNING:** Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
<input checked="" type="checkbox"/>	Low Level Category	33.86%	77.25%	0%	888KB	events

7. Cliquez sur **Sauvegarder**.
8. Dans la page Gestion de l'index, dans la zone de recherche, entrez sense.
9. Sélectionnez **senseValue** et **senseOverallScore**, puis cliquez sur **Activer l'index**.

Enable Index
  Disable Index
 
?

Display: Last 24 Hours | View: All | Database: All | Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

**WARNING:** Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
<input checked="" type="checkbox"/>	senseValue (custom)	11.5%	0%	100%	0KB	events
<input checked="" type="checkbox"/>	senseOverallScore (custom)	0.06%	0%	100%	0KB	events
<input type="checkbox"/>	senseOffenseId (custom)	0%	0%	0%	0KB	events
<input type="checkbox"/>	senseOffenseScore (custom)	0%	0%	0%	0KB	events
<input type="checkbox"/>	senseWindowScore (custom)	0%	0%	0%	0KB	events

10. Cliquez sur **Sauvegarder**.
11. Dans la page Gestion de l'index, dans la zone de recherche, entrez Nom d'utilisateur.
12. Sélectionnez **Nom d'utilisateur**, puis cliquez sur **Activer l'index**.

Enable Index
  Disable Index
 
?

Display: Last 24 Hours | View: All | Database: All | Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

**WARNING:** Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
<input checked="" type="checkbox"/>	Username	10.12%	99.45%	0%	22MB	events
<input type="checkbox"/>	Identity Username	0%	0%	0%	0KB	events

13. Cliquez sur **Sauvegarder**.

## Intégration de contenu QRadar (nouveau ou existant) à l'application UBA

Utilisez l'assistant de règles dans QRadar pour intégrer des règles QRadar (existantes ou personnalisées) à l'application UBA.

## Pourquoi et quand exécuter cette tâche

Pour répondre à vos besoins spécifiques, vous pouvez utiliser les fonctions de QRadar en intégrant vos règles QRadar existantes à l'application UBA.

**Restriction :** Ne personnalisez pas vos règles de telle sorte que les ensembles de référence UBA et Machine Learning soient utilisés. Une tentative d'utiliser les ensembles de référence dans des règles personnalisées peut générer des défaillances dans l'application UBA.

### Procédure

1. Créez une copie de la règle. Ainsi, les mises à jour apportées à la règle de base n'affectent aucunement les modifications apportées à la nouvelle règle.
2. Ouvrez la règle dans l'assistant de règles puis accédez à la section Réponse à la règle.
3. Activez ou éditez l'option **Attribuer le nouvel élément** en vous assurant que le texte **Description de l'événement** est formaté de la manière suivante :  
senseValue=#,senseDesc='sometext',usecase\_id='rule UUID'
4. Sélectionnez **Catégorie de niveau supérieur** pour l'option **Sense**.
5. Cliquez sur **Terminer** pour sauvegarder les modifications.

**Remarque :** Si la règle fonctionne sur les données de flux, vous devez activer l'option **Rechercher des actifs pour un nom d'utilisateur, lorsque celui-ci n'est pas disponible dans les données d'événement ou de flux** afin que les événements sans nom d'utilisateur puissent tenter d'effectuer une recherche de mappage d'utilisateur.

---

## Ensembles de référence

L'application User Behavior Analytics et l'application Machine Learning utilisent des ensembles de référence pour stocker les informations utilisateur. Certaines de ces ensembles sont réservés à l'usage de ces applications. Vous ne devez pas les modifier ni les utiliser pour créer des règles personnalisées.

### Ensembles de référence personnalisables

Ensemble de référence	Description
UBA : Utilisateurs à haut risque	L'ensemble de référence <i>UBA : Utilisateurs à haut risque</i> est construit à partir de la valeur <b>Seuil de risque pour déclencher des infractions</b> sur la page Paramètres UBA. Le nombre maximum d'utilisateurs est de 10.000 et l'ensemble de référence est reconstruit toutes les 5 minutes.
UBA : Trusted Usernames	Vous pouvez ajouter des noms d'utilisateur à l'ensemble de référence <i>UBA : Trusted Usernames</i> (noms d'utilisateur de confiance), mais vous ne devez pas l'utiliser pour les règles ou les rapports. Aucune infraction n'est générée pour les utilisateurs membres de l'ensemble de référence <i>UBA : Trusted Usernames</i> .
UBA : ML Always Tracked Watchlist	L'ensemble de référence <i>UBA : ML Always Tracked Watchlist</i> est construit à partir des utilisateurs que vous choisissez de <b>Toujours suivre avec Machine Learning</b> dans la <b>Paramètres avancés</b> de la page Détails de l'utilisateur. Vous pouvez ajouter des noms d'utilisateur à l'ensemble de référence <i>UBA : ML Always Tracked Watchlist</i> (liste des utilisateurs toujours suivis par ML), mais vous ne devez pas l'utiliser pour les règles ou les rapports.

### Ensembles de référence non personnalisables

**Restriction :** Les ensembles de référence suivants ne doivent pas être modifiés ni utilisés pour créer des règles personnalisées.

- UBA - Current ML Tracked Users

- UBA - Previous ML Tracked Users
- UBA - Current Abridged ML Tracked Users
- UBA - Previous Abridged ML Tracked Users
- UBA - Current Peer Group ML Tracked Users
- UBA - Previous Peer Group ML Tracked Users

---

## 7 Règles et réglages pour l'application UBA

L'application User Behavior Analytics (UBA) d'IBM QRadar prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

L'application User Behavior Analytics (UBA) inclut des scénarios d'utilisation s'appuyant sur des règles personnalisées. Ces règles permettent de générer des données pour le tableau de bord de l'application UBA. A partir de la version 3.0.0 de l'application UBA, vous pouvez afficher, filtrer et définir des règles au sein de l'application UBA. Dans la version 2.8.0 et les versions antérieures, vous pouvez afficher et modifier les règles dans User Behavior Analytics Group, sous Liste de règles.

### Remarque :

- Par défaut, les règles de l'application UBA ne sont pas toutes activées.
- Une ou plusieurs des sources de journaux doivent fournir des informations pour la règle UBA spécifique. Les sources des journaux ne sont pas hiérarchisées dans un ordre quelconque.

**Restriction :** Ne personnalisez pas vos règles de telle sorte que les ensembles de référence UBA et Machine Learning soient utilisés. Une tentative d'utiliser les ensembles de référence dans des règles personnalisées peut générer des défaillances dans l'application UBA. Pour plus d'informations, consultez «Ensembles de référence», à la page 45.

Pour plus d'informations sur l'utilisation des règles dans QRadar, consultez [https://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.3.1/com.ibm.qradar.doc/c\\_qradar\\_rul\\_mgt.html](https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_rul_mgt.html)

### Page Règles et réglages

La version 3.0.0 de l'application UBA introduit la page Règles et réglages (**Paramètres Admin > Analyse utilisateur > Règles et réglages**).

La page Règles et réglages comporte la liste de toutes les règles incluses avec la version installée de l'application UBA, ainsi que l'état actuellement activé et les ensembles de référence correspondants.

Sur la page Règles et réglages, vous pouvez :

- Activer ou désactiver des règles
- Accéder rapidement à l'Assistant Règles QRadar pour passer en revue ou éditer des règles
- Accéder rapidement aux ensembles de référence pour passer en revue ou éditer leur contenu
- Filtrer la table de règles par catégorie, statut, score du risque par défaut, ensembles de référence requis et dépendances de contenu
- Trier la table de règles par nom de règle, ensemble de référence ou statut
- Rechercher des éléments ou des mots trouvés dans l'infobulle de description de règle
- Accéder à la documentation d'aide pour les règles individuelles

---

## Accès et authentification

### UBA : Tentatives d'authentification par force brute

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Tentatives d'authentification par force brute

## Activation par défaut

Oui

## Valeur senseValue par défaut

5

## Description

Détecte une attaque par force brute (horizontale et verticale) provoquant un échec d'authentification.

## Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures
- BB:UBA : Detecting Authentication Bruteforce Attempts (Horizontal)
- BB:UBA : Detecting Authentication Bruteforce Attempts (Vertical)

## Sources de données

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete),

Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès d'un utilisateur standard à un actif destiné uniquement aux administrateurs**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès d'un utilisateur standard à un actif destiné uniquement aux administrateurs

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte lorsqu'un utilisateur non-administrateur se connecte à un actif qui est à usage administratif uniquement. Deux jeux de références vides seront importés avec cette règle : "UBA : Executive Users" et "UBA : Executive Assets". Modifiez les jeux de références de manière à ajouter ou à supprimer des comptes et des adresses IP marqués dans votre environnement. Activez cette règle après avoir configuré les jeux de références.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:CategoryDefinition: Firewall or ACL Accept

### **Configuration requise**

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Executive Users" et "UBA : Executive Assets".

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass

Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès d'un utilisateur à haut risque à une ressource critique**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès d'un utilisateur à haut risque à une ressource critique

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte lorsqu'un utilisateur impliqué dans des incidents (infractions) a accès à des ressources critiques.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "Critical Assets".

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controllor, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper

Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetalIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## **UBA : Echec de connexion de plusieurs comptes VPN à partir d'une adresse IP unique**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Echec de connexion de plusieurs comptes VPN à partir d'une adresse IP unique

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Détecte les échecs de connexion de compte VPN à partir de l'ensemble de référence "UBA : Echec de connexion de plusieurs comptes VPN à partir d'une adresse IP unique".

### **Règles de prise en charge**

- UBA : Remplir plusieurs comptes VPN dont la connexion a échoué à partir d'une adresse IP unique
- BB:UBA : VPN Login Failed

## Configuration requise

Activez la règle suivante : "UBA : Remplir plusieurs comptes VPN dont la connexion a échoué à partir d'une adresse IP unique"

## Sources de données

Cisco Adaptive Security Appliance (ASA)

## UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Mappe plusieurs utilisateurs de VPN qui proviennent de la même adresse IP puis émet le score de risque. Lorsque la règle détecte des utilisateurs de VPN provenant de la même adresse IP, cette dernière est ajoutée à la règle "UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP". Avant d'activer cette règle, assurez-vous que la règle "UBA : Remplir plusieurs comptes VPN connectés à partir d'une adresse IP unique" est activée et que l'ensemble de référence "UBA : Plusieurs comptes VPN connectés à partir d'une seule adresse IP" inclut des données.

## Règles de prise en charge

- UBA : Remplir plusieurs comptes VPN connectés à partir d'une adresse IP unique
- BB:UBA : VPN Login Successful

## Configuration requise

Activez la règle suivante : "UBA : Remplir plusieurs comptes VPN connectés à partir d'une adresse IP unique"

## Sources de données

Cisco Adaptive Security Appliance (ASA)

## UBA : Répétition d'accès non autorisés

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Répétition d'accès non autorisés

## Activation par défaut

Oui

## Valeur senseValue par défaut

10

## Description

Indique que des activités d'accès non autorisé répétées ont été détectées.

## Règle de prise en charge

UBA : Accès non autorisé

## Configuration requise

Activez la règle suivante : "UBA : Accès non autorisé"

## Sources de données

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrifry Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDoS Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication

Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

## **UBA : Accès non autorisé**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès non autorisé

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Indique que des activités d'accès non autorisé ont été détectées.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:UBA : Access Denies
- BB:UBA : Application Denies

### **Sources de données**

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrifry Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper

Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDos Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

## **UBA : Accès Unix/Linux avec un compte de service ou de machine**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Unix/Linux System Accessed With Service or Machine Account

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une session interactive (par le biais de l'interface graphique utilisateur et de l'interface de ligne de commande, avec une connexion locale et distante) lancée par le compte d'un service ou d'une machine sur des serveurs UNIX et Linux. Les comptes et les sessions interactives autorisés sont répertoriés dans les ensembles de référence UBA : Service, Machine Account et UBA : Allowed Interaction Session. Modifiez les ensembles de référence pour ajouter ou supprimer une session interactive à marquer dans votre environnement.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Firewall or ACL Accept
- BB:CategoryDefinition: Authentication Success

### **Configuration requise**

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Service, Machine Account" et "UBA : Allowed Interactive Session".

## Sources de données

Linux OS

## UBA : Accès utilisateur - Echec de l'accès à des ressources critiques

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès utilisateur - Echec de l'accès à des ressources critiques

### Activation par défaut

Oui

### Valeur senseValue par défaut

5

### Description

Cette règle détecte les échecs d'authentification pour les systèmes se trouvant dans l'ensemble de références d'actifs critiques.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

### Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "Critical Assets".

## Sources de données

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network

Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès utilisateur - Premier accès à des ressources critiques**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

Éléments pris en charge

- UBA : User Access First Access to Critical Assets
- UBA : Critical Systems Users Seen Update

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

**UBA : User Access First Access to Critical Assets** Indique que l'utilisateur a accédé à un actif critique pour la première fois. La collecte de référence "Critical Systems Users Seen" gouverne la durée de vie d'une observation. Par défaut, cette règle détecte le premier accès en trois mois.

**UBA : Critical Systems Users Seen Update** Met à jour la dernière valeur vue dans la collecte de référence "Critical Systems Users Seen" pour les correspondances Adresse IP cible/Nom d'utilisateur existantes.

## Règles de prise en charge

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "Critical Assets".

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure,

Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès utilisateur depuis plusieurs hôtes**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès utilisateur depuis plusieurs hôtes

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

5

### **Description**

Détecte les cas où un utilisateur se connecte depuis un nombre d'appareils supérieur au nombre autorisé.

### **Règle de prise en charge**

BB:UBA : Common Event Filters

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2,

IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetalIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès utilisateur au serveur interne à partir d'un serveur intermédiaire**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès utilisateur au serveur interne à partir d'un serveur intermédiaire

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte lorsqu'un utilisateur utilise un serveur d'accès direct pour accéder aux serveurs VPN ou internes.

## Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

## Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Jump Servers" et "UBA : Internal Servers".

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler

Audit, SIM Audit,SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM,Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Anomalie lors de la connexion utilisateur**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Anomalie lors de la connexion utilisateur

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Indique une séquence d'échecs de connexion sur un actif local. La règle peut également indiquer un compromis de compte ou une activité de mutation latérale. Vérifiez que la règle Multiple Login Failures for Single Username est activée. Réglez les paramètres de correspondance et de durée de cette règle pour optimiser la réactivité.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- Multiple Login Failures for Single Username

### **Configuration requise**

Activez la règle suivante : "Multiple Login Failures for Single Username"

### **Sources de données**

Toutes les sources de journaux prises en charge.

## **UBA : Utilisateur accédant à un compte à partir d'une source anonyme**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur accédant à un compte à partir d'une source anonyme

### **Activation par défaut**

Oui

## Valeur senseValue par défaut

15

### Description

Indique qu'un utilisateur accède à des ressources internes à partir d'une source anonyme comme TOR ou un VPN.

### Règles de prise en charge

- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

### Configuration requise

Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.

### Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara,

Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès utilisateur à des heures inhabituelles**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès utilisateur à des heures inhabituelles

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Indique que les utilisateurs s'authentifient correctement à des heures inhabituelles pour votre réseau, comme défini par les blocs de construction "UBA: Unusual Times, %".

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Unusual Times, Evening
- BB:UBA : Unusual Times, Overnight

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco

Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès au VPN par un compte de service ou de machine**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès au VPN par un compte de service ou de machine

## Activation par défaut

Oui

## Valeur senseValue par défaut

10

## Description

Détecte lorsqu'un compte de service ou machine accède à un réseau VPN Cisco. Les comptes sont répertoriés dans l'ensemble de référence 'UBA : Service, Machine Account'. Modifiez cette liste afin d'ajouter ou de retirer dans votre environnement des comptes à marquer.

## Règle de prise en charge

BB:UBA : VPN Mapping (logic)

## Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Service, Machine Account".

## Sources de données

Cisco Adaptive Security Appliance (ASA)

## UBA : Partage d'un certificat VPN

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Partage d'un certificat VPN

## Activation par défaut

Oui

**Remarque :** Si vous prévoyez d'utiliser la règle UBA : VPN Certificate Sharing, vous devez mettre à jour le gestionnaire de services de données de passerelle Cisco de la manière suivante.

- Pour la version 7.2.8 : DSM-CiscoFirewallDevices-7.2-20170619124928.noarch.rpm
- Pour la version 7.3.0 et les versions ultérieures : DSM-CiscoFirewallDevices-7.3-20170619132427.noarch.rpm

## Valeur senseValue par défaut

15

## Description

Cette règle détecte lorsque le nom d'utilisateur d'un événement VPN est différent de 'VPNSubjectcn'. Le cas échéant, un partage de certificat VPN peut être en cours. Le partage de certificat ou de jeton d'authentification, quel qu'il soit, peut empêcher d'identifier qui a effectué quelle action. Il peut alors s'avérer difficile de déterminer la procédure à suivre.

## Règles de prise en charge

- BB:UBA : VPN Mapping (logic)
- UBA : Subject\_CN and Username Map Update
- UBA : Subject\_CN and Username Mapping

Ces règles mettent à jour les ensembles de référence associés avec les données requises.

## Configuration requise

Activez les règles suivantes :

- UBA : Subject\_CN and Username Map Update
- UBA : Subject\_CN and Username Mapping

## Sources de données

Cisco Adaptive Security Appliance (ASA)

## UBA : Accès Windows avec un compte de service ou de machine

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès Windows avec un compte de service ou de machine

## Activation par défaut

Oui

## Valeur senseValue par défaut

15

## Description

Détecte une session interactive (RDP, connexion locale) lancée par le compte d'un service ou d'une machine sur un serveur Windows Server. Les comptes sont répertoriés dans l'ensemble de références UBA : Service, Machine Account. Modifiez la liste afin d'ajouter ou de retirer dans votre environnement des comptes à marquer.

## Règles de prise en charge

BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Service, Machine Account".

## Sources de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4776)

---

## Comptes et privilèges

### UBA : Compte, groupe ou privilège ajouté

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Compte, groupe ou privilège ajouté (auparavant appelé UBA : Account, Group or Privileges Added or Modified)

### Activation par défaut

Oui

### Valeur senseValue par défaut

5

### Description

Détecte les événements qu'un utilisateur accomplit et qui entrent dans l'une des catégories suivantes. La règle attribue un événement IBM Sense pour incrémenter le score de risque de l'utilisateur d'origine.

- Authentication.Group Added
- Authentication.Group Changed
- Authentication.Group Member Added
- Authentication.Computer Account Added
- Authentication.Computer Account Changed
- Authentication.Policy Added
- Authentication.Policy Change
- Authentication.Trusted Domain Added
- Authentication.User Account Added
- Authentication.User Account Changed
- Authentication.User Right Assigned

**Remarque :** Pour régler l'impact de cette règle sur les scores de risque globaux des utilisateurs, pensez à modifier la règle du bloc de construction "CategoryDefinition: Authentication User or Group Added or Changed" en ajoutant des catégories d'événement pertinentes pour votre organisation.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Added

### Sources de données

Akamai KONA, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Blue Coat Web Security Service, BlueCat Networks Adonis, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, Carbon Black Protection, Centrifry Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco Nexus, Cisco PIX Firewall, Cisco Wireless Services Module (WiSM), Citrix

NetScaler, Configurable Firewall Filter, CorreLog Agent for IBM zOS, Custom Rule Engine, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Epic SIEM, Event CRE Injected, Extreme Dragon Network IPS, Extreme Stackable and Standalone Switches, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, Fidelis XPS, Flow Classification Engine, Forcepoint V Series, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HP Network Automation, HP Tandem, Honeycomb Lexicon File Integrity Monitor, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Server, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Mobile, IBM Security Identity Manager, IBM Security Network IPS (GX), IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva Incapsula, Imperva SecureSphere, Juniper Junos OS Platform, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Kisco Information Systems SafeNet/i, Lieberman Random Password Manager, Linux DHCP Server, Linux OS, Linux iptables Firewall, Mac OS X, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee Web Gateway, McAfee ePolicy Orchestrator, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SQL Server, Microsoft Windows Security Event Log, NCC Group DDoS Secure, Nortel Contivity VPN Switch, Nortel Multiprotocol Router, Nortel VPN Gateway, OS Services Qidmap, OSSEC, Okta, Open LDAP Software, OpenBSD OS, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Palo Alto PA Series, PostFix MailTransferAgent, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, Solaris Operating System Authentication Messages, Solaris Operating System DHCP Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Sophos Enterprise Console, Sophos Web Security Appliance, Squid Web Proxy, Stonesoft Management Center, Sun ONE LDAP, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec Gateway Security (SGS) Appliance, Symantec System Center, Symark Power Broker, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend InterScan VirusWall, Trend Micro Deep Security, Universal DSM, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, Zscaler Nss, genua genugate, iT-CUBE agileSI

## **UBA : Compte, groupe ou privilège modifié**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Compte, groupe ou privilège modifié (auparavant appelé UBA : Compte utilisateur changé)

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Indique qu'un compte utilisateur a été affecté par une action qui change les privilèges en vigueur de l'utilisateur, à la baisse ou à la hausse.

**Remarque concernant les faux positifs :** Cet événement peut attribuer par erreur les modifications apportées à un nom de compte à l'utilisateur effectuant les modifications. Si vous souhaitez réduire cette possibilité de faux positif, vous pouvez ajouter le test 'and when Username equals AccountName'.

**Remarque concernant les faux négatifs :** Cet événement peut ne pas détecter tous les cas de modifications de compte d'un utilisateur.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : Authentication User or Group or Policy Changed

### Sources de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 626, 642, 644, 1300, 1317, 625, 629, 4672, 4722, 4725, 4738, 4765, 4767, 4781, 4737, 4755)

## UBA : Attaque DoS par suppression de comptes

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Attaque DoS par suppression de comptes

### Activation par défaut

Non

### Valeur senseValue par défaut

10

### Description

Détecte les attaques par déni de service (DoS) en comparant le nombre d'événements de suppression de comptes à un seuil fixe, au cours d'une période fixe.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : User Account Deleted

### Sources de données

Amazon AWS CloudTrail (ID d'événement : DeleteUser)

Application Security DbProtect (ID d'événement : Login revoked - Windows, Login dropped - standard, Database role - dropped, Database user revoked)

Aruba Mobility Controller (ID d'événement : authmgr\_user\_del)

Box (ID d'événement : DELETE\_USER)

Brocade FabricOS (ID d'événement : SEC-1181, SEC-3028)

CA ACF2 (ID d'événement : ACF2-L)

Check Point (ID d'événement : user\_deleted, device\_deleted, User Deleted)

Cilasoft QJRN/400 (ID d'événement : C20020)

Cisco Adaptive Security Appliance (ASA) (ID d'événement : %PIX|ASA-5-502102, %ASA-5-502102)

Cisco FireSIGHT Management Center (ID d'événement : USER\_REMOVED\_CHANGE\_EVENT)

Cisco Firewall Services Module (FWSM) (ID d'événement : 502102)

Cisco Identity Services Engine (ID d'événement : 86008, 86028)

Cisco NAC Appliance (ID d'événement : CCA-1453, CCA-1502)

Cisco Nexus (ID d'événement : SECURITYD-6-DELETE\_STALE\_USER\_ACCOUNT)

Cisco Wireless LAN Controllers (ID d'événement : 1.3.6.1.4.1.9.9.515.0.1)

CloudPassage Halo (ID d'événement : Halo user deleted, Local account deleted (linux only))

CorreLog Agent for IBM zOS (ID d'événement : RACF DELUSER: No Violations)

Custom Rule Engine (ID d'événement : 3035, 3043)

Cyber-Ark Vault (ID d'événement : 276)

EMC VMWare (ID d'événement : AccountRemovedEvent)

Extreme Dragon Network IPS (ID d'événement : HOST:LINUX:USER-DELETED, HOST:WIN:ACCOUNT-DELETED)

Extreme Matrix K/N/S Series Switch (ID d'événement : User Deleted Event, has been deleted)

Extreme NAC (ID d'événement : Deleted registered user)

Extreme NetsightASM (ID d'événement : UserRemove)

Flow Classification Engine (ID d'événement : 3035, 3043)

Forcepoint Sidewinder (ID d'événement : passport deletion, all passports revoked)

HBGary Active Defense (ID d'événement : DeleteUser)

HP Network Automation (ID d'événement : User Deleted)

Huawei S Series Switch (ID d'événement : SSH/6/DELUSER\_SUCCESS)

IBM AIX Audit (ID d'événement : USER\_Remove SUCCEDED)

IBM AIX Server (ID d'événement : USER\_Remove)

IBM DB2 (ID d'événement : DROP\_USER SUCCESS)

IBM DataPower (ID d'événement : 0x81000136)

IBM IMS (ID d'événement : USER DELETED)

IBM Proventia Network Intrusion Prevention System (IPS) (ID d'événement : Delete User)

IBM QRadar Packet Capture (ID d'événement : UserDeleted)

IBM Resource Access Control Facility (RACF) (ID d'événement : 80 17.2, DELUSER\_SUCCESS, 80 17.0)

IBM Security Access Manager for Enterprise Single Sign-On (ID d'événement : REVOKE\_IMS\_ID, DELETE\_IMS\_ID)

IBM Security Directory Server (ID d'événement : SDS Audit)

IBM Security Identity Governance (ID d'événement : 50, 43, 70005)

IBM Security Identity Manager (ID d'événement : Delete SUCCESS, Delete SUBMITTED, Delete Success)

IBM SmartCloud Orchestrator (ID d'événement : user)

IBM Tivoli Access Manager for e-business (ID d'événement : 13408 - Succeeded, 13408 Command Succeeded)

IBM i (ID d'événement : GSL2502, M250100, DO\_USRPRF, GSL2602, GSL2601, M260100, MC@0400, GSL2501)

IBM z/OS (ID d'événement : 80 1.35)

Juniper Networks Network and Security Manager (ID d'événement : adm24473)

Linux OS (ID d'événement : userDel, Account Deleted, DEL\_USER)

McAfee Application/Change Control (ID d'événement : USER\_ACCOUNT\_DELETED)

McAfee ePolicy Orchestrator (ID d'événement : 20793)

Microsoft ISA (ID d'événement : user removed)

Microsoft Office 365 (ID d'événement : Delete User-PartiallySucceeded, Delete user-success, Delete User-success, Delete user-PartiallySucceeded)

Microsoft SQL Server (ID d'événement : 24129, DR - US, DR - SL, DR - LX, DR - AR, DR - SU, 24076, 24123, 38)

Microsoft Windows Security Event Log (ID d'événement : 4743, 630, 1327, 647, 4726)

Netskope Active (ID d'événement : Delete Admin, Deleted admin)

Nortel Application Switch (ID d'événement : User Deleted)

Novell eDirectory (ID d'événement : DELETE\_ACCOUNT)

OS Services Qidmap (ID d'événement : Account Deleted, User Deleted)

OSSEC (ID d'événement : 18112)

Okta (ID d'événement : core.user\_group\_member.user\_remove, app.generic.import.details.delete\_user)

Oracle Enterprise Manager (ID d'événement : Computer Delete (successful), User Delete (successful))

Oracle RDBMS Audit Record (ID d'événement : DROP USER-Standard:1, 53:1, 53:0, DROP USER-Standard:0, 53)

PGP Universal Server (ID d'événement : ADMIN\_DELETED\_USER)

Palo Alto Endpoint Security Manager (ID d'événement : User Deleted)

Pulse Secure Pulse Connect Secure (ID d'événement : SYN24849, ADM20722, ADM24473, SYN24745, SYN24850)

RSA Authentication Manager (ID d'événement : unknown, Deleted user, REMOVE\_ORPHANED\_PRINCIPALS, REMOTE\_PRINCIPAL\_DELETE, DELETE\_PRINCIPAL)

SIM Audit (ID d'événement : Configuration-UserAccount-AccountDeleted)

STEALTHbits StealthINTERCEPT (ID d'événement : Active DirectorycomputerObject DeletedTrueFalse, Active DirectoryuserObject DeletedTrueFalse, Console user/group deleted, Console user/group deleted)

SafeNet DataSecure/KeySecure (ID d'événement : Removed user)

Skyhigh Networks Cloud Security Platform (ID d'événement : 10017)

Solaris BSM (ID d'événement : delete user)

SonicWALL SonicOS (ID d'événement : 559, 1157, 1158)

Trend Micro Deep Security (ID d'événement : 651)

Universal DSM (ID d'événement : Computer Account Removed, User Account Removed)

VMware vCloud Director (ID d'événement : com/vmware/vcloud/event/user/remove, com/vmware/vcloud/event/user/delete)

Vormetric Data Security (ID d'événement : DAO0090I)

iT-CUBE agileSI (ID d'événement : AU8, U0)

## **UBA : Compte utilisateur créé et supprimé dans une courte période de temps**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Compte utilisateur créé et supprimé dans une courte période de temps

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

15

### **Description**

Détecte quand un compte utilisateur est créé et supprimé dans une courte période de temps.

## Règles de prise en charge

- BB:UBA : User Account Created
- BB:UBA : User Account Deleted
- BB:UBA : Common Event Filters

## Sources de données

### UBA : Compte inactif utilisé

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Compte inactif utilisé

### Activation par défaut

Oui

### Valeur senseValue par défaut

10

### Description

Détecte les connexions réussies avec un compte ayant été déterminé comme compte dormant (ou inactif).

### Règle de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

## Sources de données

Toute source de journaux prise en charge fournissant un nom d'utilisateur dans l'événement.

### UBA : Tentative d'utilisation d'un compte dormant

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Tentative d'utilisation d'un compte dormant

### Activation par défaut

Oui

### Valeur senseValue par défaut

15

### Description

Détecte les tentatives infructueuses de connexion avec un compte ayant été déterminé comme compte dormant (ou inactif).

## Règle de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Failures

## Sources de données

3Com 8800 Series Switch, APC UPS, AhnLab Policy Center APC, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CRE System, CRYPTOCARD CRYPTOSHIELD, Carbon Black Protection, Centrify Identity Platform, Centrify Infrastructure Services, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, CyberGuard TSP Firewall/VPN, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, ESET Remote Administrator, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Matrix K/N/S Series Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, Extreme XSR Security Routers, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, Forcepoint Sidewinder, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM Bluemix Platform, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Illumio Adaptive Security Platform, Imperva SecureSphere, Infoblox NIOS, Itron Smart Meter, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Lieberman Random Password Manager, LightCyber Magna, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Network Security Platform, McAfee ePolicy Orchestrator, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, Motorola SymbolAP, Netskope Active, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, Okta, OpenBSD OS, Open LDAP Software, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Palo Alto PA Series, Pirean Access: One, PostFix MailTransferAgent, ProFTPd Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Monitoring, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sun ONE LDAP, Sybase ASE, Symantec Encryption Management Server, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep

Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, Venustech Venusense Security Platform, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Compte expiré utilisé**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Compte expiré utilisé. (auparavant appelé UBA : Compte orphelin, révoqué ou suspendu utilisé)

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Indique qu'un utilisateur a tenté de se connecter à un compte désactivé ou ayant expiré sur un système local. Cette règle peut également indiquer qu'un compte a été compromis.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication to Expired Account

### **Sources de données**

Cisco CatOS for Catalyst Switches, Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Juniper Junos WebApp Secure, Microsoft IAS Server, Microsoft Windows Security Event Log

## **UBA : Première escalade de privilèges**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Première escalade de privilèges

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Indique qu'un utilisateur a exécuté un accès privilégié pour la première fois. Cette règle de production de rapports peut être désactivée pour permettre le contrôle du comportement de l'utilisateur à des fins de comparaison.

## Règle de prise en charge

BB:UBA : Privileged User, First Time Privilege Use (logic)

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series Pirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director,

VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Nouvelle utilisation du compte détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Nouvelle utilisation du compte détectée

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Fournit des fonctions de génération de rapport qui indiquent qu'un utilisateur s'est correctement connecté pour la première fois. Cette règle de production de rapport peut être désactivée temporairement à des fins de comparaison.

### **Règle de prise en charge**

BB:UBA : User First Time Access (logic)

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM

zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetalIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Activité nécessitant des privilèges suspecte (première utilisation d'un privilège observée)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Activité nécessitant des privilèges suspecte (première utilisation d'un privilège observée)

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Indique qu'un utilisateur a exécuté une action privilégiée qu'il n'avait jamais exécutée auparavant. Les observations sont conservées dans la mappe d'ensembles "UBA : Observed Activities by Low Level Category and Username".

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series Pirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Activité nécessitant des privilèges suspecte (privilège rarement utilisé)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Activité nécessitant des privilèges suspecte (privilège rarement utilisé)

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Indique qu'un utilisateur a exécuté une action privilégiée qu'il n'avait pas exécutée depuis longtemps. Les observations sont conservées dans la mappe d'ensembles "UBA : Recent Activities by Low Level Category and Username". La sensibilité de cet événement peut être modifiée en changeant la durée de vie de la mappe de référence d'ensembles de "UBA : Recent Activities by Low Level Category and Username". L'augmentation de la durée de vie réduit la sensibilité. La diminution de la durée de vie augmente la sensibilité.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:UBA : Privileged Activity

### **Sources de données**

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Application Security DbProtect, Arbor Networks Pravail, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Web Application Firewall, Bit9 Security Platform, Bluemix Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2,CA Top Secret, CRE System, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACSCisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco FireSIGHT Management Center, Cisco Firewall Services Module (FWSM), Cisco IOS,Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Cloudera Navigator, CorreLog Agent for IBM zOS, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, DG Technology MEAS, EMC VMWare, Enterasys Matrix K/N/S Series Switch, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme NAC, Extreme NetsightASM, F5 Networks BIG-IP APM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, H3C Comware Platform, HBGary Active Defense, HP Network Automation, Honeycomb Lexicon File Integrity Monitor, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower,IBM Fiberlink MaaS360, IBM Guardium, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Packet Capture, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Directory Server, IBM Security Identity Governance, IBM Security Identity Manager, IBM Security Trusteer Apex Advanced Malware Protection, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, ISC BIND, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS

Platform,Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper WirelessLAN, Juniper vGW, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance,McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Endpoint Protection, Microsoft Hyper-V, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft SharePoint, Microsoft Windows Security Event Log, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS,Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA SeriesPirean Access: One, PostFix MailTransferAgent, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Samhain HIDS, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center,Sybase ASE, Symantec Critical System Protection, Symantec Endpoint Protection, Symantec System Center, System Notification, ThreatGRID Malware Threat Intelligence Platform, TippingPoint Intrusion Prevention System (IPS),TippingPoint X Series Appliances, Top Layer IPS, Trend Micro Control Manager, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Discovery Inspector, Trend Micro Deep Security, Tripwire Enterprise, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Tentative de l'utilisateur d'utiliser un compte suspendu**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Tentative de l'utilisateur d'utiliser un compte suspendu

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Détecte qu'un utilisateur a tenté d'accéder à un compte suspendu ou désactivé.

### **Règles de prise en charge**

- BB:CategoryDefinition: Authentication to Disabled Account
- BB:UBA : Common Event Filters

### **Sources de données**

Cisco Intrusion Prevention System (IPS), Extreme Dragon Network IPS, IBM Proventia Network Intrusion Prevention System (IPS), Microsoft ISA, Microsoft Windows Security Event Log

## UBA : Utilisateur inactif (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge. A compter de la version 3.2.0, les informations concernant les comptes dormants sont visibles sur le tableau de bord UBA. Pour plus d'informations, consultez «Comptes dormants», à la page 41.

UBA : Utilisateur inactif (aucune règle d'anomalie d'activité)

UBA : Compte inactif détecté (avec des privilèges)

### Activation par défaut

Non

### Valeur senseValue par défaut

10

### Description

Avant d'activer cette règle, vérifiez que la règle "UBA : User Has Gone Dormant (no activity anomaly rule)" est activée.

Cette règle indique que l'activité d'un nom d'utilisateur a changé dans une proportion supérieure à 80 %. Les règles "UBA : Compte inactif détecté (avec des privilèges)" et "UBA : User Has Gone Dormant (no activity anomaly rule)" ont pour but d'indiquer qu'un utilisateur a arrêté son activité pendant une longue période. Cette condition peut signaler que l'utilisateur n'a plus besoin d'accès, comme cela est indiqué par une longue inactivité associée au nom d'utilisateur. Les fausses alarmes sont possibles si l'activité d'un nom d'utilisateur tombe à zéro durant une courte période (14 jours par défaut) et avant que zéro ne soit la nouvelle référence (28 jours par défaut). Elles n'affectent pas le score de risque d'un utilisateur si la limite de fréquence de réponse de la règle "UBA : Compte inactif détecté (avec des privilèges)" est égale ou supérieure à l'intervalle long par nom d'utilisateur.

**Remarque :** Les fausses alarmes sont possibles pour 'UBA : User Has Gone Dormant (no activity anomaly rule)' si l'activité d'un nom d'utilisateur tombe à zéro durant une courte période (14 jours par défaut) et avant que zéro soit la nouvelle référence (28 jours par défaut). Les fausses alarmes n'affectent pas le score de risque d'un utilisateur si la limite de fréquence de réponse de "UBA : Compte inactif détecté (avec des privilèges)" est définie sur une période égale ou supérieure à l'intervalle long par nom d'utilisateur.

### Règle de prise en charge

UBA : Compte inactif détecté (avec des privilèges)

### Configuration requise

Activez la règle suivante : "UBA : Compte inactif détecté (avec des privilèges)".

### Sources de données

Toutes les sources de journaux prises en charge.

---

## Comportement de navigation

### **UBA : Accès à un site web commercial/de services**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès à un site web commercial/de services

#### **Activation par défaut**

Oui

#### **Valeur senseValue par défaut**

5

#### **Description**

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### **Règle de prise en charge**

BB:UBA : URL Category Filter

#### **Sources de données**

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### **UBA : Accès à un site web de communication**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès à un site web de communication

#### **Activation par défaut**

Oui

#### **Valeur senseValue par défaut**

5

#### **Description**

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### **Règle de prise en charge**

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

## UBA : Accès à un site web de divertissement

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web de divertissement

### Activation par défaut

Oui

### Valeur senseValue par défaut

5

### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

## UBA : Accès à un site web de jeux d'argent

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web de jeux d'argent

### Activation par défaut

Oui

### Valeur senseValue par défaut

5

### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Accès à un site web d'informatique

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web d'informatique

#### Activation par défaut

Oui

#### Valeur senseValue par défaut

5

#### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Accès à un site web de recherche d'emploi

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web de recherche d'emploi

#### Activation par défaut

Oui

#### Valeur senseValue par défaut

15

#### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Accès à un site web sur le mode de vie

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès à un site web sur le mode de vie

#### Activation par défaut

Oui

#### Valeur senseValue par défaut

5

#### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Accès à un site web malveillant

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web malveillant

#### Activation par défaut

Oui

#### Valeur senseValue par défaut

15

#### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

## UBA : Accès à un site web de contenu mixte/potentiellement pour adultes

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web de contenu mixte/potentiellement pour adultes

### Activation par défaut

Oui

### Valeur senseValue par défaut

10

### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

## UBA : Accès à un site web de hameçonnage

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web de hameçonnage

### Activation par défaut

Oui

### Valeur senseValue par défaut

15

### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### **UBA : Accès à un site web pornographique**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web pornographique

#### **Activation par défaut**

Oui

#### **Valeur senseValue par défaut**

10

#### **Description**

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### **Règle de prise en charge**

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### **UBA : Accès à un site web frauduleux/douteux/illégal**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un site web frauduleux/douteux/illégal

#### **Activation par défaut**

Oui

#### **Valeur senseValue par défaut**

5

#### **Description**

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### **Règle de prise en charge**

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Accès à un site web non catégorisé

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès à un site web non catégorisé

#### Activation par défaut

Oui

#### Valeur senseValue par défaut

5

#### Description

Un utilisateur a accédé à une URL pouvant présenter un risque juridique ou de sécurité élevé.

#### Règle de prise en charge

BB:UBA : URL Category Filter

## Sources de données

Blue Coat SG Appliance, Cisco IronPort, McAfee Web Gateway, Check Point, Squid Web Proxy, Palo Alto PA Series

### UBA : Utilisateur accédant à une URL risquée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA: Utilisateur accédant à une URL risquée (auparavant appelée URL risquée X-Force)

#### Activation par défaut

Oui

#### Description

Cette règle détecte quand un utilisateur local accède à un contenu en ligne douteux.

#### Règles de prise en charge

- X-Force Risky URL
- BB:UBA : Common Event Filters

#### Configuration requise

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky URL.

## Sources de données

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

## Cloud

### UBA : Accès à la console AWS par un utilisateur non autorisé

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à la console AWS par un utilisateur non autorisé

#### Activation par défaut

Non

#### Valeur senseValue par défaut

10

#### Description

Détecte toute tentative d'accès non autorisé à la console AWS (Amazon Web Services) par un utilisateur qui n'est pas sur la liste des utilisateurs autorisés dans l'ensemble de référence 'AWS - Utilisateurs standard'.

#### Règles de prise en charge

BB:UBA : Common Event Filters

#### Configuration requise

- Installez le package suivant de l'IBM Security App Exchange : IBM QRadar Content Extension for Monitoring Amazon AWS.
- Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Domain Controller Administrators". Configurez la source de journaux suivante : Amazon AWS Cloudtrail

## Sources de données

Amazon AWS CloudTrail (ID d'événement : ConsoleLogin)

### UBA : Utilisateur non standard accédant à des ressources AWS

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Utilisateur non standard accédant à des ressources AWS

#### Activation par défaut

Non

#### Valeur senseValue par défaut

10

## Description

Détecte un utilisateur standard tentant d'accéder à des ressources AWS (Amazon Web Services).

## Source de données

Amazon Web Services Extension

---

## Contrôleur de domaine

### **UBA : Tentative de récupération de clé principale de secours DPAPI**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Tentative de récupération de clé principale de secours DPAPI

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

## Description

Détecte les cas où une récupération est tentée pour une clé principale DPAPI.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Source de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4693)

### **UBA : Enumération de comptes Kerberos détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Enumération de comptes Kerberos détectée

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

## Description

Détecte les tentatives d'énumération de comptes en repérant les cas d'utilisation d'un grand nombre de noms d'utilisateur différents pour des demandes Kerberos émises depuis une même IP source.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Source de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4768)

## UBA : Plusieurs échecs d'authentification Kerberos pour le même utilisateur

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Plusieurs échecs d'authentification Kerberos pour le même utilisateur

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte les rejets ou les échecs multiples des tickets d'authentification Kerberos.

## Règle de prise en charge

- BB:UBA : Common Log Source Filters
- BB:UBA : Kerberos Authentication Failures

## Sources de données

Journal des événements de sécurité Microsoft Windows

## UBA : Accès non administrateur au contrôleur de domaine

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès non administrateur au contrôleur de domaine

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Détecte les tentatives d'accès non administrateur au contrôleur de domaine.

## Règle de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- BB:CategoryDefinition: Authentication Failures

## Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants : "UBA : Domain Controllers" et "UBA : Domain Controller Administrators"

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication

Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## **UBA : Attaque Pass-the-Hash**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Attaque Pass-the-Hash

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte les événements de connexion Windows pouvant être générés lors d'attaques exploitant les hachages.

### **Règle de prise en charge**

BB:UBA : Common Event Filters

### **Configuration requise :**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : UBA : Trusted Domains.

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4624)

## **UBA : Possible énumération de services d'annuaires**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Possible énumération de services d'annuaires

### **Activation par défaut**

Non

## Valeur senseValue par défaut

5

### Description

Détecte les tentatives de reconnaissance par énumération des services d'annuaire.

### Règle de prise en charge

BB:UBA : Common Event Filters

### Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Domain Controller Administrators"

### Source de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4661)

## UBA : Possible énumération des sessions SMB sur un contrôleur de domaine.

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Possible énumération des sessions SMB sur un contrôleur de domaine.

### Activation par défaut

Non

## Valeur senseValue par défaut

10

### Description

Détecte les tentatives d'énumération des sessions SMB sur un contrôleur de domaine.

### Règle de prise en charge

BB:UBA : Common Event Filters

### Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants :

- UBA : Domain Controllers
- UBA : Domain Controller Administrators

### Source de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 5140)

## **UBA : Falsification possible des tickets d'octroi d'autorisations**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Falsification possible des tickets d'octroi d'autorisations

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte les tickets d'octroi Kerberos qui incluent des anomalies liées au nom de domaine. Ces anomalies peuvent indiquer des tickets générés via des attaques Pass-The-Ticket.

### **Règle de prise en charge**

BB:UBA : Common Event Filters

### **Configuration requise**

Ajoutez les valeurs appropriées aux ensembles de référence suivants : UBA : Trusted Domains.

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4768)

## **UBA : Falsification possible des tickets d'octroi d'autorisations avec un PAC**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Falsification possible des tickets d'octroi d'autorisations avec un PAC

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte les cas d'utilisation d'un certificat d'attribut de privilège (PAC) falsifié pour obtenir un ticket de service du service d'octroi d'autorisations (TGS) Kerberos.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:UBA : TCT PAC Forgery Patched Server

- BB:UBA : TCT PAC Forgery Unpatched Server

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Domain Controller Administrators".

### **Source de données**

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4672, 4769)

### **UBA : Demande de réplication d'un contrôleur autre que de domaine**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Demande de réplication d'un contrôleur autre que de domaine

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Détecte les demandes de réplication émanant d'un contrôleur de domaine illégitime

### **Règles de prise en charge**

BB:UBA : Common Event Filters

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Domain Controller Administrators".

### **Source de données**

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4662)

### **UBA : TGT Ticket Used by Multiple Hosts**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : TGT Ticket Used by Multiple Hosts

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

## Description

Détecte les cas d'utilisation de tickets d'octroi d'autorisations Kerberos sur plusieurs ordinateurs.

## Règle de prise en charge

BB:UBA : Common Event Filters

UBA : Kerberos Account Mapping

Cette règle met à jour les ensembles de référence associés avec les données requises.

## Configuration requise

Activez les règles suivantes : "UBA : Kerberos Account Mapping"

## Sources de données

Journal des événements de sécurité Microsoft Windows (ID d'événement : 4768)

---

## Point d'extrémité

### UBA : Détecter un protocole non sécurisé ou non standard

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Détecter un protocole non sécurisé ou non standard

### Activation par défaut

Non

### Valeur senseValue par défaut

5

## Description

Détecte les utilisateurs qui communiquent via des protocoles non autorisés considérés comme non fiables ou non standard. Les protocoles autorisés sont répertoriés dans l'ensemble de référence UBA : Ports of Authorized Protocols avec la valeur par défaut 0, qui est le port des événements QRadar. Modifiez l'ensemble de référence UBA : Ports of Authorized Protocols à marquer dans votre environnement avant d'activer cette règle.

## Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : Insecure Ports
- 

## Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : UBA : Ports Of Authorized Protocols.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Détecter les sessions SSH persistantes

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Détecter les sessions SSH persistantes

### Activation par défaut

Oui

### Valeur senseValue par défaut

10

### Description

Détecte les sessions SSH actives pendant plus de dix heures.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : SSH Session Closed
- BB:UBA : SSH Session Opened

### Configuration requise

Pour une détection précise, cette règle requiert l'occurrence des deux événements SSH Opened et SSH Closed. Si la source de journaux utilisée ne comporte pas l'eventID correspondant à chacun de ces deux événements, les résultats reçus risquent d'être inexacts. Consultez la liste des sources de données pour déterminer les ID d'événement de la source de journaux utilisée.

### Source de données (SSH Opened)

Centrify Infrastructure Services (ID d'événement : 27100, 27104)

Cisco IOS (ID d'événement : %SSH-5-SSH2\_SESSION, %SSH-SW2-5-SSH2\_SESSION)

Custom Rule Engine (ID d'événement : 18037, 3071)

Cyber-Ark Vault (ID d'événement : 378)

Extreme XSR Security Routers (ID d'événement : NEW\_SSH\_CONNECTION)

Flow Classification Engine (ID d'événement : 3071, 18037)

Huawei S Series Switch (ID d'événement : SSH/4/SFTP\_REQ\_RECORD)

HyTrust CloudControl (ID d'événement : AUN0120, unknown)

IBM AIX Server (ID d'événement : sshd2 connection established, ssh-server connect, ssh-server session open)

IBM DataPower (ID d'événement : 0x8100011e, 0x810001e4, 0x810001e5)

Juniper MX Series Ethernet Services Router (ID d'événement : SSH)

Juniper Networks AVT (ID d'événement : SSH)

Mac OS X (ID d'événement : OSX ssh session started)

OS Services Qidmap (ID d'événement : Connection from, pam\_open\_session, pam\_sm\_open\_session)

Solaris Operating System Authentication Messages (ID d'événement : ssh session opened)

Universal DSM (ID d'événement : SSH Opened, SSH Session Started)

### **Source de données (SSH Closed)**

Aruba Mobility Controller (ID d'événement : sshd\_disconnect)

Centrify Infrastructure Services (ID d'événement : 27102)

Cisco IOS (ID d'événement : %SSH-5-SSH\_CLOSE, %SSH-SW2-5-SSH2\_CLOSE, %SSH-5-SSH2\_CLOSE)

Custom Rule Engine (ID d'événement : 3072, 18038, 18040)

Cyber-Ark Vault (ID d'événement : 380, 381)

Flow Classification Engine (ID d'événement : 3072, 18038, 18040)

Huawei S Series Switch (ID d'événement : SSH/6/RECV\_DISCONNECT)

IBM AIX Server (ID d'événement : ssh-server disconnect, sshd2 connection lost, SSH Disconnect, sshd2 local disconnect, ssh-server session close)

OS Services Qidmap (ID d'événement : Done with connection, pam\_sm\_close\_session, pam\_close\_session, Did not receive identification string, Connection timed out, Received disconnect from IP, Connection closed)

Pulse Secure Pulse Connect Secure (ID d'événement : GWE24572)

Universal DSM (ID d'événement : SSH Terminated, SSH Session Finished, SSH Closed)

### **UBA : Paramètres Internet modifiés**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Paramètres Internet modifiés

#### **Activation par défaut**

Oui

#### **Valeur senseValue par défaut**

15

## Description

Détecte les modifications des paramètres Internet sur le système.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4657)

## UBA : Activité de logiciel malveillant - Registre modifié en vrac

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activité de logiciel malveillant - Registre modifié en vrac

## Activation par défaut

Oui

## Valeur senseValue par défaut

15

## Description

Détecte les processus qui modifient plusieurs valeurs de registre en bloc dans un court intervalle.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4657)

## UBA : Détection de processus Netcat (Linux)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Détection de processus Netcat (Linux)

## Activation par défaut

Oui

## Valeur senseValue par défaut

15

## Description

Détecte un processus netcat sur un système Linux.

## Règle de prise en charge

BB:UBA : Common Log Source Filters

### Sources de données

Système d'exploitation Linux (ID d'événement : SYSCALL)

## UBA : Détection de processus Netcat (Windows)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Détection de processus Netcat (Windows)

### Activation par défaut

Oui

### Valeur senseValue par défaut

15

### Description

Détecte un processus Netcat sur un système Windows.

## Règle de prise en charge

BB:UBA : Common Event Filters

### Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4688)

## UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Linux)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Linux)

### Activation par défaut

Non

### Valeur senseValue par défaut

15

### Description

Détecte les processus créés sur un système Linux et émet une alerte lorsque le processus se trouve hors de la liste blanche du processus de disque d'or.

**Remarque :** Cette règle est désactivée par défaut. Activez la règle uniquement lorsque vous chargez ou modifiez les noms de processus à placer sur liste blanche dans l'ensemble de référence 'UBA : Gold Disk Process Whitelist - Linux'.

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Gold Disk Process Whitelist - Linux".

### **Règle de prise en charge**

BB:UBA : Common Log Source Filters

### **Sources de données**

Système d'exploitation Linux (ID d'événement : SYSCALL)

## **UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Windows)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Processus exécuté en dehors de la liste blanche Gold Disk (Windows)

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte les processus créés sur un système Windows et émet une alerte lorsque le processus est hors de la liste blanche du processus de disque d'or.

**Remarque :** Cette règle est désactivée par défaut. Activez la règle uniquement lorsque vous chargez ou modifiez les noms de processus à placer sur liste blanche dans l'ensemble de référence 'UBA : Gold Disk Process Whitelist - Windows'.

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Gold Disk Process Whitelist - Windows".

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4688)

## **UBA : Comportement de rançongiciel détecté**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Comportement de rançongiciel détecté

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte un comportement généralement observé lors d'une infection par un rançongiciel.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Windows Common Processes".

## Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4663)

## UBA : Utilisation du programme restreinte

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisation du programme restreinte

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Indique qu'un processus a été créé et que son nom correspond à l'un des noms binaires répertoriés dans l'ensemble de références "UBA : Restricted Program Filenames". Cet ensemble de références est vide par défaut pour que vous puissiez le personnaliser. Vous pouvez alimenter l'ensemble de références avec les noms de fichiers que vous souhaitez contrôler dans le cadre d'une gestion des risques.

Pour plus d'informations sur l'ajout ou la suppression de programmes de surveillance, voir [Managing restricted programs](#).

## Règle de prise en charge

BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Restricted Program Filenames".

## Sources de données

Journal des événements de sécurité Microsoft Windows

## UBA : Utilisateur installant une application suspecte

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

Prend en charge les règles suivantes :

- UBA : Utilisateur installant une application suspecte
- UBA : Populate Authorized Applications

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte les événements d'installation d'application, puis génère une alerte lorsque des applications suspectes sont détectées. Remarque : Remplissez l'ensemble de référence "UBA : Authorized Applications" avec les noms d'application autorisées dans l'organisation. La règle "UBA : Populate Authorized Applications" peut être activée pendant une courte durée pour remplir cet ensemble de référence.

La règle "UBA : Populate Authorized Applications" remplit l'ensemble de référence "UBA : Authorized Applications" avec les noms des applications installées alors que cette règle est activée. Remarque : La règle est désactivée par défaut. Activez-la pendant une durée pour courte pour remplir les noms lorsque les utilisateurs installent des applications.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

## UBA : Utilisateur exécutant un nouveau processus

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

Prend en charge les règles suivantes :

- UBA : Utilisateur exécutant un nouveau processus
- UBA : Populate Process Filenames

## Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte les processus créés par l'utilisateur, puis alerte lorsqu'un utilisateur exécute un nouveau processus.

La règle "UBA : Populate Process Filenames" remplit l'ensemble de référence "UBA : Process Filenames" utilisé comme règle utilitaire pour "UBA : Utilisateur exécutant un nouveau processus." Remarque : La règle est désactivée par défaut. Activez la règle pendant une durée plus courte pour remplir les noms de fichier.

### Règle de prise en charge

BB:UBA : Common Event Filters, UBA : Populate Process Filenames

### Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : "UBA : Process Filenames".

### Sources de données

Journaux d'événements système Microsoft Windows (ID d'événement : 4688)

## UBA : Copie miroir d'un volume créée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Copie miroir d'un volume créée

### Activation par défaut

Oui

## Valeur senseValue par défaut

15

### Description

Détecte les copies miroir créées en utilisant vssadmin.exe ou la ligne de commande WMIC (Windows Management Instrumentation Command-line).

### Règle de prise en charge

BB:UBA : Common Event Filters

### Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 1 ou 4688)

---

## Exfiltration

### UBA : Abnormal data volume to external domain (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

**Remarque :** Cette règle a été remplacée par l'analyse Machine Learning suivante : Volume anormal de données circulant vers des domaines externes.

- UBA : Abnormal data volume to external domain
- UBA : Abnormal data volume to external domain Found

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

### Activation par défaut

Non

### Valeur senseValue par défaut

15

### Description

**UBA : Abnormal data volume to external domain** Cette règle utilise le moteur de détection des anomalies pour surveiller le trafic utilisateur et envoyer une alerte lorsque le volume de données du trafic vers les domaines externes est anormal.

**UBA : Abnormal data volume to external domain Found** Règle CRE prenant en charge la règle ADE correspondante UBA: Abnormal data volume to external domain, qui utilise le moteur de détection des anomalies pour surveiller le trafic utilisateur et signaler des volumes de données anormaux pour le trafic vers des domaines externes.

### Sources de données

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

### UBA : Tentatives de transfert sortant anormales (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

**Remarque :** Cette règle a été remplacée par l'analyse Machine Learning suivante : Tentatives de transfert sortant anormales. Pour plus d'informations, voir «Configuration de l'analyse *Tentatives de transfert sortant anormales*», à la page 180.

UBA : Abnormal Outbound Transfer Attempts ("UBA : Abnormal Outbound Attempts" dans V2.4.0)

UBA : Abnormal Outbound Transfer Attempts Found

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

**UBA : Abnormal Outbound Transfer Attempts (règle ADE)** Cette règle utilise le moteur de détection des anomalies pour surveiller le trafic et envoyer une alerte lorsque le nombre de tentatives est anormal.

**UBA : Abnormal Outbound Transfer Attempts Found** Règle CRE prenant en charge la règle ADE correspondante UBA : Abnormal Outbound Attempts, qui utilise le moteur de détection des anomalies pour surveiller le trafic et envoyer une alerte lorsque le nombre de tentatives est anormal.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Transfert sortant volumineux effectué par un utilisateur à haut risque

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Transfert sortant volumineux effectué par un utilisateur à haut risque

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte un transfert sortant d'au moins 200 000 octets par un utilisateur à risque élevé.

## Règles de prise en charge

BB:UBA : Common Event Filters

## Sources de données

Sources de journaux pour lesquelles CEP BytesSent est défini.

## UBA : Plusieurs transferts de fichier bloqués suivis d'un transfert de fichier réussi

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Plusieurs transferts de fichier bloqués suivis d'un transfert de fichier réussi

## Activation par défaut

Oui

## Valeur senseValue par défaut

10

## Description

Détecte les exfiltrations en vérifiant si, sur une période de 5 minutes, des transferts de fichiers initialement bloqués ont été suivis d'un transfert réussi.

## Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : Blocked File Transfer
- BB:UBA : Successful File Transfer

## Configuration requise

Pour une détection précise, cette règle requiert l'occurrence des deux événements Blocked file transfers (transferts de fichier bloqués) et Successful file transfers (transferts de fichier réussis). Si la source de journaux utilisée ne comporte pas l'eventID correspondant à chacun de ces deux événements, les résultats reçus risquent d'être inexacts. Consultez la liste des sources de données pour déterminer les ID d'événement de la source de journaux utilisée.

## Sources de données (Blocked file transfers)

Cilasoft QJRN/400 (ID d'événement : C21020)

Cisco Call Manager (ID d'événement : %UC\_DRF-3-DRFSftpFailure)

Cisco IOS (ID d'événement : %UPDATE-3-SFTP\_TRANSFER\_FAIL)

Custom Rule Engine (ID d'événement : 18014, 18071, 18187, 4032)

Extreme Stackable and Standalone Switches (ID d'événement : FFTP request failed)

Flow Classification Engine (ID d'événement : 4032, 18187, 18014, 18071)

Forcepoint Sidewinder (ID d'événement : FTP Permits, denied ftp command)

IBM i (ID d'événement : UNR0907, UNR0908, UNR2302, GSL0118, GSL0119, GSL0318, GSL0319, GSL3718, GSL3719, GSL0618, UNR0701, UNR0707, UNR0901, UNR0910, UNR2301, UNR0705, UNR0706, UNR0708, UNR0710, UNR0801, UNR0802, UNR0905, UNR0906, GSL0619)

Juniper Networks Intrusion Detection and Prevention (IDP) (ID d'événement : TFTP:AUDIT:READ-FAILED)

Microsoft IIS (ID d'événement : 530)

Microsoft Operations Manager (ID d'événement : 22095)

OSSEC (ID d'événement : 11504, 11512)

Universal DSM (ID d'événement : FTP Action Denied, TFTP Session Denied,FTP Denied,FileTransfer Denied)

WatchGuard Fireware OS (ID d'événement : 1CFF0002,1CFF0006,1CFF0007,1CFF0009, 1CFF0001,1CFF0019, 1CFF0000, 1CFF0003)

### **Sources de données (Successful file transfers)**

Cilasoft QJRN/400 (ID d'événement : C21031)

Cisco FireSIGHT Management Center (ID d'événement : FILE\_EVENT, FILE\_EVENT\_0)

Cisco IOS (ID d'événement : %FTPSERVER-6-NEWCONN)

Cisco IronPort (ID d'événement : FTP\_connection)

Custom Rule Engine (ID d'événement : 18010, 4031,18431, 18183)

DG Technology MEAS (ID d'événement : 119-003, 119-070)

Flow Classification Engine (ID d'événement : 18010, 4031,18431, 18183)

Flow Device Type (ID d'événement : 21984, 21879, 51337, 51336, 35159, 21910)

Huawei S Series Switch (ID d'événement : FTPS/5/REQUEST)

IBM Proventia Network Intrusion Prevention System (IPS) (ID d'événement : FTP, TFTP)

IBM i (ID d'événement : MLD1200, MLD2100, MO10300,MO10400, MO11800, MO12100, MO12400, MO20200, MO20300, MO21300, MO21800, MO21900, GSL0101, GSL0102, GSL0301, GSL0302, GSL3701,GSL3702, M090100, UNA0705, UNA0706, UNA0708, UNA0710, UNA0801, UNA0802, UNA0905, UNA0906, UNA0907,UNA0908, UNA2302,UNA0601, UNA0604, UNA0605, UNA0607, UNA0701, UNA0707, UNA0901, UNA0902, UNA0910, UNA2301, M030100, MLD1100)

Juniper MX Series Ethernet Services Router (ID d'événement : TFTP, FTP)

Juniper Networks AVT (ID d'événement : TFTP, FTP)

Microsoft IIS (ID d'événement : 150, 125, 225)

ProFTPD Server (ID d'événement : FTP session opened)

Solaris Operating System Authentication Messages (ID d'événement : ftp connection)

SonicWALL SonicOS (ID d'événement : 1112, 1113)

Squid Web Proxy (ID d'événement : 3C0002\_ALLOWED)

Trend InterScan VirusWall (ID d'événement : Trend ftpconnect)

Universal DSM (ID d'événement : File Transfer, FTP Opened, FTP Action Allowed, TFTP Session Opened)

Verdasys Digital Guardian (ID d'événement : Network Transfer Upload, Network Transfer Download)

WatchGuard Fireware OS (ID d'événement : 2AFF0004, 1CFF0019)

## UBA : Accès suspects suivis d'une exfiltration de données

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès suspects suivis d'une exfiltration de données

### Activation par défaut

Non

### Valeur senseValue par défaut

10

### Description

Détecte les accès depuis des endroits inhabituels, restreints ou interdits, suivis d'une tentative d'exfiltration de données.

### Règle de prise en charge

- BB:UBA : Common Event Filters
- BB:UBA : Exfiltration de données
- UBA : Accès utilisateur depuis un emplacement restreint
- UBA : Accès utilisateur depuis un emplacement interdit
- UBA : Zone géographique de l'utilisateur, Accès depuis des emplacements inhabituels

### Configuration requise

Activez les règles suivantes :

- UBA : Accès utilisateur depuis un emplacement restreint
- UBA : Accès utilisateur depuis un emplacement interdit
- UBA : Zone géographique de l'utilisateur, Accès depuis des emplacements inhabituels

### Source de données

Cisco Stealthwatch (ID d'événement : 45)

IBM Security Trusteer Apex Advanced Malware Protection (ID d'événement : ConnectionCreate.Connection\_Test, CerberusNG.ent\_create\_remote\_thread, ConnectionCreate.in\_suspend\_state, ConnectionCreate.orphan\_thread\_connect, close.file\_inspection, processcreate.file\_inspection)

Skyhigh Networks Cloud Security Platform (ID d'événement : 10003, 10004)

## UBA : Anomalies liées aux volumes utilisateur - Détection du trafic vers des domaines externes (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge.

- UBA : User Volume Activity Anomaly - Traffic to External Domains
- UBA : User Volume Activity Anomaly - Traffic to External Domains Found

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

**UBA : User Volume Activity Anomaly - Traffic to External Domains** Règle CRE prenant en charge la règle ADE correspondante, UBA : User Volume of Activity Anomaly - Traffic, qui utilise le moteur de détection des anomalies pour surveiller le trafic utilisateur et alerter sur les volumes de trafic anormaux.

**UBA : User Volume Activity Anomaly - Traffic to External Domains Found** Règle CRE prenant en charge la règle correspondante, UBA : User Volume Activity Anomaly - Traffic to External Domains, qui utilise le moteur de détection des anomalies pour surveiller l'utilisation de trafic sortant et alerter sur les nombres de tentatives anormaux.

## Sources de données

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

## Géographie

### UBA : Compte erroné créé depuis un nouvel emplacement

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Compte erroné créé depuis un nouvel emplacement

## Activation par défaut

Oui

## Valeur senseValue par défaut

5

## Description

Détecte toute activité de création de compte erroné créé depuis un nouvel emplacement.

## Règles de prise en charge

- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created
- BB:UBA : Common Event Filters
- UBA : Changement de zone géographique de l'utilisateur

## Configuration requise

Activez la règle suivante : "UBA : Changement de zone géographique de l'utilisateur".

## Sources de données

AhnLab Policy Center APC (ID d'événement : Administrator Account Add:Succeeded, ADD\_ADMIN\_ACCOUNT\_SUCCESS)

Application Security DbProtect (ID d'événement : Database user created, Login created - standard, Login added - Windows, Database role - created)

Aruba Mobility Controller (ID d'événement : authmgr\_user\_add)

Bit9 Security Platform (ID d'événement : User\_group\_created, User\_group\_modified, User\_group\_deleted, Console\_user\_created, Console\_user\_modified, Console\_user\_deleted)

Box (ID d'événement : NEW\_USER)

Brocade FabricOS (ID d'événement : SEC-1180,SEC-3025, SEC-1182)

CA ACF2 (ID d'événement : ACF2-L)

Check Point (ID d'événement : User Added, device\_added)

Cilasoftware QJRN/400 (ID d'événement : C20010, C20011)

Cisco Adaptive Security Appliance (ASA) (ID d'événement : %PIX|ASA-5-502101, %ASA-5-502101)

Cisco Firewall Services Module (FWSM) (ID d'événement : 502101, 504001)

Cisco IOS (ID d'événement : %APF-6-USER\_NAME\_CREATED)

Cisco Identity Services Engine (ID d'événement : 86006)

Cisco NAC Appliance (ID d'événement : CCA-1500)

Cisco PIX Firewall (ID d'événement : %PIX-0-502101, %PIX-1-502101, %PIX-2-502101, %PIX-3-502101, %PIX-4-502101, %PIX-5-502101, %PIX-6-502101, %PIX-7-502101)

Cisco PIX Firewall (ID d'événement : 502101)

Cisco Wireless LAN Controllers (ID d'événement : %APF-6-USER\_NAME\_CREATED, 1.3.6.1.4.1.9.9.515.0.2)

Cisco Wireless Services Module (WiSM) (ID d'événement : %AAA-6-GUEST\_ACCOUNT\_CREATE, %APF-6-USER\_NAME\_CREATED)

CloudPassage Halo (ID d'événement : Halo user added, Halo user re-added, Local account created (linux only))

CorreLog Agent for IBM zOS (ID d'événement : RACF ADDUSER: No Violations)

Cyber-Ark Vault (ID d'événement : 180, 2)

EMC VMWare (ID d'événement : AccountCreatedEvent)

Extreme Dragon Network IPS (ID d'événement : HOST:WIN:ACCOUNT-CREATED)

Extreme Matrix K/N/S Series Switch (ID d'événement : created with, User Created Event)

Extreme NAC (ID d'événement : Added registered user, Add Registered User)

Flow Classification Engine (ID d'événement : 3031, 3041)

Forcepoint Sidewinder (ID d'événement : passport addition)

Fortinet FortiGate Security Gateway (ID d'événement : add, auth-logon)

Foundry Fastiron (ID d'événement : SNMP\_USER\_ADDED)

HBGary Active Defense (ID d'événement : CreateUser)

HP Network Automation (ID d'événement : User Added)

IBM AIX Audit (ID d'événement : USER\_Create SUCCEEDED)

IBM AIX Server (ID d'événement : USER\_Create)

IBM DB2 (ID d'événement : ADD\_USER SUCCESS)

IBM IMS (ID d'événement : USER CREATED)

IBM QRadar Packet Capture (ID d'événement : UserAdded)

IBM Resource Access Control Facility (RACF) (ID d'événement : 80 10.0, 80 10.2)

IBM Security Access Manager for Enterprise Single Sign-On (ID d'événement : PRE\_PROVISION\_IMS\_USER, AA\_SCR\_REGISTRATION, REGISTER\_MAC\_IDENTITY, REGISTER\_IDENTITY)

IBM Security Directory Server (ID d'événement : SDS Audit)

IBM Security Identity Governance (ID d'événement : 49, 70004, 42)

IBM Security Identity Manager (ID d'événement : Add Success, Add SUBMITTED, Add SUCCESS)

IBM SmartCloud Orchestrator (ID d'événement : user)

IBM Tivoli Access Manager for e-business (ID d'événement : 13402 - Succeeded, 13401 - Succeeded, 13402 Command Succeeded, 13401 Command Succeeded)

IBM i (ID d'événement : GSL2401,MC@0300, GSL2402, M240100, CP\_CRT)

Imperva SecureSphere (ID d'événement : NEW\_USERS\_ACCOUNT, SOX\_NEW\_USERS, SOX - New users, New Users Account)

Itron Smart Meter (ID d'événement : CEUI-AUDIT-27, CEUI.AUDIT.26)

Juniper Networks Network and Security Manager (ID d'événement : adm23303, aut20167, adm30407, aut20168, adm20716, adm20717)

Linux OS (ID d'événement : ADD\_USER)

McAfee Application/Change Control (ID d'événement : USER\_ACCOUNT\_CREATED)

McAfee ePolicy Orchestrator (ID d'événement : 20792)

Microsoft ISA (ID d'événement : user added)

Microsoft SQL Server (ID d'événement : CR - SU, CR - US, CR - SL, CR - LX, CR - AR, CR - WU, 24127, 24121, 24075)

Microsoft SharePoint (ID d'événement : 37)

Microsoft Windows Security Event Log (ID d'événement : 624, 645, 1318, 4720, 4741)

NCC Group DDos Secure (ID d'événement : 1003)

Netskope Active (ID d'événement : Create Admin, Created new admin)

Novell eDirectory (ID d'événement : CREATE\_ACCOUNT)

OS Services Qidmap (ID d'événement : User Account Added)

OSSEC (ID d'événement : 5902, 18110)

Okta (ID d'événement : app.user\_management.push\_new\_user\_success, app.generic.import.details.add\_user, app.generic.import.new\_user, app.user\_management.provision\_user, app.user\_management.push\_new\_user, app.user\_management.push\_profile\_success, core.user.config.user\_creation.success, core.user\_group\_member.user\_add, cvd.user\_profile\_bootstrapped, cvd.appuser\_profile\_bootstrapped)

OpenBSD OS (ID d'événement : add user)

Oracle Enterprise Manager (ID d'événement : User Create (successful), Computer Create (successful))

Oracle RDBMS Audit Record (ID d'événement : 51:1, 51:0, CREATE USER-Standard:1, CREATE USER-Standard:0)

Oracle RDBMS OS Audit Record (ID d'événement : 51)

Pirean Access: One (ID d'événement : IsimUserRegistration;\*,1)

Pulse Secure Pulse Connect Secure (ID d'événement : ADM23303, ADM20265, AUT20167, ADM30407, AUT20168)

RSA Authentication Manager (ID d'événement : Added user, unknown, REMOTE\_PRINCIPAL\_CREATE, CREATE\_PRINCIPAL, CREATE\_AM\_PRINCIPAL)

SIM Audit (ID d'événement : Configuration-UserAccount-AccountAdded)

STEALTHbits StealthINTERCEPT (ID d'événement : Active DirectorycomputerObject AddedTrueFalse, Console ? user/group added, Console ∆ user/group added, Active DirectoryuserObject AddedTrueFalse, Console - user/group added)

SafeNet DataSecure/KeySecure (ID d'événement : Added user)

Salesforce Security Auditing (ID d'événement : Created new Customer User, Created new user)

Skyhigh Networks Cloud Security Platform (ID d'événement : 10016)

Solaris BSM (ID d'événement : create user)

SonicWALL SonicOS (ID d'événement : 558)

Symantec Encryption Management Server (ID d'événement : ADMIN\_IMPORTED\_USER)

ThreatGRID Malware Threat Intelligence Platform (ID d'événement : user-account-creation)

Trend Micro Deep Discovery Email Inspector (ID d'événement :  
SYSTEM\_EVENT\_ACCOUNT\_CREATED)

Trend Micro Deep Security (ID d'événement : 650)

Universal DSM (ID d'événement : Computer Account Added, User Account Added)

VMware vCloud Director (ID d'événement : com/vmware/vcloud/event/user/create,  
com/vmware/vcloud/event/user/import)

Vormetric Data Security (ID d'événement : DAO0089I)

iT-CUBE agileSI (ID d'événement : U0, AU7)

## **UBA : Compte de cloud erroné créé depuis un nouvel emplacement**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Compte de cloud erroné créé depuis un nouvel emplacement

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

10

### **Description**

Détecte des activités de création de compte de cloud depuis un nouvel emplacement.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:UBA : Cloud Endpoints
- BB:UBA : User Account Created
- UBA : Changement de zone géographique de l'utilisateur

### **Configuration requise**

Activez la règle suivante : "UBA : Changement de zone géographique de l'utilisateur".

### **Sources de données**

Amazon AWS CloudTrail (ID d'événement : CreateUser)

Microsoft Office 365 (ID d'événement : Add User-success, Add user-PartiallySucceeded)

## UBA : Accès utilisateur depuis des emplacements différents

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Accès utilisateur depuis des emplacements différents

### Activation par défaut

Oui

### Valeur senseValue par défaut

5

### Description

Indique que plusieurs emplacements ou sources utilisent le même compte simultanément. Réglez les paramètres de correspondance et de durée pour optimiser la réactivité.

### Règle de prise en charge

BB:UBA : Common Event Filters

### Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman

Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## **UBA : Accès utilisateur depuis un emplacement interdit**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès utilisateur depuis un emplacement interdit

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte les accès des utilisateurs depuis un emplacement qui ne figure pas dans la liste des emplacements autorisés ("UBA : Allowed Location List").

### **Règles de prise en charge :**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- 

### **Configuration requise**

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : UBA : Allowed Location List

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDoS Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venustech Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## UBA : Accès utilisateur depuis un emplacement restreint

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès utilisateur depuis un emplacement restreint

### Activation par défaut

Non

### Valeur senseValue par défaut

15

### Description

Détecte les accès des utilisateurs depuis un emplacement figurant dans la liste des emplacements restreints ("UBA : Restricted Location List"). Vous pouvez ajouter des pays d'"Emplacements géographiques" à cette liste.

### Règles de prise en charge

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success
- 

### Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : UBA : Restricted Location List

### Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for

Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSM, VMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasy's Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

## **UBA : Changement de zone géographique de l'utilisateur**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Changement de zone géographique de l'utilisateur

### **Activation par défaut**

Oui

### **Valeur senseValue par défaut**

5

### **Description**

Une correspondance indique qu'un utilisateur s'est connecté à distance depuis un pays différent du pays dans lequel il a effectué sa dernière connexion à distance. Cette règle peut également indiquer une situation de danger pour le compte, particulièrement si les correspondances de règles ont été rapprochées dans le temps.

### **Règles de prise en charge**

- BB:UBA : Common Event Filters
- BB:CategoryDefinition: Authentication Success

- UBA : User Geography Map

## Configuration requise

Activez la règle suivante : UBA : User Geography Map

## Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHIELD, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security

Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Firewall OS, genua genugate, iT-CUBE agileSI

## Règle de prise en charge

Carte géographique d'utilisateur

Cette règle met à jour les ensembles de référence associés avec les données requises.

## UBA : Zone géographique de l'utilisateur, Accès depuis des emplacements inhabituels

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Zone géographique de l'utilisateur, Accès depuis des emplacements inhabituels

### Activation par défaut

Oui

### Valeur senseValue par défaut

15

### Description

Indique que les utilisateurs ont pu s'authentifier dans des pays inhabituels pour votre réseau (voir la définition établie dans la règle de bloc de construction "UBA : BB : Unusual Source Locations").

### Règles de prise en charge

- BB:UBA : Unusual Source Locations
- BB:CategoryDefinition: Authentication Success
- BB:UBA : Common Event Filters

### Sources de données

APC UPS, AhnLab Policy Center APC, Amazon AWS CloudTrail, Apache HTTP Server, Application Security DbProtect, Arpeggio SIFT-IT, Array Networks SSL VPN Access Gateways, Aruba ClearPass Policy Manager, Aruba Mobility Controller, Avaya VPN Gateway, Barracuda Spam & Virus Firewall, Barracuda Web Application Firewall, Barracuda Web Filter, Bit9 Security Platform, Box, Bridgewater Systems AAA Service Controller, Brocade FabricOS, CA ACF2, CA SiteMinder, CA Top Secret, CRE System, CRYPTOCard CRYPTOSHield, Carbon Black Protection, Centrify Server Suite, Check Point, Cilasoft QJRN/400, Cisco ACS, Cisco Adaptive Security Appliance (ASA), Cisco Aironet, Cisco CSA, Cisco Call Manager, Cisco CatOS for Catalyst Switches, Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Identity Services Engine, Cisco Intrusion Prevention System (IPS), Cisco IronPort, Cisco NAC Appliance, Cisco Nexus, Cisco PIX Firewall, Cisco VPN 3000 Series Concentrator, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Citrix Access Gateway, Citrix NetScaler, CloudPassage Halo, Configurable Authentication message filter, CorreLog Agent for IBM zOS, CrowdStrike Falcon Host, Custom Rule Engine, Cyber-Ark Vault, DCN DCS/DCRS Series, EMC VMWare, ESET Remote Administrator, Enterasys Matrix K/N/S Series Switch, Enterasys XSR Security

Routers, Enterprise-IT-Security.com SF-Sherlock, Epic SIEM, Event CRE Injected, Extreme 800-Series Switch, Extreme Dragon Network IPS, Extreme HiPath, Extreme Matrix E1 Switch, Extreme Networks ExtremeWare Operating System (OS), Extreme Stackable and Standalone Switches, F5 Networks BIG-IP APM, F5 Networks BIG-IP LTM, F5 Networks FirePass, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, FreeRADIUS, H3C Comware Platform, HBGary Active Defense, HP Network Automation, HP Tandem, Huawei AR Series Router, Huawei S Series Switch, HyTrust CloudControl, IBM AIX Audit, IBM AIX Server, IBM BigFix, IBM DB2, IBM DataPower, IBM Fiberlink MaaS360, IBM IMS, IBM Lotus Domino, IBM Proventia Network Intrusion Prevention System (IPS), IBM QRadar Network Security XGS, IBM Resource Access Control Facility (RACF), IBM Security Access Manager for Enterprise Single Sign-On, IBM Security Access Manager for Mobile, IBM Security Identity Governance, IBM Security Identity Manager, IBM SmartCloud Orchestrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM i, IBM z/OS, IBM zSecure Alert, Illumio Adaptive Security Platform, Imperva SecureSphere, Itron Smart Meter, Juniper Junos OS Platform, Juniper MX Series Ethernet Services Router, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, Juniper Steel-Belted Radius, Juniper WirelessLAN, Kaspersky Security Center, Lieberman Random Password Manager, Linux OS, Mac OS X, McAfee Application/Change Control, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Metainfo MetaIP, Microsoft DHCP Server, Microsoft Exchange Server, Microsoft IAS Server, Microsoft IIS, Microsoft ISA, Microsoft Office 365, Microsoft Operations Manager, Microsoft SCOM, Microsoft SQL Server, Microsoft Windows Security Event Log, Motorola SymbolAP, NCC Group DDos Secure, Netskope Active, Niara, Nortel Application Switch, Nortel Contivity VPN Switch, Nortel Contivity VPN Switch (obsolete), Nortel Ethernet Routing Switch 2500/4500/5500, Nortel Ethernet Routing Switch 8300/8600, Nortel Multiprotocol Router, Nortel Secure Network Access Switch (SNAS), Nortel Secure Router, Nortel VPN Gateway, Novell eDirectory, OS Services Qidmap, OSSEC, ObserveIT, Okta, OpenBSD OS, Oracle Acme Packet SBC, Oracle Audit Vault, Oracle BEA WebLogic, Oracle Database Listener, Oracle Enterprise Manager, Oracle RDBMS Audit Record, Oracle RDBMS OS Audit Record, PGP Universal Server, Palo Alto Endpoint Security Manager, Palo Alto PA Series, Pirean Access: One, ProFTPD Server, Proofpoint Enterprise Protection/Enterprise Privacy, Pulse Secure Pulse Connect Secure, RSA Authentication Manager, Radware AppWall, Radware DefensePro, Redback ASE, Riverbed SteelCentral NetProfiler Audit, SIM Audit, SSH CryptoAuditor, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Salesforce Security Auditing, Salesforce Security Monitoring, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, Solaris BSM, Solaris Operating System Authentication Messages, Solaris Operating System Sendmail Logs, SonicWALL SonicOS, Sophos Astaro Security Gateway, Squid Web Proxy, Starent Networks Home Agent (HA), Stonesoft Management Center, Sybase ASE, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), TippingPoint X Series Appliances, Trend Micro Deep Discovery Email Inspector, Trend Micro Deep Security, Tripwire Enterprise, Tropos Control, Universal DSMVMware vCloud Director, VMware vShield, Venustech Venusense Security Platform, Verdasys Digital Guardian, Vormetric Data Security, WatchGuard Fireware OS, genua genugate, iT-CUBE agileSI

---

## Trafic et attaques du réseau

### UBA : Détection d'attaques par refus de service

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Détection d'attaques par refus de service

#### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte les attaques par refuse de service (DoS) d'un utilisateur dans le réseau.

**Remarque :** Pour pouvoir utiliser cette règle, procédez comme suit :

1. Dans l'onglet **Admin**, cliquez sur **Paramètres UBA**.
2. Sélectionnez la case à cocher **Rechercher des actifs pour un nom d'utilisateur, lorsque celui-ci n'est pas disponible dans les données d'événement ou de flux** pour effectuer une recherche par noms d'utilisateur dans la table des actifs. L'application UBA utilise des actifs pour rechercher un utilisateur via une adresse IP lorsque aucun utilisateur n'est répertorié dans un événement.
3. Pour pouvoir fonctionner, la règle d'événement doit disposer de la source de journaux "Snort Open Source IDS".

### Règles de prise en charge

- BB:UBA : Common Log Source Filters
- BB:CategoryDefinition: DDoS Attack Events
- BB:CategoryDefinition: Network DoS Attack
- BB:CategoryDefinition: Service DoS

### Sources de données

Akamai KONA, Application Security DbProtect, Aruba Mobility Controller, Barracuda Web Application Firewall, Brocade FabricOS, CRE System, Check Point, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), Cisco IOS, Cisco Intrusion Prevention System (IPS), Cisco PIX Firewall, Cisco Stealthwatch, Cisco Wireless LAN Controllers, Cisco Wireless Services Module (WiSM), Custom Rule Engine, CyberGuard TSP Firewall/VPN, Enterprise-IT-Security.com SF-Sherlock, Event CRE Injected, Extreme Dragon Network IPS, Extreme HiPath, F5 Networks BIG-IP AFM, F5 Networks BIG-IP ASM, F5 Networks BIG-IP LTM, Fair Warning, FireEye, Flow Classification Engine, ForeScout CounterACT, Fortinet FortiGate Security Gateway, Foundry Fastiron, Huawei AR Series Router, IBM Proventia Network Intrusion Prevention System (IPS), IBM Security Network IPS (GX), Imperva Incapsula, Juniper Junos OS Platform, Juniper Junos WebApp Secure, Juniper Networks Firewall and VPN, Juniper Networks Intrusion Detection and Prevention (IDP), Juniper Networks Network and Security Manager, McAfee Firewall Enterprise, McAfee IntruShield Network IPS Appliance, McAfee ePolicy Orchestrator, Motorola SymbolAP, NCC Group DDos Secure, Niksun 2005 v3.5, Nortel Application Switch, OS Services Qidmap, OSSEC, Palo Alto PA Series, Radware AppWall, Radware DefensePro, Riverbed SteelCentral NetProfiler, STEALTHbits StealthINTERCEPT, SafeNet DataSecure/KeySecure, Sentrigo Hedgehog, Skyhigh Networks Cloud Security Platform, Snort Open Source IDS, SonicWALL SonicOS, Squid Web Proxy, Stonesoft Management Center, Symantec Endpoint Protection, TippingPoint Intrusion Prevention System (IPS), Top Layer IPS, Trend Micro Deep Security, Universal DSM, Vectra Networks Vectra, Venustech Venusense Security Platform, WatchGuard Fireware OS

### UBA : Activité Honeytoken

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activité Honeytoken

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte une activité utilisant un compte Honeytoken.

## Règles de prise en charge

BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées aux ensembles de référence suivants : UBA : Comptes Honeytoken

Ajoutez les sources de journaux appropriées aux groupes de sources de journaux suivants : UBA : Systèmes avec Comptes Honeytoken.

## Sources de données

Ensemble des sources de journaux ajoutées à l'application UBA : Systèmes avec groupe de source de journaux Comptes Honeytoken.

## UBA : Trafic réseau : surveillance des données acquises et utilisation du programme d'analyse

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Trafic réseau : surveillance des données acquises et utilisation du programme d'analyse

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Indique qu'un processus est créé et que le nom du processus correspond à l'un des noms binaires répertoriés dans l'ensemble de références "UBA : Network Capture, Monitoring and Analysis Program Filenames". Cet ensemble de références répertorie les noms binaires du logiciel de capture de paquets réseau. L'ensemble de références est pré-rempli et inclut les noms de fichiers de certains logiciels d'analyse de protocole réseau communs.

Pour plus d'informations sur l'ajout ou la suppression de programmes de surveillance, voir Gestion des outils de surveillance du réseau.

## Règle de prise en charge

BB:UBA : Common Event Filters

## Configuration requise

Ajoutez les valeurs appropriées à l'ensemble de référence suivant : UBA : Network Capture, Monitoring and Analysis Program Filenames.

## Sources de données

Microsoft Windows Security Event Log

## UBA : Anomalie de session par adresse IP de destination (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge.

UBA : User Behavior, Session Anomaly by Destination

UBA : User Behavior, Session Anomaly by Destination Found

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

**UBA : User Behavior, Session Anomaly by Destination** Indique qu'un utilisateur accède à des adresses IP cible significativement différentes de celles auxquelles il accédait auparavant. L'événement n'indique pas nécessairement une situation de danger. Le changement de comportement peut indiquer un changement important au niveau des responsabilités professionnelles ou du mode de travail de l'utilisateur.

**UBA : User Behavior, Session Anomaly by Destination Found** Règle CRE prenant en charge la règle ADE correspondante UBA : User Behavior, Session Anomaly by Destination qui indique qu'un utilisateur accède à des adresses IP cible significativement différentes de celles auxquelles il accédait auparavant. L'événement n'indique pas nécessairement une situation de danger. Le changement de comportement peut indiquer un changement important au niveau des responsabilités professionnelles ou du mode de travail de l'utilisateur.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : User Event Frequency Anomaly Categories (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle a été remplacée par l'analyse Machine Learning suivante : *Activité par catégorie*. Pour plus d'informations, consultez «Configuration de l'analyse *Activité par catégorie*», à la page 182.

UBA : User Event Frequency Anomaly Categories (règle ADE)

UBA : User Event Frequency Anomaly - Categories Found

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

### Activation par défaut

Non

### Valeur senseValue par défaut

5

### Description

**UBA : User Event Frequency Anomaly Categories** Utilise le moteur de détection des anomalies afin de surveiller la distribution des catégories des événements d'un utilisateur. Il informe en cas de changement de fréquence inhabituel.

**UBA : User Event Frequency Anomaly - Categories Found** Règle CRE prenant en charge la règle ADE correspondante UBA : User Event Frequency Anomaly - Categories qui utilise le moteur de détection des anomalies afin de surveiller la distribution des catégories des événements d'un utilisateur. Elle signale les changements de fréquence inhabituels.

### Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Anomalies liées aux volumes utilisateur - Détection du trafic vers des domaines internes (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge.

- UBA : User Volume Activity Anomaly - Traffic to Internal Domains
- UBA : User Volume Activity Anomaly - Traffic to Internal Domains Found

### Activation par défaut

Non

### Valeur senseValue par défaut

10

## Description

Règle CRE prenant en charge la règle correspondante UBA : User Volume of Activity Anomaly - Traffic to Internal Domains, qui utilise le moteur de détection des anomalies pour surveiller le trafic utilisateur et alerter sur les volumes de trafic anormaux.

## Sources de données

Juniper SRX Series Services Gateway, Microsoft ISA, Pulse Secure Pulse Connect Secure

---

## QRadar DNS Analyzer

Pour plus d'informations, consultez IBM QRadar DNS Analyzer.

## UBA : Accès potentiel à un domaine en liste noire

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès potentiel à un domaine en liste noire

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Détecte les événements indiquant que l'utilisateur a potentiellement accédé à un domaine en liste noire. L'application IBM QRadar DNS Analyzer est requise.

## Configuration requise

Avant d'activer cette règle, vous devez installer l'application IBM QRadar DNS Analyzer. Pour plus d'informations, consultez IBM QRadar DNS Analyzer.

## Sources de données

IBM QRadar DNS Analyzer

## UBA : Accès potentiel à un domaine DGA

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès potentiel à un domaine DGA

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Détecte les événements indiquant que l'utilisateur a potentiellement accédé à un domaine DGA (Domain Generated by Algorithm). L'application IBM QRadar DNS Analyzer est requise.

## Configuration requise

Avant d'activer cette règle, vous devez installer l'application IBM QRadar DNS Analyzer. Pour plus d'informations, consultez IBM QRadar DNS Analyzer.

## Sources de données

IBM QRadar DNS Analyzer

## UBA : Potential Access to Squatting Domain

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Potential Access to Squatting Domain

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Détecte les événements indiquant que l'utilisateur a potentiellement accédé à un domaine squatté. L'application IBM QRadar DNS Analyzer est requise.

## Configuration requise

Avant d'activer cette règle, vous devez installer l'application IBM QRadar DNS Analyzer. Pour plus d'informations, consultez IBM QRadar DNS Analyzer.

## Sources de données

IBM QRadar DNS Analyzer

## UBA : Accès potentiel à un domaine Tunneling

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Potential Access to Tunneling Domain

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Détecte les événements indiquant que l'utilisateur a potentiellement accédé à un domaine Tunneling. Requier l'application IBM DNS Analyzer.

## Configuration requise

Avant d'activer cette règle, vous devez installer l'application IBM QRadar DNS Analyzer. Pour plus d'informations, consultez IBM QRadar DNS Analyzer.

## Sources de données

IBM QRadar DNS Analyzer

---

## QRadar Network Insights (QNI)

Pour plus d'informations sur l'installation des règles QNI dans QRadar V7.2.8, consultez QRadar Network Insights Content v7.2.8.

Pour QRadar V7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## UBA : QNI - Accès à un service incorrectement sécurisé - Certificat arrivé à expiration

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Accès à un service incorrectement sécurisé - Certificat arrivé à expiration

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

QRadar Network Insights (QNI) a détecté une session SSL/TLS qui utilise un certificat arrivé à expiration. Les serveurs et les clients utilisent des certificats lors de l'établissement des communications à l'aide de SSL (Secure Sockets Layer) ou de TLS (Transport Layer Security). Les certificats sont émis avec une date qui indique la durée de validité du certificat.

## Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## Sources de données

QRadar Network Insights (QNI)

## **UBA : QNI - Accès à un service incorrectement sécurisé - Certificat non valide**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Accès à un service incorrectement sécurisé - Certificat non valide

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

5

### **Description**

QRadar Network Insights (QNI) a détecté une session SSL/TLS qui utilise un certificat non valide. Les serveurs et les clients utilisent des certificats X.509 lors de l'établissement des communications à l'aide de SSL (Secure Sockets Layer). Les certificats sont émis et une mention précise la date de début de validité.

### **Configuration requise**

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

### **Sources de données**

QRadar Network Insights (QNI)

## **UBA : QNI - Accès à un service incorrectement sécurisé - Longueur de clé publique faible**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Accès à un service incorrectement sécurisé - Longueur de clé publique faible

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

5

### **Description**

QRadar Network Insights (QNI) a détecté une session SSL/TLS qui utilise un certificat avec un nombre de bits de clé publique inférieur à 2048. Un serveur qui fournit un certificat de clé publique faible (inférieur à 1024 bits) peut représenter un risque de sécurité. D'après la publication NIST 800-57, le début de clé RSA minimal recommandé en 2011 est de 2048 bits.

## Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## Sources de données

QRadar Network Insights (QNI)

## UBA : QNI - Accès à un service incorrectement sécurisé - Certificat auto-signé

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Accès à un service incorrectement sécurisé - Certificat auto-signé

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

QRadar Network Insights (QNI) a détecté une session SSL/TLS qui utilise un certificat autosigné. Un tel certificat dans une application de serveur de production ou accessible au public peut permettre à un pirate distant de lancer une attaque de l'homme du milieu (man-in-the-middle).

## Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## Sources de données

QRadar Network Insights (QNI)

## UBA : QNI - Transfert en cours d'un contenu confidentiel vers une zone géographique étrangère

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Transfert en cours d'un contenu confidentiel vers une zone géographique étrangère

## Activation par défaut

Non

## Valeur senseValue par défaut

5

### Description

Détecte le contenu confidentiel qui est en cours de transfert vers des pays et des régions dont l'accès est restreint. Détecte le contenu confidentiel qui est en cours de transfert vers des pays et des régions dont l'accès est restreint. Notez que ces pays et régions sont définis dans le bloc de construction suivant : "Countries/Regions with Restricted Access". Avant d'activer cette règle, vérifiez que le bloc de construction est configuré en fonction de votre cas d'utilisation métier.

### Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

### Sources de données

QRadar Network Insights (QNI)

## **UBA : QNI - Hachage de fichier comportant une menace logicielle observé**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Hachage de fichier comportant une menace logicielle observé

### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Cette règle se déclenche lorsque le contenu de flux inclut un hachage de fichier correspondant aux hachages de fichier incorrects connus inclus dans un flux de données Threat Intelligence. Cela signifie qu'une personne a transféré des logiciels malveillants via le réseau.

### Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

### Sources de données

QRadar Network Insights (QNI)

## **UBA : QNI - Hachage de fichier sur plusieurs hôtes observé**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Hachage de fichier sur plusieurs hôtes observé

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Cette règle se déclenche lorsqu'il est détecté que le même hachage de fichier associé à un logiciel malveillant est transféré vers plusieurs destinations.

### **Configuration requise**

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

### **Sources de données**

QRadar Network Insights (QNI)

## **UBA : QNI - Courrier indésirable/Hameçonnage potentiel détecté pour le destinataire d'un courrier électronique rejeté**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Courrier indésirable/Hameçonnage potentiel détecté pour le destinataire d'un courrier électronique rejeté

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

5

### **Description**

Cette règle se déclenche lorsqu'il est détecté dans le système que des e-mails envoyés à une adresse de destinataire qui n'existe pas ont été rejetés. Cela peut indiquer une tentative d'hameçonnage ou de spam. Configurez le bloc de construction BB:CategoryDefinition: Rejected Email Recipient afin d'inclure des éléments QID adaptés à votre organisation. Les QID suivants pouvant être surveillés sont inclus par défaut : Microsoft Exchange ; Système d'exploitation Linux [sendmail en cours d'exécution] ; Journaux Sendmail de système d'exploitation Solaris et pare-feu de spam et de virus Barracuda.

## Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## Sources de données

QRadar Network Insights (QNI)

### **UBA : QNI - Objet de courrier indésirable/hameçonnage potentiel détecté à partir de plusieurs serveurs d'envoi**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : QNI - Objet de courrier indésirable/hameçonnage potentiel détecté à partir de plusieurs serveurs d'envoi

## Activation par défaut

Non

## Valeur senseValue par défaut

5

## Description

Cette règle se déclenche lorsque plusieurs serveurs d'envoi expédient le même sujet de message électronique pendant une période spécifique, ce qui peut indiquer une opération de spam ou de hameçonnage.

## Configuration requise

Avant d'activer cette règle QNI, vous devez installer le package de contenus QRadar Network Insights et activer les règles qu'il contient. Pour QRadar 7.2.8, consultez QRadar Network Insights Content v7.2.8. Pour QRadar 7.3.0 et éditions ultérieures, consultez QRadar Network Insights Content v7.3.0+.

## Sources de données

QRadar Network Insights (QNI)

---

## Reconnaissance

Pour plus d'informations, voir IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs DHCP détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs DHCP détectée

## Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs DHCP.

### Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs de base de données détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs de base de données détectée

### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs de base de données.

### Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs DNS détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs DNS détectée

### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs DNS.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs FTP détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs FTP détectée

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

15

#### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs FTP.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs de jeu détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs de jeu détectée

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

15

#### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs de jeu.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle du protocole ICMP générique détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle du protocole ICMP générique détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle dans le réseau au niveau des serveurs qui utilisent le protocole ICMP.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle du protocole TCP générique détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle du protocole TCP générique détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs qui utilisent des ports TCP communs.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle du protocole UDP générique détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle du protocole UDP générique détectée

### **Activation par défaut**

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs qui utilisent des ports UDP communs.

### Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## UBA : Analyse inhabituelle des serveurs IRC détectée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs IRC détectée

### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs IRC.

### Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## UBA : Analyse inhabituelle des serveurs LDAP détectée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs LDAP détectée

### Activation par défaut

Non

## Valeur senseValue par défaut

15

### Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs LDAP.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs de messagerie détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs de messagerie détectée

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

15

#### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs de messagerie.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs de messagerie détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs de messagerie détectée

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

15

#### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs de discussion.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

### **UBA : Analyse inhabituelle des serveurs P2P détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs P2P détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs P2P.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs proxy détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs proxy détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs proxy.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs RPC détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs RPC détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

## Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs RPC.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## UBA : Analyse inhabituelle des serveurs SNMP détectée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs SNMP détectée

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs SNMP.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## UBA : Analyse inhabituelle des serveurs SSH détectée

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs SSH détectée

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs SSH.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs Web détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs Web détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs Web.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

## **UBA : Analyse inhabituelle des serveurs Windows détectée**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Analyse inhabituelle des serveurs Windows détectée

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

15

### **Description**

Détecte une analyse inhabituelle sur le réseau au niveau des serveurs Windows.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM Security Reconnaissance Content et activer les règles qu'il contient. Pour plus d'informations, consultez IBM Security Reconnaissance Content.

---

## **Surveillance du système (Sysmon)**

Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## **UBA : Outils d'exploitation courants détectés**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Outils d'exploitation courants détectés

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte l'utilisation d'outils d'exploitation courants (enregistreurs de frappe, psexec, par exemple).

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows

## **UBA : Outils d'exploitation courants détectés (actif)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Outils d'exploitation courants détectés (actif)

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte l'utilisation d'outils d'exploitation courants (enregistreurs de frappe, psexec, par exemple).

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows

## **UBA : Processus malveillant détecté**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Processus malveillant détecté

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte les processus qui indiquent un comportement malveillant sur les hôtes Windows.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

### **Sources de données**

Journaux Microsoft Windows Security Event Log

### **UBA : Accès à un partage réseau**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Accès à un partage réseau

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte les activités suspectes impliquant des partages réseau.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

### **Sources de données**

Règles sysmon

## **UBA : Processus créant des unités d'exécution distantes suspectes détectés (actif)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Processus créant des unités d'exécution distantes suspectes détectés (actif)

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte les processus créant des unités d'exécution de façon suspecte sur un ordinateur distant.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

### **Sources de données**

Journaux des événements de sécurité Microsoft Windows

## **UBA : Activités suspectes sur des hôtes compromis**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes sur des hôtes compromis

### **Activation par défaut**

Non

### **Valeur senseValue par défaut**

10

### **Description**

Détecte les activités effectuées sur un hôte compromis.

### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Activités suspectes sur des hôtes compromis (actifs)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes sur des hôtes compromis (actifs)

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les activités effectuées sur un hôte compromis.

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Suspicious Administrative Activities Detected**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Suspicious Administrative Activities Detected

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les activités d'administration rarement exécutées qui semblent suspectes.

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Activité d'invite de commande suspecte**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activité d'invite de commande suspecte

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les activités liées aux scripts d'invite de commande

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Entrées suspectes dans le registre système (actif)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Entrées suspectes dans le registre système (actif)

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les activités suspectes impliquant des modifications ou des mises à jour du registre Windows.

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Charge suspecte des images détectée (actif)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Charge suspecte des images détectée (actif)

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les images suspectes téléchargées à des emplacements sensibles.

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### **UBA : Activités suspectes du pipe (actif)**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes du pipe (actif)

#### **Activation par défaut**

Non

#### **Valeur senseValue par défaut**

10

#### **Description**

Détecte les activités suspectes impliquant des tuyaux de processus sur des hôtes Windows.

#### **Configuration requise**

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### UBA : Activité PowerShell suspecte

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activité PowerShell suspecte

#### Activation par défaut

Non

#### Valeur senseValue par défaut

10

#### Description

Détecte les activités liées aux scripts Microsoft PowerShell.

#### Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

### UBA : Activité PowerShell suspecte (actif)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activité PowerShell suspecte (actif)

#### Activation par défaut

Non

#### Valeur senseValue par défaut

10

#### Description

Détecte les activités liées aux scripts Microsoft PowerShell. Pour cette règle, la fonctionnalité "Rechercher des actifs pour un nom d'utilisateur, lorsque celui-ci n'est pas disponible dans les données d'événement ou de flux" doit être activée.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

## UBA : Activités suspectes des tâches planifiées

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes des tâches planifiées

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte la création suspecte de tâches planifiées sur des hôtes Windows

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

## UBA : Activités suspectes des services

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes des services

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte les activités suspectes des services sur les ordinateurs Windows.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

## UBA : Activités suspectes des services (actif)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Activités suspectes des services (actif)

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte les activités suspectes des services sur les ordinateurs Windows.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

## UBA : Contournement du contrôle d'accès utilisateur détecté (actif)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Contournement du contrôle d'accès utilisateur détecté (actif)

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte les activités de processus indiquant que le contrôle d'accès utilisateur a été ignoré.

## Configuration requise

Avant d'activer cette règle, vous devez installer le package IBM QRadar Content Extension for Sysmon et activer les règles qu'il contient. Pour plus d'informations, consultez IBM QRadar Content Extension for Sysmon.

## Sources de données

Journaux des événements de sécurité Microsoft Windows

---

## Renseignement sur les menaces

### UBA : Abnormal visits to Risky Resources (règle ADE)

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge.

- UBA : Abnormal visits to Risky Resources
- UBA : Abnormal visits to Risky Resources Found

**Remarque :** L'activation des règles ADE peut affecter les performances de l'application UBA et de votre système QRadar.

### Activation par défaut

Non

### Valeur senseValue par défaut

15

### Description

**UBA : Abnormal visits to Risky Resources** Cette règle utilise le moteur de détection des anomalies pour surveiller le nombre de fois où un utilisateur a accédé à des ressources à risque (URL suspectes, services d'anonymat et hôtes de logiciel malveillant) et émet une alerte lorsque le nombre de visites change de manière anormale.

**UBA : Abnormal visits to Risky Resources Found** Règle CRE prenant en charge la règle ADE correspondante UBA : Abnormal visits to Risky Resources, qui utilise le moteur de détection des anomalies pour surveiller le nombre de fois où un utilisateur a accédé à des ressources à risque (URL suspectes, services d'anonymat et hôtes de logiciel malveillant) et émet une alerte lorsque le nombre de visites change de manière anormale.

### Sources de données

Toutes les sources de journaux prises en charge.

### UBA : Indicateurs de compromission pour Locky détectés

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Indicateurs de compromission pour Locky détectés

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte les ordinateurs d'utilisateur montrant des indicateurs de compromission (IOC) pour Locky en utilisant des adresses URL ou des adresses IP chargées à partir des flux de campagne X-Force.

## Règles de prise en charge

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect Locky Using IP
- BB:UBA : Detect Locky Using URL

## Configuration requise

- Ajoutez les valeurs appropriées aux ensembles de référence suivants : UBA : IOCs-Locky IP et UBA : IOCs-Locky URL.
- Activez "User Lookup from Asset" dans **Paramètres Admin > Paramètres UBA**.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Indicateurs de compromission pour WannaCry détectés

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Indicateurs de compromission pour WannaCry détectés

## Activation par défaut

Non

## Valeur senseValue par défaut

10

## Description

Détecte les ordinateurs d'utilisateur montrant des indicateurs de compromission (IOC) pour WannaCry en utilisant des adresses URL, des adresses IP ou des hachages chargés à partir des flux de campagne X-Force.

## Règles de prise en charge

- BB:UBA : Common Log Source Filters
- BB:UBA : Detect WannaCry Using Hashes
- BB:UBA : Detect WannaCry Using IP
- BB:UBA : Detect WannaCry Using URL

## Configuration requise :

- Ajoutez les valeurs appropriées aux ensembles de référence suivants : UBA : Malware Activity WannaCry - Hash, UBA : Malware Activity WannaCry - IP et UBA : Malware Activity WannaCry - URL.
- Activez "User Lookup from Asset" dans **Paramètres Admin > Paramètres UBA**.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Clés de registre modifiées par un rançongiciel

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation en fonction de règles pour certaines anomalies de comportement.

UBA : Clés de registre modifiées par un rançongiciel

### Activation par défaut

Oui

### Valeur senseValue par défaut

10

### Description

Détecte les modifications de registre ShellBag indiquant le comportement typique d'un logiciel malveillant ou d'un rançongiciel.

### Règles de prise en charge

BB:UBA : Common Event Filters

## Sources de données

Journaux des événements de sécurité Microsoft Windows (ID d'événement : 4657)

## UBA : Utilisateur accédant à des ressources risquées

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

**Remarque :** Cette règle n'est plus prise en charge.

La règle UBA : Utilisateur accédant à des ressources risquées est désactivée par défaut depuis la version 2.3.0. Les règles sont désormais répertoriées en fonction des types suivants et sont activées par défaut :

- UBA : Utilisateur qui accède à une adresse IP risquée, Anonymisation
- UBA : Utilisateur qui accède à une adresse IP risquée, Botnets
- UBA : Utilisateur qui accède à une adresse IP, Dynamique
- UBA : Utilisateur qui accède à une adresse IP risquée, Logiciels malveillants
- UBA : Utilisateur accédant à une adresse IP risquée, spam

## Activation par défaut

Non

## Valeur senseValue par défaut

15

## Description

Indique qu'un utilisateur a accédé à une ressource externe jugée inappropriée ou risquée, ou montrant des signes d'infection.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Utilisateur qui accède à une adresse IP risquée, Anonymisation

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur qui accède à une adresse IP risquée, Anonymisation (auparavant appelée Adresse IP risquée, Anonymisation)

## Activation par défaut

Oui

## Description

Cette règle se déclenche lorsqu'un hôte ou un utilisateur local se connecte à un service d'anonymisation externe.

## Règles de prise en charge

- X-Force Risky IP, Anonymization
- BB:UBA : Common Event Filters

## Configuration requise

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky IP, Anonymization.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Utilisateur qui accède à une adresse IP risquée, Botnets

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur qui accède à une adresse IP risquée, Botnets (auparavant appelée Adresse IP X-Force risquée, Botnets)

## Activation par défaut

Oui

## Description

Cette règle détecte quand un hôte ou un utilisateur local se connecte à un serveur de commande et de contrôle de réseau de zombies (botnet).

## Règles de prise en charge

- X-Force Risky IP, Botnet
- BB:UBA : Common Event Filters

## Configuration requise

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky IP, Botnet.

## Sources de données

Toutes les sources de journaux prises en charge.

## UBA : Utilisateur qui accède à une adresse IP risquée, Dynamique

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur qui accède à une adresse IP risquée, Dynamique (auparavant appelée dresse IP risquée X-Force, Dynamique)

## Activation par défaut

Oui

## Description

Cette règle détecte quand un hôte ou un utilisateur local se connecte à une adresse IP affectée dynamiquement.

## Règles de prise en charge

- X-Force Risky IP, Dynamic
- BB:UBA : Common Event Filters

## Configuration requise

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky IP, Dynamic.

## Sources de données

Toutes les sources de journaux prises en charge.

## **UBA : Utilisateur qui accède à une adresse IP risquée, Logiciels malveillants**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur qui accède à une adresse IP risquée, Logiciels malveillants (auparavant appelé IP risquée X-Force, Logiciels malveillants)

### **Activation par défaut**

Oui

### **Description**

Cette règle détecte quand un hôte ou un utilisateur local se connecte à un hôte de logiciel malveillant.

### **Règles de prise en charge**

- X-Force Risky IP, Malware
- BB:UBA : Common Event Filters

### **Configuration requise**

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky IP, Malware.

### **Sources de données**

Toutes les sources de journaux prises en charge.

## **UBA : Utilisateur accédant à une adresse IP risquée, spam**

L'application QRadar User Behavior Analytics (UBA) prend en charge des scénarios d'utilisation s'appuyant sur des règles définies pour certaines anomalies comportementales.

UBA : Utilisateur accédant à une adresse IP risquée, spam (auparavant appelée IP risquée X-Force, Spam)

### **Activation par défaut**

Oui

### **Description**

Cette règle détecte quand un hôte ou un utilisateur local se connecte à un hôte envoyant des courriers indésirables (spam).

### **Règles de prise en charge**

- X-Force Risky IP, Spam
- BB:UBA : Common Event Filters

### **Configuration requise**

- Définissez "Activer le flux X-Force Threat Intelligence" sur Oui dans **Paramètres Admin > Paramètres de système**.
- Activez la règle suivante : X-Force Risky IP, Spam.

## Sources de données

Toutes les sources de journaux prises en charge.

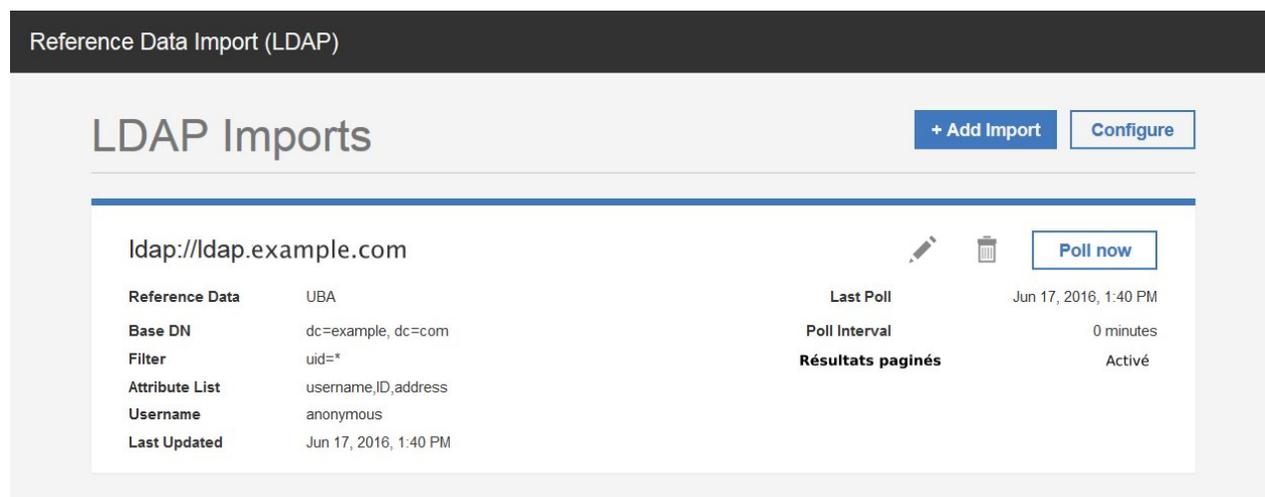
## 8 Application Reference Data Import - LDAP

L'application Reference Data Import - LDAP permet de collecter les informations d'identité contextuelle de plusieurs sources LDAP dans QRadar Console.

**Avertissement :** L'application Reference Data Import - LDAP n'est pas utilisable avec QRadar on Cloud.

L'installation de l'application User Behavior Analytics (UBA) d'IBM® QRadar® installe également l'application Reference Data Import - LDAP. Vous pouvez utiliser l'application LDAP pour importer des données d'utilisateurs dans une table de référence QRadar à partir d'un serveur LDAP/AD ou d'un fichier CSV. La table de référence est alors consommée par l'application UBA, ou bien elle peut servir aux recherches ou aux règles QRadar.

**Remarque :** Pour l'application Reference Data Import - LDAP, vous devez disposer de QRadar version 7.2.8 ou d'une version ultérieure.



Reference Data	UBA	Last Poll	Jun 17, 2016, 1:40 PM
Base DN	dc=example, dc=com	Poll Interval	0 minutes
Filter	uid=*	Résultats paginés	Activé
Attribute List	username, ID, address		
Username	anonymous		
Last Updated	Jun 17, 2016, 1:40 PM		

### Utilisation des données LDAP de QRadar

Chaque fois que la table de référence est mise à jour, un événement ReferenceDataUpdated est déclenché. Vous pouvez définir une valeur de durée de vie pour les données LDAP dans la table de référence. Lorsque la période de durée de vie est dépassée, un événement ReferenceDataExpiry est déclenché. Vous pouvez créer des règles qui répondent à ces événements ou créer des recherches pour interroger les contenus de ces événements sur l'onglet QRadar **Activité du journal**.

### Accès à l'application Reference Data Import - LDAP

Pour accéder à l'application QRadar Reference Data Import - LDAP, cliquez simplement sur l'icône correspondante sous l'onglet **Admin**.

Pour plus d'informations sur les collectes de données de référence dans QRadar, voir *IBM QRadar SIEM Administration Guide*.

---

## Navigateurs pris en charge pour l'application LDAP

Pour que les produits IBM Security QRadar fonctionnent correctement, vous devez utiliser un navigateur Web pris en charge.

Le tableau ci-après répertorie les versions prises en charge des navigateurs Web.

Tableau 1. Navigateurs Web pris en charge pour l'application QRadar

Navigateur Web	Versions prises en charge
Mozilla Firefox	45.2 Extended Support Release
Google Chrome	Dernière version

---

## Importation de données d'utilisateurs à partir d'un fichier CSV

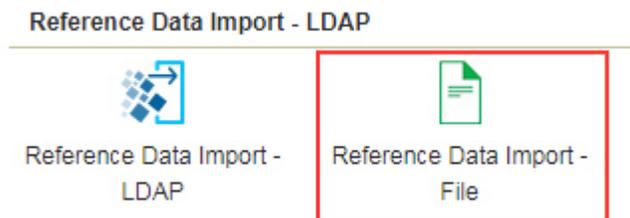
Avec l'application Importation des données de référence - LDAP, vous pouvez transférer un fichier CSV contenant des données d'utilisateurs.

### Pourquoi et quand exécuter cette tâche

Si vous avez des données d'utilisateurs dans un fichier CSV, vous pouvez importer celui-ci dans l'application UBA.

### Procédure

1. Dans IBM QRadar versions 7.3.1 et ultérieures, cliquez sur le menu de navigation (☰), puis sur **Admin** pour ouvrir l'onglet d'administration.
2. Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Importation des données de référence - LDAP > Importation des données de référence - Fichier**.



3. Dans la fenêtre Importation des données de référence (Fichier), cliquez sur **Configurer** afin de créer un jeton de service autorisé.
4. Dans la fenêtre Importation des données de référence (Fichier), cliquez sur **Importer**.
5. Dans l'écran Ajouter des données utilisateur, recherchez et sélectionnez le fichier CSV contenant les données d'utilisateurs à importer.

#### Remarque :

Le fichier ne doit pas dépasser 5 Mo, doit comporter une ligne d'en-tête avec les noms des colonnes et doit contenir au moins une colonne dont chaque donnée est unique.

6. Cliquez sur **Suivant** et indiquez si vous voulez fusionner les données avec celles d'une table de référence existante ou si vous souhaitez créer une nouvelle table de référence.
  - Si vous choisissez de fusionner dans une table de référence existante, cliquez sur **Suivant** et sélectionnez la table de référence en question.
  - Si vous choisissez de créer une table de référence, cliquez sur **Suivant** et créez la table en question.

7. Cliquez sur **Suivant**.
8. Sur l'écran Mappage d'attributs, spécifiez les noms d'attributs et la clé pour la table de référence et cliquez sur **Importer**.

---

## Création d'un jeton de service autorisé

Pour pouvoir configurer un serveur LDAP afin d'ajouter des données à une table de références, vous devez au préalable créer un jeton de service autorisé.

### Avant de commencer

**Avertissement :** En raison de leurs capacités d'administration limitées, les administrateurs QRadar on Cloud ne peuvent pas créer de jeton de service autorisé pour les applications QRadar. Si vous êtes un client QRadar on Cloud, contactez le service clients afin qu'il crée pour vous un jeton de service autorisé.

### Pourquoi et quand exécuter cette tâche

**Remarque :** Une fois que vous avez envoyé le jeton du service autorisé, vous devez déployer les modifications pour que le nouveau jeton de service autorisé soit appliqué. IBM QRadar exige que vous utilisiez un jeton d'authentification pour authentifier les appels d'API effectués par l'application Reference Data Import - LDAP. Utilisez la fenêtre Gérer les services autorisés dans les paramètres **Admin** pour créer un jeton de service autorisé.

### Procédure

1. Dans la fenêtre de l'application Reference Data Import - LDAP, cliquez **Configurer**.
2. Dans la boîte de dialogue Configurer un jeton de service autorisé, cliquez sur **Gérer les services autorisés**.
3. Dans la fenêtre Gérer les services autorisés, cliquez sur **Ajouter un service autorisé**.
4. Ajoutez les informations pertinentes dans les zones suivantes puis cliquez sur **Créer un service** :
  - a. Dans la zone **Nom du service**, indiquez pour ce service autorisé un nom pouvant contenir jusqu'à 225 caractères.
  - b. Dans la liste **Rôle utilisateur**, sélectionnez **Admin**.
  - c. Dans la liste **Profil de sécurité**, sélectionnez le profil de sécurité à affecter à ce service autorisé. Le profil de sécurité détermine les réseaux et les sources de journaux auxquels peut accéder ce service dans l'interface utilisateur de QRadar.
  - d. Dans la liste **Date d'expiration**, entrez ou sélectionnez la date à laquelle ce service doit expirer. Si une date d'expiration n'est pas requise, sélectionnez **Pas d'expiration**.
5. Cliquez sur la ligne qui contient le service que vous avez créé, sélectionnez et copiez la chaîne de jeton de la zone **Jeton sélectionné** dans la barre de menu, puis fermez la fenêtre Gérer les services autorisés.
6. Dans la boîte de dialogue Configurer un jeton de service autorisé, collez la chaîne de jeton dans la zone **Jeton** et cliquez sur **OK**.
7. Déployez les modifications pour que le nouveau jeton de service autorisé soit appliqué.

### Que faire ensuite

«Ajout d'une configuration LDAP», à la page 166

---

## Ajout d'une autorité de certification racine privée

Vous pouvez télécharger un ensemble d'autorités de certification racine privées sur IBM QRadar pour une utilisation avec l'application LDAP.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône correspondant à Reference Data Import - LDAP.
3. Dans la fenêtre principale de cette application, cliquez sur **Configurer**.
4. Cliquez sur l'option de choix de fichier puis sur **Télécharger**. Seul le type de fichier .pem est pris en charge.
5. Cliquez sur **OK**.

---

## Ajout d'une configuration LDAP

Ajoutez les informations de serveur LDAP que vous utilisez pour insérer des données utilisateur dans une mappe de référence des mappes.

### Avant de commencer

Vous devez créer et ajouter un jeton d'authentification à l'application Reference Data Import - LDAP pour pouvoir ajouter une configuration LDAP.

## Procédure

1. Dans la fenêtre de l'application Reference Data Import - LDAP, cliquez **Ajouter une importation**.
2. Entrez les informations suivantes dans l'onglet **Configuration LDAP** :
  - a. Entrez une URL qui commence par `ldap://` ou `ldaps://` (pour TLS) dans la zone **URL LDAP**.
  - b. Entrez le point dans l'arborescence de l'annuaire LDAP à partir duquel le serveur doit rechercher des utilisateurs dans la zone **Nom distinctif de base**.  
Par exemple, si votre serveur LDAP se trouvait dans le domaine `example.com`, vous pouvez utiliser `dc=example,dc=com`
  - c. Entrez l'attribut ou les attributs que vous souhaitez utiliser pour trier les données qui sont importées dans la table de référence, dans la zone **Filtre**. Par exemple :  
`cn=*; uid=*; sn=*`  
Les valeurs par défaut suivantes fonctionnent avec Active Directory :  
`(&(sAMAccountName=*)(samAccountType=805306368))`.
  - d. Entrez les attributs que vous souhaitez importer dans la table de référence, dans la zone **Liste d'attributs**.  
Les valeurs par défaut suivantes fonctionnent avec Active Directory :  
`userPrincipalName,cn,sn,telephoneNumber,l,co,department,displayName,mail,title`.
  - e. Entrez le nom d'utilisateur qui est utilisé pour authentifier le serveur LDAP dans la zone **Nom d'utilisateur**.
  - f. Entrez le mot de passe du serveur LDAP dans la zone **Mot de passe**.
3. Cliquez sur **Tester la connexion** afin de confirmer que IBM QRadar peut se connecter au serveur LDAP avant de continuer.  
Si votre tentative de connexion aboutit, les informations de votre serveur LDAP sont affichées sous l'onglet **Configuration LDAP**.
4. Cliquez sur **Suivant**.

## Que faire ensuite

«Sélection d'attributs».

### Tâches associées:

«Ajout d'une autorité de certification racine privée», à la page 165

Vous pouvez télécharger un ensemble d'autorités de certification racine privées sur IBM QRadar pour une utilisation avec l'application LDAP.

«Création d'un jeton de service autorisé», à la page 165

Pour pouvoir configurer un serveur LDAP afin d'ajouter des données à une table de références, vous devez au préalable créer un jeton de service autorisé.

«Ajout de mappages d'attributs LDAP»

Vous pouvez ajouter des alias et spécifier la clé pour la table de référence.

---

## Sélection d'attributs

Sélectionnez les attributs à extraire de votre serveur LDAP.

### Procédure

1. Sous l'onglet **Sélectionner des attributs**, recherchez des attributs spécifiques et choisissez ceux que vous voulez extraire du serveur LDAP.
2. Cliquez sur **Suivant**.

## Que faire ensuite

Ajoutez des mappages d'attributs LDAP.

---

## Ajout de mappages d'attributs LDAP

Vous pouvez ajouter des alias et spécifier la clé pour la table de référence.

### Pourquoi et quand exécuter cette tâche

Si vous souhaitez fusionner les données LDAP provenant de plusieurs sources dans la même table de référence, vous pouvez utiliser des alias personnalisés pour différencier les attributs LDAP ayant le même nom dans différentes sources.

### Procédure

1. Sous l'onglet **Mappage d'attributs**, spécifiez la clé pour la table de référence.

**Conseil :** Vous pouvez créer de nouveaux champs d'attributs LDAP en cliquant sur **Ajouter** et en combinant deux attributs. Par exemple, vous pouvez utiliser la syntaxe suivante : "Last: {ln}, First: {fn}".

2. Cliquez sur **Suivant**.

## Que faire ensuite

Configurez une table de données de référence pour stocker des données LDAP.

### Tâches associées:

«Ajout d'une configuration de données de référence», à la page 168

Utilisez l'onglet Configuration de référence pour définir une table de données de référence afin de stocker les données LDAP.

«Création d'une règle répondant aux mises à jour de données LDAP», à la page 170

Après avoir configuré l'application IBM QRadar Reference Data Import - LDAP pour stocker des données à partir de votre serveur LDAP dans une table de référence dans QRadar, vous pouvez utiliser les données pour créer des règles d'événement.

## Ajout d'une configuration de données de référence

Utilisez l'onglet Configuration de référence pour définir une table de données de référence afin de stocker les données LDAP.

### Avant de commencer

Après avoir configuré vos informations de serveur LDAP, vous devez configurer une table de référence pour stocker les données LDAP transmises à l'application. Vous pouvez ensuite utiliser les données stockées pour construire des règles dans QRadar ou pour créer des recherches et des rapports.

### Procédure

1. Utilisez l'onglet **Configuration de référence** pour entrer une nouvelle table de références ou désigner une table de références existante à laquelle ajouter des données LDAP.
  - a. Entrez un nom pour la collecte des données de référence dans la zone **Données de référence** ou sélectionnez une collecte de données de référence existante dans la liste.
  - b. La case à cocher **Générer une mappe d'ensembles** est désactivée par défaut. Si vous l'activez, des données au format d'ensemble de référence sont envoyées afin d'améliorer la recherche QRadar. Cela peut avoir des conséquences sur les performances.
  - c. Utilisez les zones **Durée de vie** pour définir la durée pendant laquelle vous souhaitez que les données demeurent dans la table de références. Par défaut, les données que vous ajoutez n'arrivent jamais à expiration. Lorsque la période de durée de vie est dépassée, un événement ReferenceDataExpiry est déclenché.

**Remarque :** Si vous ajoutez des données à une mappe de références de mappes existante, l'application utilise les paramètres de durée de vie d'origine. Ces paramètres ne peuvent pas être remplacés sous l'onglet **Configuration de référence**.

LDAP Configuration    Select Attributes    Attribute Mapping    **Reference Configuration**    Polling Interval

Enter a new reference table name or select an existing reference table.

Reference table    Test-LDAP    Test-LDAP

Generate map of sets   

Time to live (YY:MM:DD:hh:mm:ss)

+ 0 - : + 0 - : + 0 - : + 3 - : + 10 - : + 0 -

2. Cliquez sur **Suivant**.

### Que faire ensuite

Définissez l'intervalle d'interrogation.

**Tâches associées:**

«Configuration de l'interrogation»

Utilisez l'onglet **Intervalle d'interrogation** pour configurer la fréquence à laquelle l'application interroge votre serveur LDAP pour de nouvelles informations.

---

## Configuration de l'interrogation

Utilisez l'onglet **Intervalle d'interrogation** pour configurer la fréquence à laquelle l'application interroge votre serveur LDAP pour de nouvelles informations.

### Avant de commencer

Après avoir configuré les informations de votre serveur LDAP et la collecte de données de référence, vous pouvez configurer la fréquence à laquelle l'application prélève des données à partir du serveur LDAP.

### Procédure

1. Utilisez la zone **Intervalle d'interrogation en minutes** afin de définir la fréquence d'interrogation par l'application des données de votre serveur LDAP.  
La valeur de l'intervalle d'interrogation minimal est 120.
2. Dans la zone **Limite d'extraction des enregistrements**, entrez une valeur pour le nombre d'enregistrements que l'interrogation doit renvoyer.  
Par défaut, 100 000 enregistrements sont renvoyés. Le nombre maximal d'enregistrements pouvant être retournés est 200 000.
3. La case à cocher **Résultats paginés** est sélectionnée par défaut afin de ne pas limiter le nombre d'enregistrements renvoyés par le serveur LDAP pour chaque interrogation.

**Remarque :** Les résultats paginés ne sont pas pris en charge par tous les serveurs LDAP.

4. Cliquez sur **Sauvegarder**.

LDAP Configuration    Select Attributes    Attribute Mapping    Reference Configuration    **Polling Interval**

Enter a polling interval to retrieve your LDAP data. Enter "0" (zero) for manual polling.

Polling interval in minutes    120

Record retrieval limit    1000

Paged results   

Note: Not all servers support paged results.  
See [RFC2696](#) for details.

### Résultats

Les données de votre serveur LDAP sont ajoutées à la collecte de données de référence que vous avez sélectionnée à l'intervalle que vous avez configuré. Vous pouvez utiliser la page de l'API sur votre console IBM QRadar pour vérifier que les données ont été ajoutées à la collecte de données de référence.

#### Tâches associées:

«Vérification que les données sont ajoutées à la collection de données de référence», à la page 170  
Vous pouvez utiliser la page de documentation de l'API IBM QRadar pour tester si les données ont été ajoutées à la collecte de données de référence que vous avez créée.

---

## Vérification que les données sont ajoutées à la collection de données de référence

Vous pouvez utiliser la page de documentation de l'API IBM QRadar pour tester si les données ont été ajoutées à la collecte de données de référence que vous avez créée.

### Pourquoi et quand exécuter cette tâche

La page de documentation de l'API sur votre console QRadar Console peut afficher les données stockées dans la table de référence créée dans l'application Reference Data Import - LDAP. Vous pouvez utiliser la page de documentation de l'API pour vérifier que les informations LDAP ont été mises à jour par l'application.

### Procédure

1. Connectez-vous à la page QRadar API Documentation.  
`https://<Console_IP>/api_doc`
2. Dans l'arborescence de navigation, ouvrez l'API la plus récente.
3. Accédez à `/reference_data > /table > /name > GET`
4. Dans la zone **Value** du paramètre **Name**, entrez le nom de la collecte de données de référence que vous avez créée pour stocker des informations LDAP, puis cliquez sur **Try it out!**.

Les données ajoutées par l'application sont renvoyées dans la zone **Response Body**.

---

## Création d'une règle répondant aux mises à jour de données LDAP

Après avoir configuré l'application IBM QRadar Reference Data Import - LDAP pour stocker des données à partir de votre serveur LDAP dans une table de référence dans QRadar, vous pouvez utiliser les données pour créer des règles d'événement.

### Pourquoi et quand exécuter cette tâche

Lorsque vous interrogez votre serveur LDAP, et les données sont ajoutées à la table de référence, les événements ReferenceDataUpdated sont déclenchés. Lorsque la période de durée de vie que vous avez configurée sur l'onglet **Reference Configuration** est dépassée, un événement ReferenceDataExpiry est déclenché. Vous pouvez créer des règles qui répondent au contenu dans des contenus d'événement ReferenceDataUpdated ou ReferenceDataExpiry.

Les données LDAP stockées par l'application dans une collecte de données de référence sont disponibles pour des règles que vous pouvez configurer en utilisant l'**Assistant Règles QRadar**. Vous pouvez accéder à l'**Assistant Règles** via les onglets **Infractions**, **Activité du journal**, ou **Activité réseau**.

### Procédure

1. Cliquez sur **Activité du journal > Règles > Actions > Nouvelle règle d'événement**.
2. Dans la page d'introduction de l'**Assistant Règles**, cliquez sur **Suivant**.
3. Vérifiez que le bouton d'option **Événements** est sélectionné, et cliquez sur **Suivant**.
4. Entrez un nom pour la règle dans la zone prévue.
5. Sélectionnez un test dans la liste **Groupe de test** et cliquez sur l'icône + en regard du test que vous souhaitez utiliser :

Le test de règle que vous sélectionnez dépend des informations que vous souhaitez récupérer à partir de la collecte de données de référence qui contient vos données LDAP.

Les mappes de référence suivantes du test de propriété d'événements de mappes sont conçues pour tester les événements qui se déclenchent lorsque la table de référence de l'application Reference Data Import - LDAP est mise à jour :

when **any of these event properties** is the key of the first map  
and **any of these event properties** is the key of the second map  
and **any of these event properties** is the value  
in **any of these reference map of maps**.

Une règle est configurée pour tester la charge d'événement ReferenceDataExpiry si l'attribut LDAP **PasswordIsExpired** est mis à jour sur true pour tout identifiant d'utilisateur (UID) dans la collecte de données de référence **LDAPtest1**.

Rule Wizard

### Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: All Export as Building Block

Type to filter

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**
- when the local IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply LDAP\_PwdExpired on events which are detected by the Local system  
and when any of outer key (custom) is the key of the first map and any of inner key (custom) is the key of the second map and any of LDAPvalue (custom) is the value in any of LDAPtest1

Please select any groups you would like this rule to be a member of:

- Anomaly
- Asset Reconciliation Exclusion
- Authentication
- Botnet
- Category Definitions

Notes (Enter your notes about this rule)  
Checks if passwordIsExpired=true is updated for any UID in the LDAPtest1 reference map of maps.

<< Back Next >> Finish Cancel

Pour utiliser ce test de propriété d'événement, vous devez créer des propriétés d'événements personnalisées pour les champs **outer key** (clé de la première mappe), **inner key** (clé de la deuxième mappe) et **value**. Dans l'exemple suivant, l'application Reference Data Import - LDAP a été configurée pour importer des informations sur les utilisateurs dont le mot de passe a expiré depuis un serveur LDAP sur example.com.

**Add a New LDAP Configuration**

LDAP Configuration
LDAP Attribute Mapping
Reference Configuration
Polling

---

ID New

LDAP URL

Base DN

Filter

Attribute List

Username

Password

Sample LDAP is displayed here after you test your connection

### Clé externe

Cette propriété contient les données entrées dans les champs LDAP spécifiés dans les zones **Nom distinctif (DN) de base** et **Filtre** de l'onglet de configuration LDAP de l'application. L'expression régulière pour la propriété d'événement personnalisée peut se présenter comme suit :

```
(uid=(.*?),dc=example,dc=com)
```

### Clé interne

Cette propriété contient les données entrées dans les champs LDAP spécifiés dans la zone **Attribut** de l'onglet de configuration LDAP de l'application. Vous pouvez utiliser des alias d'attribut dans cette zone. L'expression régulière pour la propriété d'événement personnalisée peut se présenter comme suit :

```
(passwordIsExpired)
```

### Champ de valeur

Cette propriété contient les données récupérées pour l'attribut LDAP **passwordIsExpired** pour chaque utilisateur. L'expression régulière pour la propriété d'événement personnalisée peut se présenter comme suit :

```
(\[ 'true' \])
```

Pour plus d'informations sur les propriétés d'événements personnalisées, voir *IBM QRadar SIEM - Guide d'utilisation*.

6. Cliquez sur **Suivant**.
7. Sélectionnez l'action de règle, la réponse à la règle et le limiteur de règle à appliquer à la règle et cliquez sur **Terminer**.

Pour plus d'informations sur les règles d'événements personnalisées, voir *IBM QRadar SIEM - Guide d'utilisation*.

## Résultats

La prochaine fois que vous interrogerez votre serveur LDAP et que la collecte de données de référence que vous avez créée est mise à jour, votre règle se déclenchera.

### Tâches associées:

«Ajout de mappages d'attributs LDAP», à la page 167

Vous pouvez ajouter des alias et spécifier la clé pour la table de référence.

«Ajout d'une configuration de données de référence», à la page 168

Utilisez l'onglet Configuration de référence pour définir une table de données de référence afin de stocker les données LDAP.



---

## 9 Application Machine Learning Analytics

L'application Machine Learning Analytics (ML) étend les fonctions de votre système QRadar et de l'application QRadar User Behavior Analytics (UBA) en ajoutant des scénarios d'utilisation pour Machine Learning Analytics. Les scénarios d'utilisation Machine Learning Analytics vous permettent d'avoir une vision plus précise du comportement utilisateur concernant la modélisation prédictive. Grâce à l'application ML, votre système peut détecter plus facilement le comportement attendu des utilisateurs au sein de votre réseau.

**Avvertissement :** Vous devez installer IBM QRadar V7.2.8 ou une version ultérieure avant d'installer les applications UBA et ML.

### Important :

- Il est préférable d'activer les paramètres Machine Learning Analytics un jour après la configuration initiale de l'application UBA. Cette période d'attente permet à l'application UBA de disposer de suffisamment de temps pour créer des profils de risque pour les utilisateurs.
- Le modèle est mis à jour tous les 7 jours. Cela permet de s'assurer que l'application Machine Learning Analytics comporte les utilisateurs les plus risqués à surveiller.
- La console QRadar Console limite la quantité de mémoire pouvant être utilisée par les applications. Les options de taille d'installation de l'application ML dépendent de la quantité de mémoire dont dispose actuellement QRadar pour les applications.
  - La quantité minimum de mémoire libre nécessaire à l'installation de l'application ML est de 2 Go sur une console QRadar et de 5 Go sur un noeud d'application.
  - Le nombre d'utilisateurs surveillés par l'application ML dépend de la taille d'installation de celle-ci et de l'analyse Machine Learning utilisée. Le nombre maximum d'utilisateurs surveillés, quelle que soit l'analyse, est de 500 par Go de taille d'installation. Par exemple, pour une taille d'installation de l'application ML de 2 Go, la limite sera de 1000 utilisateur. Pour 50 Go, elle sera de 25.000 utilisateurs.
- L'installation peut échouer en raison d'un manque de mémoire disponible. Cette situation peut survenir si la quantité de mémoire disponible pour les applications est réduite car d'autres applications sont installées.

---

## Problèmes connus de Machine Learning Analytics

L'application Machine Learning Analytics inclut des informations pour l'installation ainsi que des problèmes connus.

L'application Machine Learning Analytics inclut les problèmes connus suivants :

- L'application Machine Learning peut afficher des messages d'erreur dans la section Statut Machine Learning. Pour plus d'informations, voir «Le statut de l'application Machine Learning affiche un avertissement dans le tableau de bord», à la page 206.
- L'installation peut échouer en raison d'un manque de mémoire disponible. Cette situation peut survenir sur les consoles de 128 Go lorsque d'autres applications sont déjà installées et que vous disposez de moins de 10 Go pour l'application ML. Si l'installation échoue, un message d'erreur s'affiche. Pour résoudre ce problème, désinstallez des applications puis faites une nouvelle tentative.

---

## Conditions préalables à l'installation de l'application Machine Learning Analytics

Avant d'installer l'application Machine Learning Analytics, vérifiez que les conditions préalables sont respectées.

Avant de pouvoir installer l'application Machine Learning Analytics, la configuration système suivante doit être respectée et vous devez avoir intégralement installé et configuré l'application User Behavior Analytics (UBA).

Composant	Configuration minimale requise
Mémoire système	<ul style="list-style-type: none"><li>• Console : 64 Go</li><li>• Noeud de l'application : 5 Go</li></ul>
Version IBM QRadar	V7.2.8 ou version ultérieure
Sense DSM	Installation du fichier RPM DSM.
Application UBA	<ul style="list-style-type: none"><li>• Installez l'application UBA version 3.1.0.</li><li>• Configurez les paramètres UBA.</li><li>• Cliquez sur l'onglet <b>Analyse utilisateur</b> et confirmez le fait que le tableau de bord UBA contient des données utilisateur.</li></ul>

### Installation manuelle d'IBM Sense

Les applications UBA et Machine Learning Analytics utilisent les fichiers IBM Sense DSM suivants pour ajouter des scores de risque et des infractions à QRadar.

- Pour la version 7.2.8 : DSM-IBMSense-7.2-20180814101121.noarch.rpm
- Pour QRadar versions 7.3.0 et ultérieures : DSM-IBMSense-7.3-20180814141146.noarch.rpm

**Restriction :** La désinstallation d'un module de support de périphérique (DSM) n'est pas prise en charge dans QRadar.

1. Copiez le fichier DSM RPM dans QRadar Console.
2. Utilisez SSH pour vous connecter à l'hôte QRadar en tant qu'utilisateur root.
3. Accédez au répertoire contenant le fichier téléchargé.
4. Entrez la commande suivante :  
`rpm -Uvh <nom-fichier_rpm>`
5. Dans les paramètres **Admin**, cliquez sur **Avancé > Déployer la configuration entière**.

**Remarque :** Des instructions d'installation et de configuration de l'application UBA sont disponibles dans IBM Knowledge Center.

#### Tâches associées:

«Installation de l'application User Behavior Analytics», à la page 17

Utilisez l'outil Gestion des extensions d'IBM QRadar pour charger et installer directement votre archive d'application dans QRadar Console.

«Configuration des paramètres UBA», à la page 28

Pour afficher des informations dans l'application User Behavior Analytics (UBA) d'IBM QRadar, vous devez configurer les paramètres de l'application UBA.

---

## Installation de l'application Machine Learning Analytics

Installez l'application Machine Learning Analytics après l'installation de l'application UBA à partir de l'outil Extension Manager.

## Avant de commencer

Vérifiez que toutes les conditions requises pour l'installation de l'application Machine Learning Analytics sont respectées.

## Pourquoi et quand exécuter cette tâche

Une fois que vous avez installé l'application User Behavior Analytics (UBA) version 2.1.0 ou version ultérieure, vous pouvez installer l'application Machine Learning Analytics à partir de la page Paramètres Machine Learning.

## Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation (☰) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.

### User Analytics

  
UBA Settings

  
Machine Learning  
Settings

  
Help and Support

- Sur la page Paramètres Machine Learning, cliquez sur **Installer l'application ML**.
- A l'invite, cliquez sur **Oui** pour installer l'application. Cette opération dure quelques minutes.

## Que faire ensuite

Une fois l'installation terminée, vous pouvez activer les scénarios d'utilisation ML puis cliquer sur **Sauvegarder la configuration**.

---

## Mise à niveau de l'application Machine Learning Analytics

Mettez à niveau l'application Machine Learning Analytics à partir de la page Paramètres Machine Learning.

## Avant de commencer

Depuis UBA avec ML V2.2.0, plus aucune procédure de mise à niveau n'est nécessaire. L'application Machine Learning est automatiquement mise à niveau avec l'application UBA. Une fois que vous avez installé ou mis à niveau votre application UBA (User Behavior Analytics), vous pouvez mettre à niveau votre application Machine Learning Analytics existante à partir de la page Paramètres Machine Learning.

**Avertissement :** Si l'application Machine Learning Analytics (ML) V2.0.0 est installée et que vous effectuez la mise à niveau vers la dernière version de l'application UBA, ne désinstallez pas l'application

Machine Learning Analytics à partir de QRadar Extension Manager. Si vous tentez de désinstaller l'application Machine Learning Analytics à partir de l'outil Extension Manager, des problèmes peuvent survenir lors de l'installation de votre application ML.

**Remarque :** Si vous effectuez une mise à niveau à partir de l'application Machine Learning Analytics V2.1.0 ou inférieure, la valeur **Valeur de risque de l'événement Sense** de chaque User Analytic sera mise à niveau sur la valeur Machine Learning actuelle.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation (☰) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.

### User Analytics

  
UBA Settings

  
Machine Learning  
Settings

  
Help and Support

3. Sur la page Paramètres Machine Learning, cliquez sur **Mettre à niveau l'application ML**.
4. A l'invite, cliquez sur **Oui**. La mise à niveau de l'application ML dure quelques minutes.
5. Une fois la mise à niveau terminée, la génération du modèle recommence.

## Que faire ensuite

Vérifiez que vos paramètres Machine Learning sont correctement configurés. Si vous changez des paramètres, pensez à sélectionner l'option **Sauvegarder la configuration**.

---

## Configuration des paramètres Machine Learning Analytics

Pour afficher des informations dans l'application Machine Learning Analytics, vous devez configurer les paramètres de cette dernière.

### Configuration de l'analyse *Activité totale*

Configurez l'analyse Machine Learning *Activité totale* pour afficher, sur le Tableau de bord UBA, le nombre d'activités des utilisateurs réelles et attendues (apprises) relevées au cours de la journée.

### Pourquoi et quand exécuter cette tâche

**Avertissement :** Une fois les paramètres configurés ou modifiés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

**Important :** Depuis la version 2.2.0, les valeurs par défaut de **Valeur de risque de l'événement Sense** ont été modifiées. Etant donné que ces nouvelles valeurs sont significativement inférieures aux valeurs par défaut précédentes, elles remplacent les valeurs par défaut existantes ou toutes les valeurs que vous avez précédemment modifiées.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
3. Sur la page Paramètres Machine Learning, cliquez sur **Activité totale**.

4. Cliquez sur **Activé**  pour activer l'analyse *Activité totale*.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Activité totale*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Activité totale* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

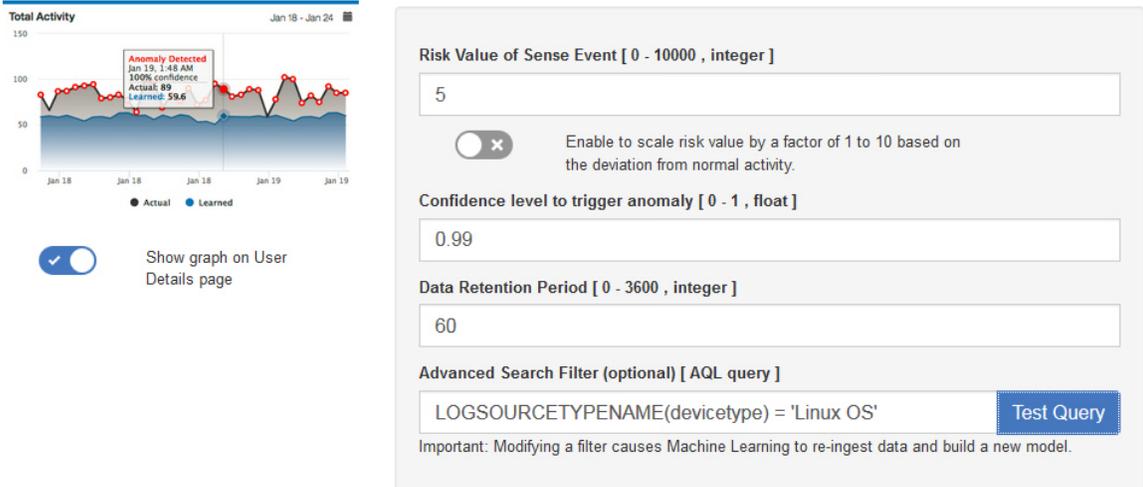
- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**

- `INCIDR('172.16.0.0/12', sourceip)` or `INCIDR('10.0.0.0/8', sourceip)` or `INCIDR('192.168.0.0/16', sourceip)`

Pour plus d'informations, consultez Ariel Query Language.

## 11. Cliquez sur **Sauvegarder la configuration**.

**Total Activity** Track a user's general activity by time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.



## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Tentatives de transfert sortant anormales*

Configurez l'analyse Machine Learning *Tentatives de transfert sortant anormales* pour afficher la part de trafic sortant utilisée par chaque utilisateur, sur le Tableau de bord UBA.

## Pourquoi et quand exécuter cette tâche

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

L'analyse Machine Learning *Tentatives de transfert sortant anormales* est disponible dans la version 2.8.0 et éditions ultérieures.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.

- Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
3. Sur la page Paramètres Machine Learning, cliquez sur **Tentatives de transfert sortant anormales**.
  4. Cliquez sur **Activé**  pour activer l'analyse *Tentatives de transfert sortant anormales*.

**Important :** Vous devez disposer de sept jours de données à compter du moment où le contenu UBA est activé sur le système.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est désactivée par défaut. Activez-la si vous voulez afficher le graphique *Tentatives de transfert sortant anormales* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

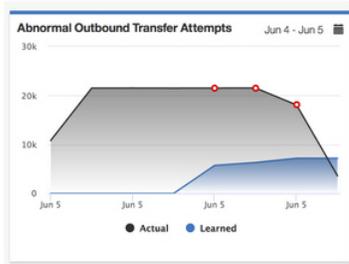
- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

11. Cliquez sur **Sauvegarder la configuration**.

### Abnormal Outbound Transfer Attempts

Monitors outbound traffic usage for each user and alerts on abnormal behavior. When the actual number of transfer attempts exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.



Show graph on User Details page

Risk Value of Sense Event [ 0 - 10000 , integer ]

5



Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

0.99

Data Retention Period [ 0 - 3600 , integer ]

60

Advanced Search Filter (optional) [ AQL query ]

LOGSOURCETYPENAME(devicetype) = 'Linux OS'

Test Query

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Activité par catégorie*

Configurez l'analyse Machine Learning *Activité par catégorie* pour afficher, sur le Tableau de bord UBA, les schémas comportementaux réels et attendus des activités des utilisateurs, par catégorie de haut niveau.

## Pourquoi et quand exécuter cette tâche

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

**Important :** Depuis la version 2.2.0, les valeurs par défaut de **Valeur de risque de l'événement Sense** ont été modifiées. Etant donné que ces nouvelles valeurs sont significativement inférieures aux valeurs par défaut précédentes, elles remplacent les valeurs par défaut existantes ou toutes les valeurs que vous avez précédemment modifiées.

## Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
- Sur la page Paramètres Machine Learning, cliquez sur **Activité par catégorie**.

4. Cliquez sur **Activé**  pour activer l'analyse *Activité par catégorie* et afficher le graphique correspondant sur la page Détails de l'utilisateur.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle initial. Si vous disposez de moins de sept jours de données utilisateur pour ce système QRadar, le modèle initial sera alors généré dès que vous disposerez de ces données.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Activité par catégorie*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Activité par catégorie* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 1.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la section **Catégories à suivre**, les catégories d'événement de niveau élevé sont activées par défaut. Cliquez sur une catégorie pour qu'elle ne soit pas surveillée. Pour plus d'informations sur les catégories, voir la rubrique relative aux catégories de niveau élevé dans IBM Knowledge Center.
10. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
11. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

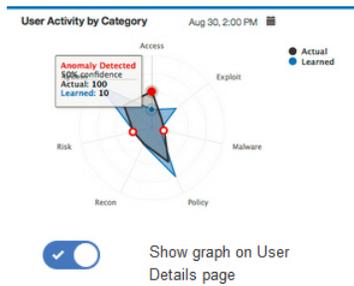
- `REFERENCESETCONTAINS('Important People', username)`
- `LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')`
- `INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)`

Pour plus d'informations, consultez Ariel Query Language.

12. Cliquez sur **Sauvegarder la configuration**.

## Activity by Category

Track a user's activity per high-level category in time and create a model for the predicted weekly behavior patterns. If the user's activity pattern (per category) deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.



**Risk Value of Sense Event [ 0 - 10000 , integer ]**  
1

Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

**Confidence level to trigger anomaly [ 0 - 1 , float ]**  
0.99

**Categories to track** ?

<input checked="" type="checkbox"/> Access	<input checked="" type="checkbox"/> Application
<input checked="" type="checkbox"/> Audit	<input checked="" type="checkbox"/> Authentication
<input checked="" type="checkbox"/> Control System	<input checked="" type="checkbox"/> DOS
<input checked="" type="checkbox"/> Exploit	<input checked="" type="checkbox"/> Flow
<input checked="" type="checkbox"/> Malware	<input checked="" type="checkbox"/> Policy
<input checked="" type="checkbox"/> Potential Exploit	<input checked="" type="checkbox"/> Recon
<input checked="" type="checkbox"/> Risk	<input checked="" type="checkbox"/> SIM Audit
<input checked="" type="checkbox"/> Suspicious Activity	<input checked="" type="checkbox"/> System
<input checked="" type="checkbox"/> Unknown	<input checked="" type="checkbox"/> User Defined

**Data Retention Period [ 0 - 3600 , integer ]**  
60

**Advanced Search Filter (optional) [ AQL query ]**  
LOGSOURCETYPENAME(devicetype) = 'Linux OS' Test Query

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Degré d'exposition au risque*

Configurez l'analyse Machine Learning *Degré d'exposition au risque* pour afficher, sur le Tableau de bord UBA, l'écart du score de risque de l'utilisateur par rapport au schéma attendu.

## Pourquoi et quand exécuter cette tâche

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

**Important :** Depuis la version 2.2.0, les valeurs par défaut de **Valeur de risque de l'événement Sense** ont été modifiées. Etant donné que ces nouvelles valeurs sont significativement inférieures aux valeurs par défaut précédentes, les nouvelles valeurs remplaceront les valeurs par défaut existantes ou toute valeur précédemment modifiée.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
3. Sur la page Paramètres Machine Learning, cliquez sur **Degré d'exposition au risque**.

4. Cliquez sur **Activé**  pour activer l'analyse *Degré d'exposition au risque*.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Degré d'exposition au risque*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Degré d'exposition au risque* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

11. Cliquez sur **Sauvegarder la configuration**.

## Risk Posture

Track a user's risky activity by the rate of sense events generated and create a baseline model. If the user's risky activity deviates from the baseline, it is deemed suspicious and a sense event is generated to increase the user's overall risk score.



Risk Value of Sense Event [ 0 - 10000 , integer ]

5



Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

0.99

Data Retention Period [ 0 - 3600 , integer ]

60

Advanced Search Filter (optional) [ AQL query ]

LOGSOURCETYPENAME(devicetype) = 'Linus OS'

Test Query

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Volume anormal de données circulant vers des domaines externes*

Configurez l'analyse Machine Learning *Volume anormal de données circulant vers des domaines externes* pour afficher, sur le Tableau de bord UBA, le volume de téléchargement local et distant pour chaque utilisateur.

## Pourquoi et quand exécuter cette tâche

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

L'analyse Machine Learning *Volume anormal de données circulant vers des domaines externes* est disponible dans la version 3.0.0 et éditions ultérieures.

## Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation (☰) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
3. Sur la page Paramètres Machine Learning, cliquez sur **Volume anormal de données circulant vers des domaines externes**.

4. Cliquez sur **Activé**  pour activer l'analyse *Volume anormal de données circulant vers des domaines externes*.

**Important :** Vous devez disposer de sept jours de données à compter du moment où le contenu UBA est activé sur le système.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est désactivée par défaut. Activez-la si vous voulez afficher le graphique *Volume anormal de données circulant vers des domaines externes* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 1.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

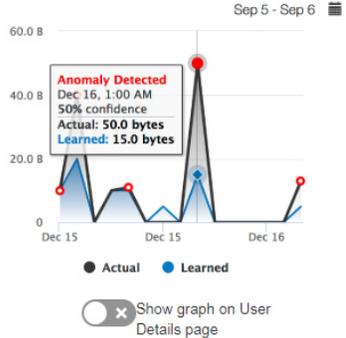
11. Cliquez sur **Sauvegarder la configuration**.

### Abnormal Volume of Data to External Domains

Monitors external domain data usage for each user and alerts on abnormal behavior. When the actual number of external domain data usage exceeds the model's predicted number, a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.



#### Abnormal Volume of Data to External Domains



Risk Value of Sense Event [ 0 - 10000 , integer ]

5

Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

0.99

Data Retention Period [ 0 - 3600 , integer ]

60

Advanced Search Filter (optional) [ AQL query ]

Example query: LOGSOURCETYPENAME(devicetype) = 'Linux OS'

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Distribution de l'activité*

Configurez l'analyse Machine Learning *Distribution de l'activité* pour afficher, sur le Tableau de bord UBA, les groupes (clusters) de comportements dynamiques pour tous les utilisateurs surveillés par Machine Learning.

## Pourquoi et quand exécuter cette tâche

L'analyse Machine Learning *Distribution de l'activité* est disponible dans la version 2.2.0 et éditions ultérieures.

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

## Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
- Sur la page Paramètres Machine Learning, cliquez sur **Distribution de l'activité**.
- Cliquez sur **Activé**  pour activer l'analyse *Distribution de l'activité* et afficher le graphique correspondant sur la page Détails de l'utilisateur.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Distribution de l'activité*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Distribution de l'activité* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

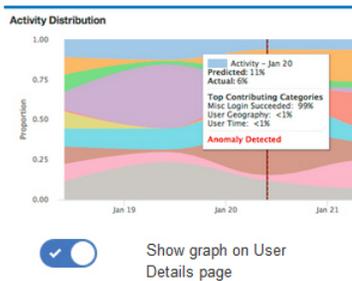
- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

11. Cliquez sur **Sauvegarder la configuration**.

## Activity Distribution

For each user, learn behavior clusters that represent groups of similar activity (similar low-level categories of QRadar). Search for deviations from the normal distribution of these clusters over time. Malicious behavior can manifest as changes in the distribution of a user's behavior cluster; that is, the user's activities begin to deviate from his customary activities. Similar activities are represented by the same colors for all users.



Risk Value of Sense Event [ 0 - 100 , integer ]

5



Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

0.99

Data Retention Period [ 0 - 3600 , integer ]

60

Advanced Search Filter (optional) [ AQL query ]

LOGSOURCETYPENAME(devicetype) = 'Linux OS'

Test Query

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Groupe d'homologues défini*

Configurez l'analyse Machine Learning *Groupe d'homologues défini* pour afficher, sur le Tableau de bord UBA, une indication de l'écart entre l'activité d'un utilisateur (en termes d'événements) et celle de son groupe d'homologues défini.

### Avant de commencer

- Pour activer l'analyse *Groupe d'homologues défini* défini, vous devez avoir des groupes d'utilisateurs valides dans une table de référence puis configurer **Paramètres UBA > Afficher les attributs > Groupe personnalisé** pour utiliser la table de référence. Pour plus d'informations, voir «Groupes d'utilisateurs pour l'analyse du groupe d'homologues défini», à la page 201.
- Vous devez disposer de sept jours de données d'événement pour que l'analyse puisse générer un modèle.

### Pourquoi et quand exécuter cette tâche

L'analyse Machine Learning *Groupe d'homologues défini* est disponible dans la version 2.6.0 et éditions ultérieures.

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.

- Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
    - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
    - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
  3. Sur la page Paramètres Machine Learning, cliquez sur *Groupe d'homologues défini*.

4. Cliquez sur **Activé**  pour activer l'analyse *Groupe d'homologues défini*.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Groupe d'homologues défini*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Groupe d'homologues défini* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Dans la zone **Grouper par**, sélectionnez le groupe devant être utilisé par l'analyse *Groupe d'homologues défini*.
11. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

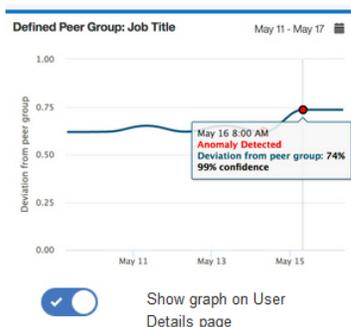
- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

12. Cliquez sur **Sauvegarder la configuration**.

## Defined Peer Group

Users are grouped and analyzed based on the "Group by" field. If a user's current behavior is significantly different from the user's defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.



Risk Value of Sense Event [ 0 - 100 , integer ]

Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

Data Retention Period [ 0 - 3600 , integer ]

Group By

Custom Group

Advanced Search Filter (optional) [ AQL query ]

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Configuration de l'analyse *Groupe d'homologues enregistré*

Configurez l'analyse Machine Learning *Groupe d'homologues enregistré* pour afficher, sur le Tableau de bord UBA, dans quelle mesure l'utilisateur diffère du groupe d'homologues déduit dans lequel on s'attendait à le trouver.

### Avant de commencer

- Vous devez installer un noeud d'application pour activer l'analyse *Groupe d'homologues enregistré*. Pour plus d'informations, voir [https://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.3.0/com.ibm.qradar.doc/c\\_adm\\_appnode\\_intro.html](https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/c_adm_appnode_intro.html)
- Vous devez disposer de sept jours de données d'événement pour que l'analyse *Groupe d'homologues enregistré* puisse générer un modèle.

### Pourquoi et quand exécuter cette tâche

L'analyse Machine Learning *Groupe d'homologues enregistré* est disponible dans la version 2.2.0 et éditions ultérieures.

**Avertissement :** Une fois les paramètres configurés, il est nécessaire d'attendre au minimum une heure avant l'ingestion des données, la génération d'un modèle initial et l'affichage des résultats initiaux pour les utilisateurs.

### Procédure

1. Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.

- Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation () puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
2. Cliquez sur l'icône **Paramètres Machine Learning**.
    - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
    - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.
  3. Sur la page Paramètres Machine Learning, cliquez sur *Groupe d'homologues enregistré*.

4. Cliquez sur **Activé**  pour activer l'analyse *Groupe d'homologues enregistré*.

**Important :** Vous devez disposer de sept jours de données pour que l'analyse puisse générer un modèle.

5. L'option **Afficher le graphique sur la page Détails de l'utilisateur** est activée par défaut pour le graphique *Groupe d'homologues enregistré*, qui sera donc affiché sur la page Détails de l'utilisateur. Désactivez-la si vous ne voulez pas afficher le graphique *Groupe d'homologues enregistré* sur la page Détails de l'utilisateur.
6. Dans la zone **Valeur de risque de l'événement Sense**, entrez une valeur afin d'augmenter le score de risque de l'utilisateur avant le déclenchement d'un événement Sense. La valeur par défaut est 5.
7. Activez l'option de basculement pour évaluer la valeur de risque. Lorsque cette option est activée, la valeur du risque de base est multipliée par un facteur compris entre 1 et 10. Ce facteur est déterminé en fonction du degré d'écart de l'utilisateur par rapport à son comportement attendu.
8. Dans la zone **Intervalle de confiance pour le déclenchement d'une anomalie**, entrez le pourcentage de confiance de l'algorithme Machine Learning avant le déclenchement d'un événement d'anomalie. La valeur par défaut est 0,99.
9. Dans la zone **Durée de conservation des données**, définissez le nombre de jours durant lesquels vous souhaitez conserver les données modèle. La valeur par défaut est 60. Si vous souhaitez désactiver la purge automatique des données, indiquez 0 (zéro).
10. Facultatif : Dans la zone **Filtre de recherche avancée**, vous pouvez ajouter un filtre AQL pour limiter l'étendue des données demandées par l'analyse dans QRadar. En filtrant au moyen d'une requête AQL, vous pouvez réduire le nombre d'utilisateurs ou de types de données que devra traiter l'analyse. Avant de sauvegarder la configuration, cliquez sur **Tester la requête** pour lancer une requête AQL complète dans QRadar afin de pouvoir l'examiner et vérifier ses résultats.

**Important :** Si vous modifiez le filtre AQL, le modèle existant pour l'analyse sera marqué comme non valide et sera reconstruit. Le temps nécessaire à cette reconstruction dépendra de la quantité de données retournée par le filtre modifié.

Le filtrage peut s'exercer sur des sources de journaux particulières, des noms réseau spécifiques ou des ensembles de référence contenant des utilisateurs spécifiques. Etudiez les exemples suivants :

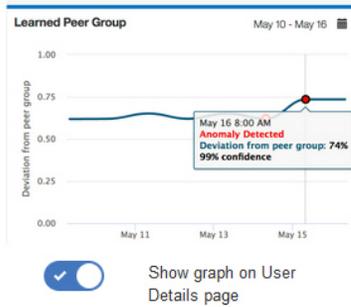
- **REFERENCESETCONTAINS('Important People', username)**
- **LOGSOURCETYPENAME(devicetype) in ('Linux OS', 'Blue Coat SG Appliance', 'Microsoft Windows Security Event Log')**
- **INCIDR('172.16.0.0/12', sourceip) or INCIDR('10.0.0.0/8', sourceip) or INCIDR('192.168.0.0/16', sourceip)**

Pour plus d'informations, consultez Ariel Query Language.

11. Cliquez sur **Sauvegarder la configuration**.

## Learned Peer Group

Identifies users who engage in similar activities and then places them into peer groups. If a user's current peer group is significantly different from former groups, then a Sense Event is generated to increase the user's risk score.



Risk Value of Sense Event [ 0 - 100 , integer ]

5



Enable to scale risk value by a factor of 1 to 10 based on the deviation from normal activity.

Confidence level to trigger anomaly [ 0 - 1 , float ]

0.99

Data Retention Period [ 0 - 3600 , integer ]

60

Advanced Search Filter (optional) [ AQL query ]

LOGSOURCETYPENAME(devicetype) = 'Linus OS'

Test Query

Important: Modifying a filter causes Machine Learning to re-ingest data and build a new model.

## Résultats

La procédure d'ingestion des données et de génération d'un modèle initial par l'application peut prendre au minimum une heure.

## Tableau de bord UBA avec Machine Learning Analytics

L'application IBM QRadar User Behavior Analytics (UBA) avec Machine Learning Analytics inclut le statut Machine Learning Analytics ainsi que des détails supplémentaires relatifs à l'utilisateur sélectionné.

### Tableau de bord

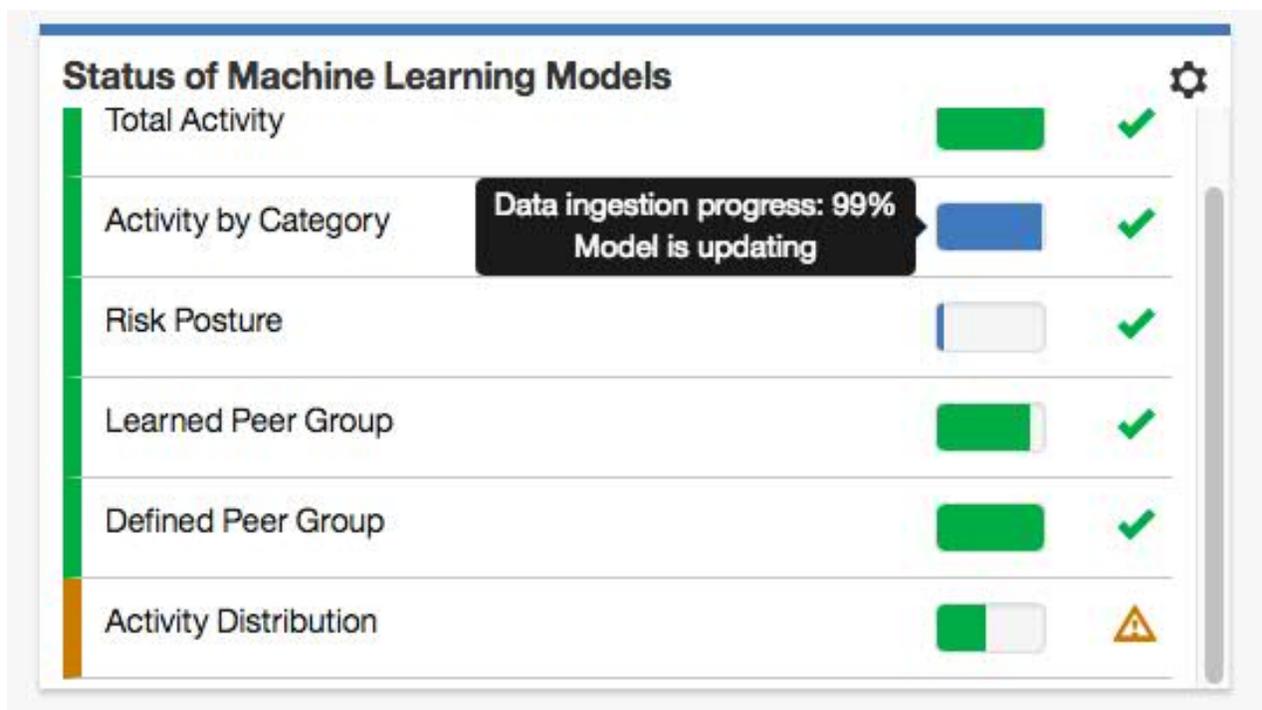
Une fois que vous avez activé l'application Machine Learning Analytics, cliquez sur l'onglet **Analyse utilisateur** pour ouvrir le tableau de bord.

La section Statut des modèles Machine Learning indique l'ingestion des modèles et la progression de la génération du modèle pour chaque analyse activée. Notez que les modèles sont mis à jour tous les sept jours.

- La barre de progression bleue indique que l'analyse est en train d'ingérer les données.
- La barre de progression verte indique que l'analyse est en train de générer le modèle.
- La coche verte indique que l'analyse est activée.
- L'icône d'avertissement jaune indique qu'un problème s'est produit lors de la phase de génération du modèle. Voir «Le statut de l'application Machine Learning affiche un avertissement dans le tableau de bord», à la page 206

Cliquez sur l'icône **Paramètres ML**  pour ouvrir la page Machine Learning Analytics et éditer la configuration des scénarios d'utilisation Machine Learning Analytics.

**Remarque :** Si vous modifiez la configuration après l'avoir enregistrée, un nouveau modèle est généré et le temps d'attente pour l'ingestion et la génération du modèle est réinitialisé.

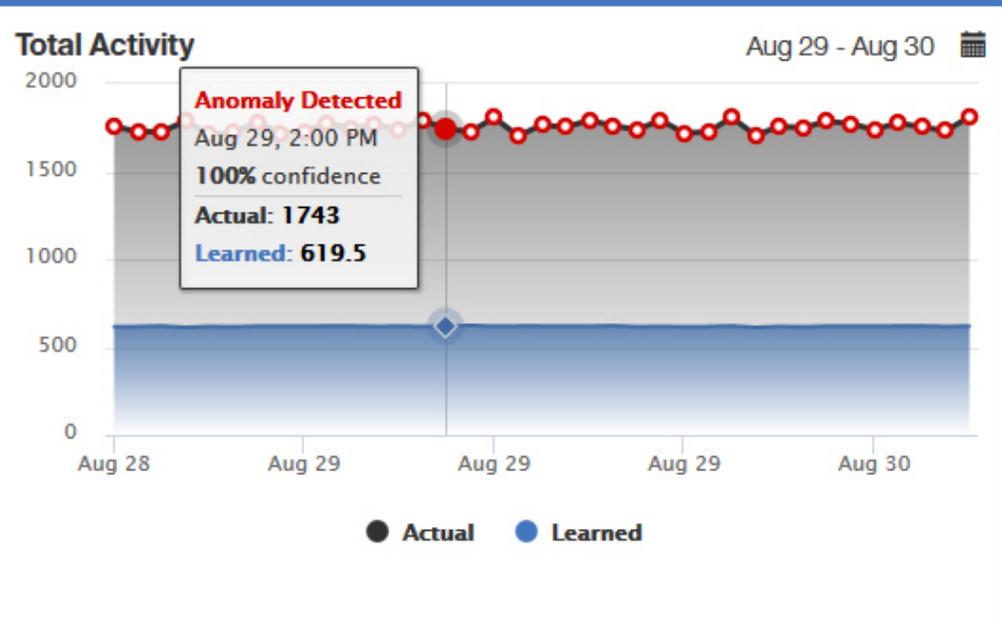


## Page Détails de l'utilisateur

Vous pouvez cliquer sur un nom d'utilisateur n'importe où dans l'application afin d'afficher des détails sur l'utilisateur sélectionné.

Depuis la version 2.5.0, vous pouvez en savoir plus sur les activités de l'utilisateur grâce au volet *Afficheur d'événements*. Le volet *Afficheur d'événements* contient des informations sur une activité sélectionnée ou un moment. Si vous cliquez sur le volet *Afficheur d'événements*, des informations supplémentaires, comme des événements syslog et des informations de contenu, s'affichent. Le volet *Afficheur d'événements* est disponible pour tous les graphiques en anneau et linéaires de la page *Détails de l'utilisateur*.

Le tableau ci-dessous décrit les graphiques Machine Learning Analytics disponibles sur la page *Détails de l'utilisateur*.

<p>Activité totale</p>	<p>Affiche le nombre d'activités réelles et attendues (apprentissage) des utilisateurs au cours de la journée. Les valeurs réelles correspondent au nombre d'événements pour cet utilisateur pendant la période sélectionnée. Les valeurs attendues correspondent au nombre d'événements prévus pour cet utilisateur pendant la période sélectionnée. Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning.</p> <p>Sur le graphique Activité totale, vous pouvez :</p> <ul style="list-style-type: none"> <li>• cliquer sur un noeud de données et obtenir une liste de requêtes des événements constituant l'anomalie.</li> <li>• cliquer sur l'icône <b>Calendrier</b> pour indiquer une plage de dates personnalisée.</li> </ul>  <p><b>Total Activity</b> Aug 29 - Aug 30 </p> <p>2000 1500 1000 500 0</p> <p><b>Anomaly Detected</b> Aug 29, 2:00 PM 100% confidence Actual: 1743 Learned: 619.5</p> <p>Aug 28 Aug 29 Aug 29 Aug 29 Aug 30</p> <p>● Actual ● Learned</p>
------------------------	--

Activité utilisateur par catégorie

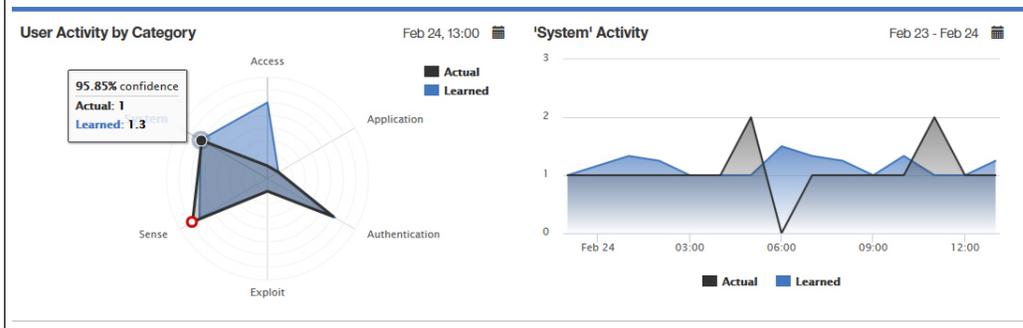
Affiche les schémas comportementaux des activités utilisateur réelles et attendues par catégorie de niveau supérieur. Les valeurs réelles correspondent au nombre d'événements par catégorie de niveau supérieur pour cet utilisateur pendant la période sélectionnée. Les valeurs attendues correspondent au nombre d'événements prévus par catégorie de niveau supérieur pour cet utilisateur pendant la période sélectionnée. Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning.

Dans le graphique Activité utilisateur par catégorie, vous pouvez :

- cliquer sur l'icône **Calendrier** pour indiquer une heure et une date.
- cliquer sur une catégorie pour ouvrir la ligne de temps correspondant à la catégorie sélectionnée.

Sur le graphique ligne de temps de la catégorie sélectionnée, vous pouvez :

- cliquer sur un noeud de données et obtenir une liste de requêtes des événements représentant ce noeud.
- cliquer sur l'icône **Calendrier** pour indiquer une plage de dates personnalisée.

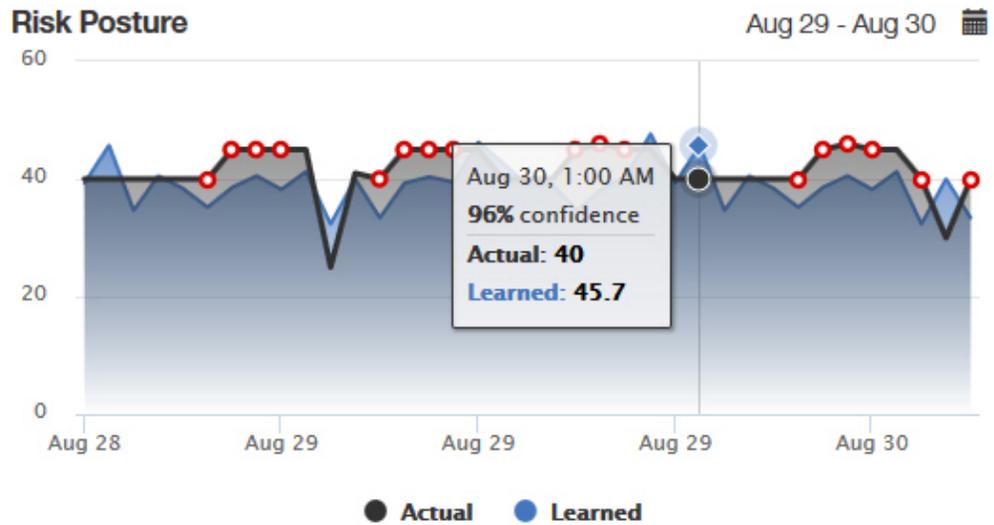


Degré d'exposition au risque

S'affiche lorsque le score de risque d'un utilisateur est différent du schéma de score de risque attendu. Les valeurs réelles correspondent à la somme des valeurs Sense pour les événements Sense de cet utilisateur pendant la période sélectionnée. Les valeurs attendues correspondent à la somme prévue des événements Sense pour cet utilisateur pendant la période sélectionnée. Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning.

Sur le graphique Degré d'exposition au risque, vous pouvez :

- cliquer sur un noeud et obtenir une liste de requêtes des événements.
- cliquer sur l'icône **Calendrier** pour indiquer une plage de dates personnalisée.

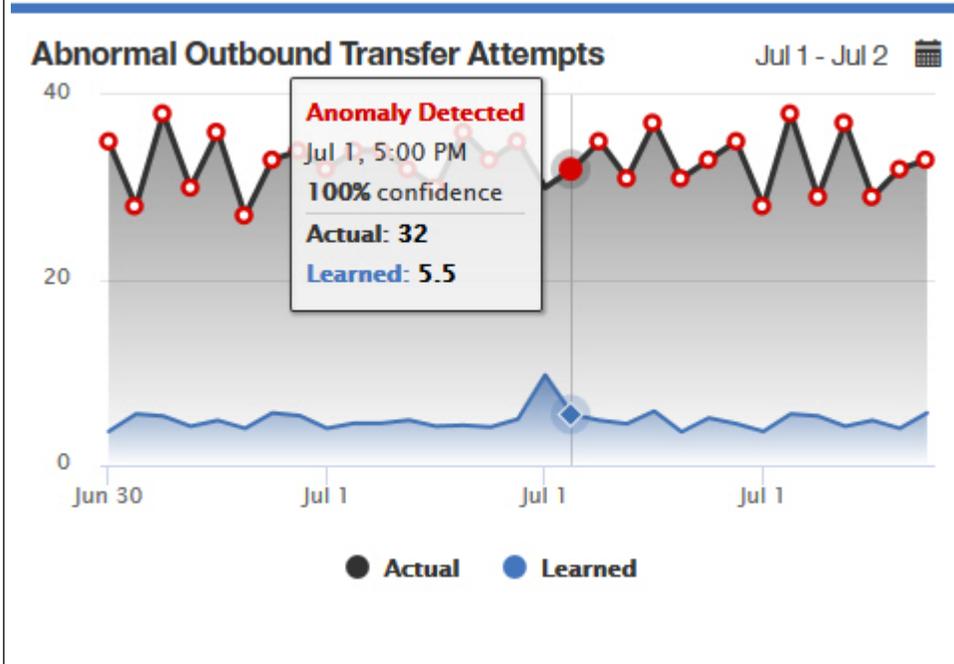


Tentatives de transfert sortant anormales

Montre si l'utilisation de trafic sortant par un utilisateur a dévié du schéma comportemental attendu. Les valeurs réelles correspondent au nombre de tentatives de transfert pour cet utilisateur pendant la période sélectionnée. Les valeurs apprises correspondent au nombre de tentatives de transfert prédit par le modèle. Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning.

Sur le graphique Tentatives de transfert sortant anormales, vous pouvez :

- cliquer sur un noeud et obtenir une liste de requêtes des événements.
- cliquer sur l'icône **Calendrier** pour indiquer une plage de dates personnalisée.

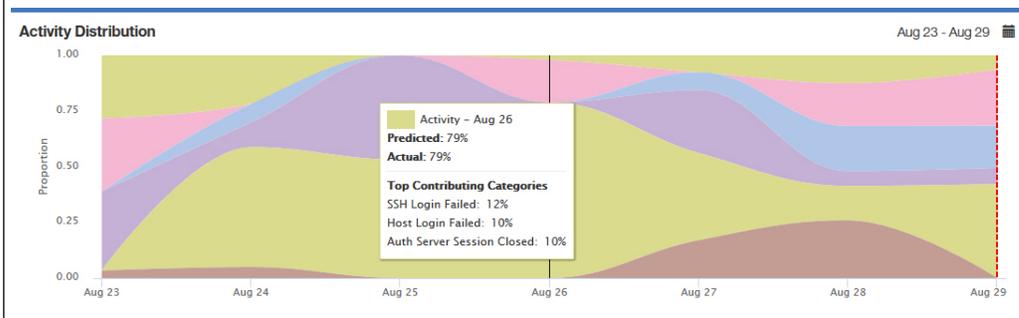


Distribution de l'activité (V2.2.0 ou version ultérieure)

Affiche les clusters de comportement dynamique pour tous les utilisateurs surveillés par l'application Machine Learning. Les clusters dépendent des catégories d'activités de niveau inférieur pour tous les utilisateurs surveillés par l'application Machine Learning. Les valeurs réelles sont la valeur en pourcentage correspondant au cluster. Les valeurs attendues sont la valeur prévue en pourcentage correspondant au cluster. Chaque couleur du graphique représente un cluster de comportement dynamique unique pour tous les utilisateurs surveillés par l'application Machine Learning. La même couleur est utilisée pour indiquer un groupe spécifique, quel que soit l'utilisateur. Une ligne rouge verticale indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning.

Dans le graphique Distribution de l'activité, vous pouvez :

- survoler chaque cluster pour afficher les percentiles réels et prévus ainsi que les trois principales catégories de niveau inférieur participantes.
- cliquer sur l'icône **Calendrier** pour indiquer une plage de dates.



Groupe d'homologues enregistré (V2.2.0 ou version ultérieure)

Présente dans quelle mesure l'utilisateur diffère du groupe d'homologues déduit dans lequel il était supposé être. Le groupe d'homologues enregistré est déduit des activités de niveau inférieur pour l'utilisateur.

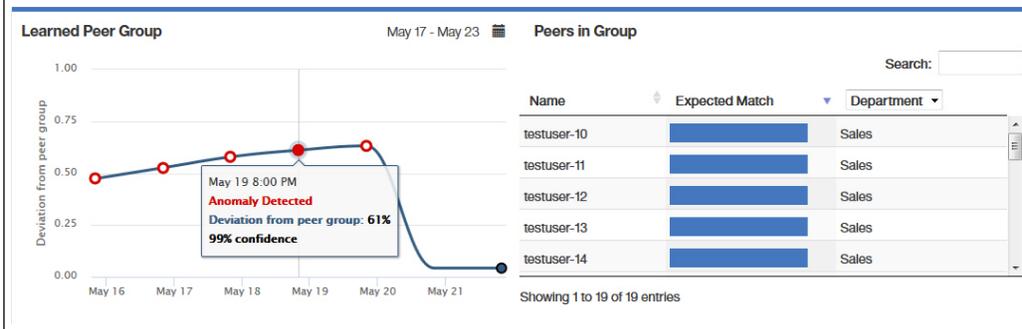
Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning. L'**Ecart vis-à-vis du groupe d'homologues** indique, en pourcentage, de combien l'utilisateur a dévié de son groupe d'homologues déduit. La **Fiabilité** est le percentile de l'écart dans le contexte des données historiques à partir desquelles le modèle est créé. Une alerte est émise si l'écart et la fiabilité dépassent tous deux leurs seuils respectifs fixés.

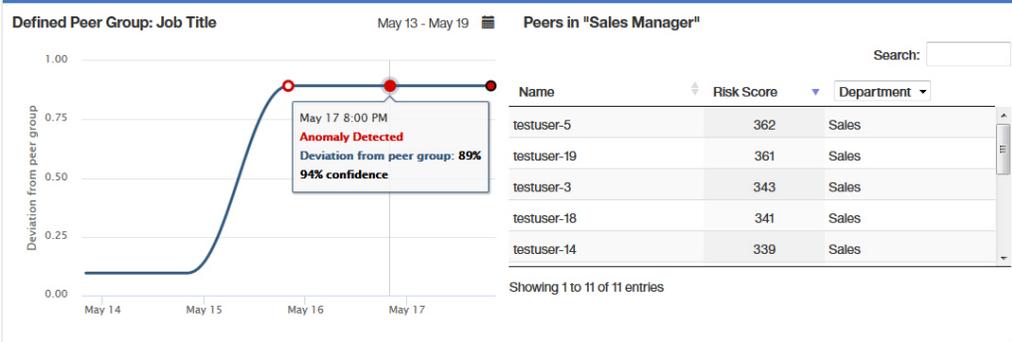
Sur le graphique Groupe d'homologues enregistré, vous pouvez :

- cliquer sur un point de données pour afficher la table Homologues dans le groupe.
- cliquer sur l'icône **Calendrier** pour indiquer une plage de dates.

La table Homologues dans le groupe présente tous les utilisateurs censés être dans le groupe et ceux se trouvant vraiment dans le groupe. Vous pouvez :

- cliquer sur un nom d'utilisateur pour ouvrir la page Détails de l'utilisateur
- La **Correspondance attendue** est le degré de fiabilité de l'analyse concernant la présence de cet utilisateur dans le groupe
- cliquer sur la liste déroulante pour sélectionner les attributs utilisateur à afficher
- effectuer une recherche en filtrant les noms d'utilisateur



<p>Groupe d'homologues défini (V2.6.0 ou version ultérieure)</p>	<p>Indique dans quelle mesure l'activité d'événement d'un utilisateur s'écarte de celle du groupe d'homologues défini. L'analyse utilise les catégories d'activité de niveau inférieur des événements des utilisateurs pour déterminer l'écart des utilisateurs par rapport au groupe d'homologues défini.</p> <p>Un cercle rouge indique qu'une anomalie a été détectée et qu'un événement Sense a été généré par l'application Machine Learning. L'<b>Ecart vis-à-vis du groupe d'homologues</b> indique, en pourcentage, de combien l'utilisateur a dévié de son groupe d'homologues défini. La <b>Fiabilité</b> est le percentile de l'écart dans le contexte des données historiques à partir desquelles le modèle est créé. Une alerte est émise si l'écart et la fiabilité dépassent tous deux leurs seuils respectifs fixés.</p> <p>Pour afficher l'analyse du groupe d'homologues défini, vous devez définir des groupes d'utilisateurs. Pour plus d'informations, voir «Groupes d'utilisateurs pour l'analyse du groupe d'homologues défini».</p> <p>Sur le graphique Groupe d'homologues défini, vous pouvez :</p> <ul style="list-style-type: none"> <li>• cliquer sur un point de données pour voir les homologues dans la table du "groupe d'homologues que vous avez défini".</li> <li>• cliquer sur l'icône <b>Calendrier</b> pour indiquer une plage de dates.</li> </ul> <p>Les homologues dans la table du "groupe d'homologues que vous avez défini" incluent les utilisateurs les plus risqués dans le groupe d'utilisateurs actuel de l'utilisateur. Vous pouvez :</p> <ul style="list-style-type: none"> <li>• cliquer sur un nom d'utilisateur pour ouvrir la page Détails de l'utilisateur</li> <li>• cliquer sur la liste déroulante pour sélectionner les attributs utilisateur à afficher</li> <li>• effectuer une recherche en filtrant les noms d'utilisateur</li> </ul> 
--	--

## Groupes d'utilisateurs pour l'analyse du groupe d'homologues défini

Vous pouvez activer l'analyse Groupe d'homologues défini dans l'application Machine Learning si UBA est configuré pour utiliser une table de référence contenant au moins deux groupements avec au minimum cinq utilisateurs utilisant un des groupes par sélection.

**Remarque :** A partir de la version 2.6.0, vous pouvez extraire des groupes d'utilisateurs dans UBA et activer l'analyse Groupe d'homologues défini.

Les sélections de regroupement sont **Fonction**, **Service**, ou toute autre propriété personnalisée que vous définissez sur la page Paramètres UBA dans la zone **Groupe personnalisé** sous Afficher les attributs. Lorsque UBA détecte plus de deux groupes distincts incluant chacun cinq utilisateurs ou plus, l'analyse Groupe d'homologues défini peut être activée. Pour avoir des groupes d'utilisateurs valides, vous pouvez configurer l'application Reference Data Import LDAP de telle sorte que les propriétés utilisateur (Fonction, Service ou autre groupement d'attributs LDAP) puissent être extraites en tant que table de référence. Vous pouvez ensuite configurer UBA afin que la table de référence que vous avez créée soit utilisée.

L'analyse Groupe d'homologues défini peut surveiller jusqu'à 20 groupes. Les 20 groupes les plus importants de la zone **Grouper par** configurée sont choisis. Le nombre d'utilisateurs à surveiller est proportionnellement réduit dans chaque groupe afin de respecter la limite de nombre d'utilisateurs surveillés pour la taille d'installation de Machine Learning.

**A faire :** L'importation de la table de référence a une planification de répétition de deux heures minimum, comme cela est configuré sur la page Paramètres UBA page. Tout nouvel attribut de groupement d'utilisateurs est importé lors de l'exécution de l'importation.

---

## Désinstallation de l'application Machine Learning Analytics

Désinstallez l'application Machine Learning Analytics à partir de la page Paramètres Machine Learning.

### Pourquoi et quand exécuter cette tâche

Avant de désinstaller l'application UBA, vous devez tout d'abord suivre la procédure présentée ci-dessous pour désinstaller l'application ML. Si vous n'avez pas effectué cette action, vous devez retirer l'application ML à partir de l'interface de la documentation d'API interactive.

### Procédure

- Ouvrez les paramètres **Admin** :
  - Dans IBM QRadar version 7.3.0 ou précédente, cliquez sur l'onglet **Admin**.
  - Dans IBM QRadar V7.3.1 et versions ultérieures, cliquez sur le menu de navigation (☰) puis cliquez sur **Admin** pour ouvrir l'onglet d'administration.
- Cliquez sur l'icône **Paramètres Machine Learning**.
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins > User Analytics > Paramètres Machine Learning**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications > Analyse utilisateur > Paramètres Machine Learning**.

#### User Analytics

---

  
UBA Settings

  
Machine Learning  
Settings

  
Help and Support

- Sur l'écran Paramètres Machine Learning, cliquez sur **Désinstaller l'application ML**.

User Analytics		Enable
<b>Total Activity</b>	Track a user's general activity by time and create a model for the predicted weekly behavior patterns. If the user's activity deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	<input checked="" type="checkbox"/>
<b>Activity by Category</b>	Track a user's activity per high-level category in time and create a model for the predicted weekly behavior patterns. If the user's activity pattern (per category) deviates from the learned behavior, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: Seven days of data are required for the analytic to generate a model and run.	<input checked="" type="checkbox"/>
<b>Risk Posture</b>	Track a user's risky activity by the rate of sense events generated and create a baseline model. If the user's risky activity deviates from the baseline, it is deemed suspicious and a sense event is generated to increase the user's overall risk score.	<input checked="" type="checkbox"/>
<b>Activity Distribution</b>	For each user, learn behavior clusters that represent groups of similar activity (similar low-level categories of QRadar). Search for deviations from the normal distribution of these clusters over time. Malicious behavior can manifest as changes in the distribution of a user's behavior cluster; that is, the user's activities begin to deviate from his customary activities. Similar activities are represented by the same colors for all users.	<input checked="" type="checkbox"/>
<b>Defined Peer Group</b>	Users are grouped and analyzed based on the "Group by" field. If a user's current behavior is significantly different from the user's defined group, it is deemed suspicious and a Sense Event is generated to increase the user's risk score. Note: You must have a minimum of two defined groups that each contains 5 or more users. If you change the group selection, a new model needs to be constructed. A significant amount of time and computer resources are required to complete the model creation. It is not recommended to change this value frequently.	<input checked="" type="checkbox"/>
<b>Learned Peer Group</b>	Identifies users who engage in similar activities and then places them into peer groups. If a user's current peer group is significantly different from former groups, then a Sense Event is generated to increase the user's risk score.	<input checked="" type="checkbox"/>

Save  
Configuration

4. A l'invite de désinstallation, cliquez sur **Oui**.

## Que faire ensuite

Vous devez vider le cache du navigateur avant de vous connecter à nouveau à la console QRadar.



---

## 10 Identification et résolution des problèmes et support

Pour identifier et résoudre les problèmes liés à votre produit IBM, vous pouvez utiliser les informations de support ainsi que d'identification et de résolution des problèmes.

Pour obtenir des réponses aux questions fréquentes concernant les applications User Behavior Analytics et Machine Learning Analytics, voir <https://developer.ibm.com/answers/topics/uba/>

---

### Page Aide et assistance d'UBA

L'application UBA (V2.5.0) inclut une section Aide et assistance pour utiliser les applications UBA, LDAP et Machine Learning Analytics.

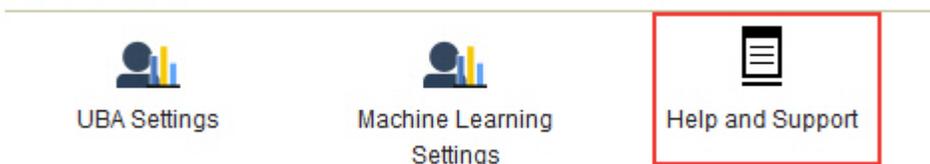
#### Accès à la page Aide et assistance d'UBA

La page Aide et assistance contient des liens vers la documentation, l'identification et la résolution des problèmes, l'assistance, les didacticiels vidéo, les fichiers journaux et les fonctions d'administration. Vous devez disposer de droits d'administrateur QRadar® pour afficher les fichiers journaux et les fonctions d'administration complètes à partir de la page Aide et assistance.

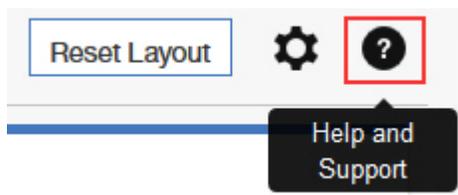
Une fois que l'application UBA a été installée, la page Aide et assistance est accessible aux endroits suivants :

- Dans les paramètres **Admin** :
  - Dans QRadar version 7.3.0 ou plus ancienne, cliquez sur **Plugins** > **User Analytics** > **Aide et assistance**.
  - Dans QRadar version 7.3.1 ou ultérieure, cliquez sur **Applications** > **Analyse utilisateur** > **Aide et assistance**.

#### User Analytics



- Sur l'onglet **Analyse utilisateur**, cliquez sur l'icône **Aide et assistance**.



### Fonctions d'administration

Pour afficher les fichiers journaux et les fonctions d'administration complètes, vous devez disposer de droits d'administrateur QRadar®.

Les fonctions d'administration incluent la possibilité d'exécuter les actions suivantes :

- Cliquez sur **Effacer les données UBA** pour supprimer toutes les données utilisateur d'UBA, mais conservez tous vos paramètres de configuration UBA actuels. Lorsque les données UBA sont effacées, l'application UBA se comporte que si vous veniez d'installer et de configurer **Paramètres UBA**. Si l'application Machine Learning est installée, le bouton **Effacer les données UBA** réinitialise également l'application ML.
- Cliquez sur **Réinitialiser les paramètres ML** si l'application Machine Learning est installée et que vous souhaitez réinitialiser tous vos paramètres Machine Learning et désactiver toutes les analyses activées.

---

## Demandes de service

Les demandes de service sont également appelées dossiers de gestion des problèmes.

Plusieurs méthodes permettent de soumettre des informations de diagnostic au support technique IBM Software. Pour ouvrir une demande de service ou pour échanger des informations avec le support technique, consultez la page IBM Software Support Exchanging information with Technical Support (<http://www.ibm.com/software/support/exchangeinfo.html>). Les demandes de service peuvent également être soumises directement en utilisant l'outil PMR ([http://www.ibm.com/support/entry/portal/Open\\_service\\_request](http://www.ibm.com/support/entry/portal/Open_service_request)).

---

## Le statut de l'application Machine Learning affiche un avertissement dans le tableau de bord

Si Statut des modèles Machine Learning affiche des messages d'avertissement dans le tableau de bord UBA, consultez les procédures pour résoudre le problème.

Si Statut des modèles Machine Learning affiche **Echec de génération du modèle** pour une analyse, vous pouvez essayer les suggestions ci-dessous pour résoudre le problème :

- Consultez les journaux des erreurs pour l'application ML.
- Vérifiez l'espace disque sur le système qui exécute l'application Machine Learning.
- Vérifiez que l'application UBA comporte des utilisateurs avec des événements.
- Contactez le service clients IBM.

### Concepts associés:

«Extraction des fichiers journaux UBA et Machine Learning», à la page 208

Les fichiers journaux UBA et Machine Learning vous permettent de résoudre plus facilement les différents problèmes.

---

## Le statut de l'application Machine Learning n'affiche pas de progression de l'ingestion des données

Si Statut des modèles Machine Learning semble être bloqué lors de la phase d'ingestion des données dans le tableau de bord UBA, consultez les procédures pour résoudre le problème.

Si Statut des modèles Machine Learning affiche n'affiche pas de progression de l'ingestion des données, vous pouvez essayer les suggestions ci-dessous pour résoudre le problème :

- Redémarrez le service serveur Ariel.
- Vérifiez l'espace disque sur le système en exécutant l'application Machine Learning.
- Vérifiez l'intérieur du conteneur ML pour savoir si le processus **UBAController** est en cours d'exécution.
- Contactez le service clients IBM.

## Statut d'erreur pour l'application ML

Si l'installation de l'application Machine Learning Analytics (ML) échoue et que la page Paramètres Machine Learning affiche le statut Erreur, vous pouvez utiliser l'outil de ligne de commande **cURL** et les paramètres de documentation d'API pour désinstaller l'application ML.

### Procédure

Si le statut de l'application ML sur la page Paramètres Machine Learning indique une erreur, procédez comme suit pour désinstaller l'application.

## Machine Learning Settings

### Setting up the Machine Learning Analytics (ML) App

1. Install and configure the User Behavior Analytics (UBA) app.
2. Verify the UBA app has polled once and that there is user data present.
3. Install proper version of the Machine Learning Analytics app. See the table for matching versions.
4. Return to the Machine Learning Analytics Configuration page to configure the Machine Learning Analytics app.

### ML APP Requirement Checks

Check	Current	Required	Status
QRadar Version	7.2.8	7.2.7+	
Security Token	Configured	Configured	
Available Memory	12 GB	5 GB	
ML App Status	Error	Running	

**Remarque :** Vous devez disposer d'un jeton d'authentification valide. Vous pouvez voir la liste des jetons d'authentification configurés dans la section Services autorisés des paramètres Admin de la console QRadar.

1. En utilisant SSH, connectez-vous à la console QRadar Console.
2. Exécutez la commande suivante :

```
# psql -U qradar -c 'select id,name,status from installed_application'
```

#### Exemple de résultat :

```
id | name | status
-----+-----
1356 | User Analytics | RUNNING
1358 | Machine Learning Analytics | ERROR
1357 | dataimport.ldap.applicationname | RUNNING
```

3. Dans le résultat de la commande, recherchez et enregistrez la valeur *id* pour Machine Learning Analytics.

4. En utilisant un jeton d'authentification valide à la place de *<jeton valide>* et la valeur de l'ID enregistrée à la place de l'élément *<id>*, exécutez la commande suivante pour désinstaller l'application Machine Learning : `# curl -X DELETE -k -H 'SEC:<jeton valide>' https://127.0.0.1/api/gui_app_framework/applications/<id>`

## Suppression de l'application Machine Learning

Pour supprimer l'application Machine Learning en utilisant l'API `gui_app_framework`, procédez comme suit :

1. Ouvrez la console QRadar Console et accédez à la page de la documentation d'API à l'emplacement suivant : `https://<port_adresse_hôte>/doc_api`
2. Ouvrez le dossier correspondant au numéro de version d'API le plus élevé (le numéro est différent en fonction de la version QRadar ; par exemple, 7.0 sur QR 7.2.8).
3. Ouvrez le dossier `/gui_app_framework` puis `select /applications`.
4. Vous êtes alors à l'étape d'obtention d'API. Cliquez sur le bouton "Essayer" pour obtenir la liste des applications installées.
5. Recherchez Machine Learning Analytics dans les résultats de l'étape 4 et obtenez la valeur de l'attribut `application_id`.
6. Développez le menu `/applications` dans les documentations d'API (même emplacement que l'étape 3), sélectionnez l'API `/application_id` puis cliquez sur l'onglet **SUPPRIMER**.
7. Entrez la valeur de l'ID application de l'étape 5 puis cliquez sur le bouton "Essayer" pour supprimer l'application.
8. L'API doit renvoyer un code d'état HTTP 204 pour indiquer que la suppression de l'application a abouti.

---

## Extraction des fichiers journaux UBA et Machine Learning

Les fichiers journaux UBA et Machine Learning vous permettent de résoudre plus facilement les différents problèmes.

### Téléchargement des fichiers journaux de l'application

Vous pouvez télécharger facilement les fichiers journaux pour l'application UBA et l'application Machine Learning sur «Page Aide et assistance d'UBA», à la page 205.

### Fichiers journaux de l'application UBA

Pour extraire manuellement les fichiers journaux de l'application UBA du conteneur Docker, procédez comme suit.

1. Sur l'hôte QRadar exécutant UBA, accédez à un répertoire disposant de suffisamment d'espace pour créer un fichier zip incluant tous les fichiers journaux de l'application.
2. Exécutez la commande suivante :

```
find /store/docker/v* -name uba.db
```

3. Copiez le chemin de répertoire précédant `uba.db`

Par exemple, pour le chemin de répertoire suivant  
`/store/docker/volumes/qapp-1001/uba.db`,  
copiez  
`/store/docker/volumes/qapp-1001/`

4. Exécutez la commande suivante en utilisant le chemin de répertoire de l'étape 1 :

```
zip -qr uba_logs.zip <votre_chemin_ici>log*
```

Par exemple :

```
zip -qr uba_logs.zip /store/docker/volumes/qapp-1001/log*
```

## Fichiers journaux de l'application Machine Learning

Pour extraire manuellement les fichiers journaux de l'application Machine Learning du conteneur Docker, procédez comme suit.

1. Sur l'hôte QRadar exécutant UBA, accédez à un répertoire disposant de suffisamment d'espace pour créer un fichier zip incluant tous les fichiers journaux de l'application.
2. Exécutez la commande suivante :

```
find /store/docker/v* -name itproot
```

3. Copiez le chemin de répertoire précédant itproot.

Par exemple, pour le chemin de répertoire suivant :

```
/store/docker/volumes/qapp-1003/itproot,
```

copiez

```
/store/docker/volumes/qapp-1003/
```

4. Exécutez la commande suivante en utilisant le chemin de répertoire de l'étape 1 :

```
zip -qr ml_logs.zip <votre_chemin_ici>log*
```

Par exemple :

```
zip -qr ml_logs.zip /store/docker/volumes/qapp-1003/log*
```



---

## Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations  
IBM Canada Ltd.  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510,  
Japon

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

---

## Marques

IBM, le logo IBM et [ibm.com](http://ibm.com) sont des marques d'International Business Machines Corp. dans de nombreux pays. D'autres noms de produit et de service peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans d'autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans d'autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et dans d'autres pays.

Java™ et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

---

## **Dispositions applicables à la documentation du produit**

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

### **Applicabilité**

Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

### **Usage personnel**

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

### **Usage commercial**

Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

### **Autorisations**

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

---

## **Déclaration IBM de confidentialité sur Internet**

Les logiciels IBM y compris les Logiciels sous forme de services ("Offres logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de

gestion des sessions et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/fr/fr>, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/details/fr/fr> ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse <http://www.ibm.com/software/info/product-privacy>.

---

## **Règlement général sur la protection des données**

Il incombe aux clients de veiller à leur propre conformité aux différentes lois et réglementations, y compris au Règlement général sur la protection des données (RGPD) de l'Union européenne. Il relève de la seule responsabilité du client de consulter les services juridiques compétents aussi bien pour identifier et interpréter les lois et règlements susceptibles d'affecter son activité, que pour toute action à entreprendre pour se mettre en conformité avec ces lois et réglementations. Les produits, services et autres fonctionnalités décrits ici ne sont pas adaptés à toutes les situations client et ne pourront être proposés que sous réserve de disponibilité. IBM ne fournit ni audit ni conseil juridique, ni déclaration, ni garantie que ses services ou produits assurent au client d'être en conformité avec la loi.

Pour en savoir plus sur la mise en conformité d'IBM avec le RGPD, ainsi que sur nos offres et fonctionnalités liées au RGPD, visitez le site <https://ibm.com/gdpr>.



