Aide de Content Gateway Manager

Websense® Content Gateway

v7.7

Aide en ligne de Websense Content Gateway

Mai 2012

Table des matières

1 Présentation

Websense® Content Gateway est le composant proxy Web des solutions Websense Web Security Gateway et Websense Web Security Gateway Anywhere.

Le proxy Web hautes performances Content Gateway, qui est configurable, fonctionne en association avec Websense Web Security pour protéger les utilisateurs et les réseaux contre tout contenu indésirable et malveillant en réalisant une analyse avancée du contenu au moment précis où celle-ci est nécessaire (c'est-à-dire quand le contenu passe par le proxy) et en exploitant les résultats de cette analyse pour appliquer la stratégie de sécurité Web appropriée. Cette analyse à la demande protège à la fois les utilisateurs et les réseaux, tout en sécurisant les sites Web 2.0 dynamiques pour votre organisation et vos utilisateurs.

L'application précise de l'analyse du contenu est configurée par l'administrateur pour chaque déploiement de Web Security Gateway (Anywhere).

Cache du proxy Web : Content Gateway peut également être configuré pour fonctionner sous forme de cache de proxy Web à hautes performances améliorant l'efficacité et les performances grâce à la mise en cache des informations fréquemment utilisées à l'extrémité du réseau. Le contenu est ainsi physiquement plus proche des utilisateurs, ce qui accélère sa livraison et réduit l'utilisation de la bande passante.

Content Gateway peut être déployé :

- *En tant que cache de proxy Web*
- *Dans une hiérarchie de caches*
- *Dans un cluster géré*
- *En tant que serveur SSL*
- *En tant que cache de proxy DNS*

Par ailleurs, Content Gateway peut être configuré pour exécuter plusieurs fonctions de sécurité :

- Contrôle de l'accès des clients au proxy
- Utilisation de différents serveurs DNS selon qu'ils doivent résoudre des noms d'hôtes situés à l'intérieur ou à l'extérieur d'un pare-feu. Vous pouvez ainsi sécuriser votre configuration réseau interne tout en autorisant un accès transparent aux sites externes via Internet.
- Authentification des clients avant leur accès au contenu. Content Gateway prend en charge l'authentification Windows intégrée et les services hérités NTLM (NTLMSSP), LDAP et RADIUS.

- Utilisation du moteur de stratégie prêt à l'emploi de Websense Data Security ou de l'interface ICAP pour que les sites qui utilisent Websense Data Security puissent examiner les documents sortants, par exemple les publications Web, et les bloquer ou les autoriser conformément à la stratégie de l'entreprise. Voir *Utilisation de Websense Data Security*, page 119.
- Contrôle de l'accès à Content Gateway Manager via :
  - Protection SSL (Secure Sockets Layer) pour un accès avec cryptage et authentification
  - Comptes utilisateur définissant les utilisateurs autorisés à accéder à Content Gateway Manager et les activités qu'ils peuvent exécuter (par exemple, afficher les statistiques seulement ou afficher les statistiques et configurer Content Gateway)
- Intégration au pare-feu et contrôle du trafic par l'intermédiaire d'un serveur SOCKS

Voir *Sécurité*, page 163.

Rubriques connexes :

- *TRITON Unified Security Center*, page 2
- *Options de déploiement*, page 3
- *Composants*, page 5
- *Fonctionnalités d'analyse du trafic du proxy*, page 8
- *Aide en ligne*, page 9
- *Support technique*, page 9

TRITON Unified Security Center

TRITON Unified Security Center est la console centrale de configuration et de gestion des modules TRITON Web Security, Data Security et Email Security. Cette console permet également d'accéder aux dispositifs V-Series.

Lors de l'installation, la console **TRITON Unified Security Center** est configurée pour que l'accès complet à l'ensemble des modules et paramètres TRITON ne soit accordé qu'à un seul compte d'administrateur : **admin**. Le mot de passe de ce compte est défini pendant l'installation.

La section **TRITON - Web Security** sert à configurer le comportement de Web Security, à surveiller l'utilisation Internet interne, à générer des rapports sur l'utilisation Internet et à gérer les paramètres de Websense Web Security. L'écran **Paramètres > Content Gateway Access** permet d'enregistrer des instances de Content Gateway. Les instances enregistrées présentent un indicateur d'intégrité du système et un lien conduisant au portail de connexion de Content Gateway Manager.

Pour obtenir une description complète de **TRITON Unified Security Center**, ouvrez la console **TRITON Unified Security Center**, puis le système d'Aide intégré.

Pour plus d'informations sur l'enregistrement et l'accès à Content Gateway Manager dans Websense Web Security, ouvrez la console **TRITON Unified Security Center**, puis le module Web Security et cliquez sur Aide.

Options de déploiement

En tant que cache de proxy Web

Lorsque Content Gateway est déployé sous forme de cache de proxy Web, les demandes de contenu Web des utilisateurs passent par Content Gateway avant de parvenir au serveur Web de destination (serveur d'origine). Si le cache de Content Gateway renferme le contenu demandé, Content Gateway répond directement à la demande. Si le cache Content Gateway ne renferme pas le contenu demandé, Content Gateway agit en tant que proxy et récupère le contenu sur le serveur d'origine au nom de l'utilisateur, tout en conservant une copie en vue des prochaines demandes.

Content Gateway est généralement déployé pour recevoir les demandes des clients de l'une des deux manières suivantes :

- En tant que *proxy explicite* dans lequel le navigateur ou le logiciel client de l'utilisateur est configuré pour envoyer directement les requêtes à Content Gateway. Voir *Proxy explicite*, page 39.
- En tant que *proxy transparent* dans lequel les requêtes des utilisateurs sont acheminées vers Content Gateway en toute transparence avant de parvenir au serveur de destination. Les utilisateurs demandent du contenu Internet de façon traditionnelle, sans aucune configuration de leur navigateur, et Content Gateway répond à ces demandes. Le logiciel client de l'utilisateur (en général, un navigateur) n'est pas conscient de communiquer avec un proxy. Voir *Proxy transparent et module ARM*, page 47.

Dans une hiérarchie de caches

Websense Content Gateway peut participer à des hiérarchies de cache flexibles, au sein desquelles les requêtes Internet non desservies par un cache peuvent être transmises à d'autres caches régionaux et tirer parti de la proximité de leur contenu. Dans une hiérarchie de serveurs proxy, Content Gateway peut agir en tant que parent ou enfant d'autres serveurs Content Gateway ou d'autres produits mis en cache. Voir *Mise en cache hiérarchique*, page 85.

Dans un cluster géré

Depuis son évolution d'un seul nœud à plusieurs nœuds, Websense Content Gateway peut former un cluster géré qui améliore les capacités, les performances et la fiabilité du système.

- Tout cluster géré détecte l'ajout et la suppression des nœuds.
- Les nœuds du cluster partageant automatiquement les informations de configuration, tous les membres du cluster peuvent être administrés simultanément.
- Lorsque SSL Manager est activé, les informations de configuration SSL sont également propagées autour du cluster. Toutefois, le mécanisme utilisé pour synchroniser ces informations n'est pas le même que pour les autres données.

Si l'option de basculement IP virtuel est activée, Content Gateway conserve un pool d'adresses IP virtuelles qu'il attribue aux nœuds du cluster. Content Gateway peut détecter les défaillances des nœuds (par exemple des pannes d'alimentation ou de processeur) et réaffecter les adresses IP du nœud défaillant aux nœuds fonctionnels. Pour plus d'informations, consultez la section *Basculement IP virtuel*, page 83.

Lorsque Content Gateway est configuré en tant que proxy transparent avec WCCP, le basculement est géré par WCCP et il est préférable de ne pas utiliser le basculement IP virtuel. Voir *Distribution de la charge WCCP*, page 52.

Pour plus d'informations, consultez la section *Clusters*, page 77.

En tant que serveur SSL

Lorsque SSL Manager est activé, les données HTTPS sont décryptées, examinées, puis à nouveau cryptées lorsqu'elles circulent entre le client et le serveur d'origine.

Content Gateway ne met pas les données HTTPS en cache.

SSL Manager inclut un jeu complet de capacités de gestion des certificats. Voir *Utilisation des données cryptées*, page 129.

Important

Même si SSL Manager n'est **pas** activé et que les données HTTPS ne sont pas décryptées, Content Gateway exécute un filtrage des URL HTTPS. Par conséquent, une recherche d'URL est effectuée pour chaque requête HTTPS et la stratégie est ensuite appliquée.

En mode proxy explicite, lorsque SSL est désactivé, Content Gateway filtre les URL sur la base du nom d'Hôte indiqué dans la requête. Si le site est bloqué, Content Gateway présente une page de blocage. Notez que certains navigateurs ne prennent pas en charge l'affichage de la page de blocage. Pour désactiver cette fonction, configurez vos clients de sorte qu'il n'envoient pas de requêtes HTTPS au proxy.

En mode proxy transparent, lorsque SSL est désactivé, Content Gateway filtre les URL sur la base du nom commun présent dans le certificat du serveur d'origine. Si le site est bloqué, la connexion au client est abandonnée. Aucune page de blocage ne s'affiche. Pour désactiver cette fonction lorsqu'elle est utilisée avec WCCP, ne créez pas de groupe de services pour HTTPS.

En tant que cache de proxy DNS

En tant que cache de proxy DNS, Content Gateway peut résoudre les requêtes DNS des clients. Ce fonctionnement décharge les serveurs DNS distants et accélère les recherches DNS. Voir *Mise en cache du proxy DNS*, page 95.

Composants

Cache

Le *cache* est constitué d'une base de données d'objets haut débit appelée magasin d'objets. Ce magasin indexe les objets en fonction des URL et des en-têtes associés. Le magasin d'objets peut mettre en cache d'autres versions du même objet, selon la langue utilisée ou le type d'encodage, et stocker des documents de petite ou grande taille, évitant ainsi le gaspillage d'espace disponible. Lorsque le cache est saturé, le proxy supprime les données périmées, les objets fréquemment demandés étant ainsi toujours à jour.

Content Gateway tolère les défaillances des disques mis en cache. En cas de panne complète d'un disque, Content Gateway le désigne comme endommagé et continue à utiliser les disques restants. En cas de défaillance de la totalité des disques mis en cache, Content Gateway passe en mode proxy uniquement.

Vous pouvez partitionner le cache afin de réserver de l'espace disque pour le stockage des données destinées à des protocoles et des serveurs d'origine spécifiques. Voir *Configuration du cache*, page 87.

Cache de mémoire RAM

Content Gateway gère un petit cache de mémoire RAM destiné aux objets extrêmement populaires. Ce cache de mémoire RAM dessert rapidement la plupart des objets populaires et réduit la charge des disques, en particulier pendant les périodes de fort trafic. La taille du cache de mémoire RAM peut être configurée. Voir *Modification de la taille du cache de mémoire RAM*, page 94.

Module ARM (Adaptive Redirection Module)

Le module ARM (Adaptive Redirection Module) assure plusieurs fonctions essentielles. L'une consiste à envoyer aux périphériques des notifications de basculement de l'interface de communication du cluster. L'autre consiste à examiner les paquets entrants avant que la couche IP ne les voit et à les envoyer ensuite à Content Gateway en vue de leur traitement.

Le module ARM est toujours actif.

Pour rediriger les requêtes des utilisateurs vers le proxy, le module ARM modifie l'adresse des paquets entrants. L'adresse IP de destination du paquet est alors remplacée par l'adresse IP du proxy, tandis que le port de destination du paquet est changé en fonction du protocole utilisé. Pour HTTP par exemple, le port de destination du paquet est remplacé par le port HTTP du proxy (en général, 8080).

Le module ARM prend en charge le contournement automatique des sites qui ne fonctionnent pas correctement avec les caches de proxy.

Le module ARM prévient également les surcharges de requêtes des clients. Lorsque le nombre de connexions client dépasse la limite définie, le module ARM transmet directement les requêtes entrantes au serveur d'origine. Voir *Délestage de la charge de connexion*, page 70.

Base de données d'hôtes

La base de données d'hôtes stocke les entrées DNS (Domain Name Server) des serveurs d'origine auxquels le proxy se connecte. Entre autres informations, cette base de données d'hôtes surveille :

- Les informations DNS (pour une conversion rapide des noms d'hôte en adresses IP)
- La version HTTP de chaque hôte (de sorte qu'il soit possible d'utiliser les fonctionnalités de protocole avancées avec les hôtes qui exécutent des serveurs modernes)
- Les informations de fiabilité et disponibilité des hôtes (pour éviter les attentes liées aux serveurs non fonctionnels)

Résolveur DNS

Pour garantir la transparence des déploiements de proxy, le proxy inclut un résolveur DNS asynchrone qui simplifie les conversions de noms d'hôte en adresses IP. Content Gateway implémente le résolveur DNS de façon native, en publiant directement des paquets de commandes DNS au lieu de compter sur les bibliothèques du résolveur. La plupart des requêtes DNS peuvent être envoyées en parallèle, tandis qu'un cache DNS rapide gère les liaisons courantes dans la mémoire, ce qui réduit le trafic DNS.

Important

En cas de modification de la configuration du serveur DNS d'un système Linux (/etc/resolv.conf), vous devez redémarrer Content Gateway.

Processus

Content Gateway comprend 5 processus principaux :

Nom du processus	Description
content_gateway	Accepte les connexions, traite les demandes de protocole et dessert les documents à partir du cache ou du serveur d'origine
content_manager	Démarre, surveille et reconfigure le processus **content_gateway** Le processus **content_manager** est également responsable de l'interface utilisateur de Content Gateway Manager, du port de configuration automatique du proxy, de l'interface des statistiques, de l'administration du cluster et du basculement IP virtuel. Lorsque le processus **content_manager** détecte une défaillance du processus **content_gateway**, il le redémarre et stocke toutes les requêtes entrantes dans une file d'attente de connexions. Les connexions entrantes reçues au cours des quelques secondes qui précèdent le redémarrage du serveur sont enregistrées dans la file d'attente des connexions et traitées en séquence. Cette mise en file d'attente des connexions protège les utilisateurs contre les délais d'inactivité liés au redémarrage du serveur.

Nom du processus	Description
content_cop	Surveille l'intégrité des processus **content_gateway** et **content_manager** Le processus **content_cop** interroge régulièrement (plusieurs fois par minute) les processus **content_gateway** et **content_manager** en émettant des requêtes de pulsation qui permettent de récupérer des pages Web synthétiques. Lorsqu'aucune réponse n'est reçue au cours de l'intervalle de délai d'expiration ou en cas de réception d'une réponse incorrecte, le processus **content_cop** redémarre les processus **content_manager** et **content_gateway**.
analytics_server	Gère les requêtes effectuées et les processus générés pour les Analyses de classification du contenu
download_service	S'exécute périodiquement afin de vérifier la présence de mises à jour sur le service Websense Database Download Service

Outils d'administration

Rubriques connexes :

- *Content Gateway Manager*, page 99
- *Interface de ligne de commande*, page 103
- *Fichiers de configuration*, page 104

Websense Content Gateway offre 3 modes d'administration :

- *Content Gateway Manager* est une interface de type Web accessible par le biais d'un navigateur. Content Gateway Manager fournit des vues graphiques et statistiques qui permettent de surveiller les performances et le trafic réseau de Content Gateway, ainsi que des options qui permettent de configurer et de paramétrer le proxy. Content Gateway Manager fournit un unique point d'administration, protégé par mot de passe et crypté via SSL, pour l'ensemble d'un cluster Content Gateway. Il s'agit là du mode d'administration conseillé.
- Une *interface de ligne de commande* vous permet de surveiller les performances et le trafic réseau de Content Gateway et de configurer le proxy. Vous pouvez exécuter des commandes individuelles ou un script d'une série de commandes dans une invite de commande. Cette méthode n'est disponible que partiellement lorsque Content Gateway est installé dans un dispositif Websense. Servez-vous dans ce cas de Content Gateway Manager et de l'outil Appliance Manager Command Line Utility.
- Les *fichiers de configuration* autorisent l'administration par le biais d'une interface d'édition des fichiers et de traitement des signaux. Vous pouvez modifier les options de configuration en éditant les fichiers de configuration au lieu d'utiliser Content Gateway Manager ou l'interface de ligne de commande. Toutes les modifications effectuées via Content Gateway Manager ou l'interface de ligne de commande sont automatiquement répliquées dans les fichiers de configuration.

Fonctionnalités d'analyse du trafic du proxy

Content Gateway fournit des options qui permettent d'analyser et de surveiller le trafic réseau :

- Les *statistiques et les graphiques de Websense Manager* donnent des informations sur le trafic réseau. Affichez les graphiques et les statistiques de Content Gateway Manager ou collectez et traitez des statistiques via l'interface de ligne de commande.
- Divers graphiques de *Performances* donnent des informations historiques sur l'utilisation de la mémoire virtuelle, les connexions des clients, les taux d'accès aux documents, etc. Affichez les graphiques *Performances* dans Content Gateway Manager.
- Les *alarmes de Websense Manager* sont présentées dans Content Gateway Manager. Content Gateway signale une alarme pour toute condition de défaillance détectée. Vous pouvez configurer Content Gateway pour qu'il envoie un e-mail au personnel d'assistance ou le prévienne par radiomessagerie lorsqu'une alarme se déclenche.

  Content Gateway envoie également certaines alarmes à TRITON - Web Security, où elles sont appelées **alertes**. Les messages d'alerte résumés s'affichent dans la page TRITON - Web Security **Status (État) > Today (aujourd'hui)**. Le message d'alerte complet s'affiche dans la page **Alertes**. Les administrateurs de TRITON - Web Security peuvent configurer quelles conditions de Content Gateway doivent entraîner l'envoi de messages d'alerte et quelles méthodes (e-mail ou SNMP) doivent être utilisées pour envoyer l'alerte.
- La *Journalisation des transactions* vous permet d'enregistrer dans un fichier journal des informations sur chaque requête reçue par le proxy et chaque erreur détectée. Servez-vous de ces journaux pour identifier le nombre d'individus utilisant le proxy, le volume d'informations demandées par chaque individu et les pages les plus populaires. Vous pouvez voir la raison pour laquelle une transaction a généré une erreur et l'état du cache du proxy à un moment donné. Par exemple, vous pouvez voir que Content Gateway a redémarré ou que la communication au cluster est arrivée à expiration.

  Content Gateway reconnaît plusieurs formats de fichier journal standard, tels que Squid et Netscape, et dispose de son propre format personnalisé. Vous pouvez analyser les fichiers journaux de format standard à l'aide de packages d'analyse prêts à l'emploi. Pour simplifier l'analyse des fichiers journaux, classez-les de sorte qu'ils contiennent des informations propres au protocole ou aux hôtes.

Pour plus d'informations sur les options d'analyse du trafic, consultez la section *Surveillance du trafic*, page 109. Pour plus d'informations sur les options de journalisation, consultez la section *Utilisation des fichiers journaux*, page 211.

Aide en ligne

Pour obtenir des informations détaillées sur l'utilisation du produit, cliquez sur le lien **Obtenir de l'aide !** dans toute page de Content Gateway Manager.

Important

Les paramètres par défaut de Microsoft Internet Explorer peuvent gêner le fonctionnement du système d'aide. Si une alerte de sécurité apparaît, sélectionnez **Autoriser le contenu bloqué** pour afficher l'Aide.

Si les règles de sécurité de votre organisation le permettent, vous pouvez désactivez définitivement le message d'avertissement dans l'onglet Avancés du menu **Outils** > **Options Internet**. (Cochez la case **Autoriser le contenu actif à s'exécuter dans des fichiers sur Mon ordinateur** sous les options de sécurité.)

Pour accéder à la version PDF de l'aide en ligne, aux Notes de publication, aux informations sur l'installation et le déploiement, aux FAQ, conseils et autres informations techniques, consultez la Bibliothèque technique de Websense.

Support technique

Des informations techniques sur les produits Websense sont disponibles 24 heures sur 24 à l'adresse :

http://support.websense.com

Le site du support technique vous permet d'accéder aux éléments suivants :

- Conseils
- Forums destinés aux clients
- Dernières informations sur les versions
- Base de connaissances Websense
- Correctifs récents
- Didacticiels et vidéos
- Documents relatifs aux produits
- Bibliothèque technique
- Réponses aux questions les plus fréquemment posées
- Documents techniques détaillés
- Wébinaires de support mensuels
- Alertes techniques
- Solutions les plus populaires

Le site du support technique de Websense permet d'accéder à l'ensemble des ressources techniques, y compris d'ouvrir un ticket d'incident via le portail Demande de service.

2 Mise en route

Dès que Content Gateway est installé dans votre système ou dans la totalité des nœuds de votre cluster, le proxy est prêt à l'emploi.

Pour commencer, reportez-vous aux procédures suivantes :

Accès à Content Gateway Manager

Content Gateway Manager est la console de gestion de Content Gateway.

Content Gateway Manager est pris en charge sur :

- Microsoft Internet Explorer 8 et 9
- Mozilla Firefox versions 5 et ultérieures
- Google Chrome 13 et versions ultérieures

L'utilisation d'autres navigateurs ou d'autres versions peut entraîner un comportement imprévu.

Java et JavaScript doivent être activés dans votre navigateur. Pour plus d'informations sur l'activation de Java et JavaScript, reportez-vous à la documentation de votre navigateur.

Trois méthodes permettent d'accéder à Content Gateway Manager :

- Par l'intermédiaire du bouton Content Gateway dans TRITON – Web Security.* Pour configurer l'accès à partir de TRITON – Web Security, reportez-vous à l'aide de ce dernier.
- En saisissant l'adresse IP et le port du système hôte de Content Gateway dans votre navigateur. Reportez-vous à la section ci-dessous.
- Lorsque Content Gateway est un module installé dans un dispositif V-Series, ouvrez le portail de connexion de V-Series et cliquez sur le bouton Content Gateway.

*Lorsque l'authentification à deux facteurs (certificat) est configurée dans TRITON Unified Security Center, le seul moyen d'accéder à Content Gateway Manager consiste

à utiliser le service d'authentification unique de TRITON – Web Security. Voir *Configuration de Content Gateway pour une authentification à deux facteurs*, page 13.

> **Remarque**
> Lorsque l'authentification unique est utilisée, le navigateur doit être configuré pour autoriser l'affichage des fenêtres contextuelles sur l'adresse IP de Content Gateway.

Pour accéder directement à Content Gateway Manager :

1. Ouvrez votre navigateur Web.
2. Entrez l'adresse suivante dans votre navigateur :

   `https://nomdunoeud:portadmin`

   où *nomdunoeud* correspond à l'adresse IP et *portadmin* au numéro de port affecté à Content Gateway Manager (8081 par défaut).

   Pour plus d'informations sur l'utilisation de HTTPS pour démarrer Content Gateway Manager, reportez-vous à la section *Utilisation de SSL pour l'administration sécurisée*, page 166.
3. Connectez-vous à Content Gateway Manager à l'aide de l'ID d'administrateur (par défaut : admin) et du mot de passe, ou à l'aide de votre compte d'utilisateur.

   Le mot de passe de Content Gateway Manager est défini lors de l'installation.

   Vous pouvez modifier l'ID et le mot de passe, et créer et modifier des comptes d'utilisateur. Voir *Contrôle de l'accès à Content Gateway Manager*, page 164.

Content Gateway Manager ouvre la page **Monitor (Surveiller) > Mon proxy > Résumé**. Cette page présente des informations sur les fonctionnalités de votre abonnement et des détails sur votre système Content Gateway. Consultez *Affichage des statistiques*, page 109 pour plus d'informations sur l'onglet Monitor (Surveiller) et *Configuration du système*, page 99, pour des informations sur les options de configuration de Content Gateway Manager.

Alertes de certificat de sécurité

Une connexion SSL est utilisée pour sécuriser les communications à base de navigateur avec Content Gateway Manager. Cette connexion utilise un certificat de sécurité émis par Websense, Inc. Les navigateurs pris en charge ne reconnaissant pas Websense, Inc. comme une autorité de certification reconnue, une erreur de certificat s'affiche au premier démarrage de Content Gateway Manager à partir d'un nouveau navigateur. Pour éviter cette erreur, vous pouvez installer ou accepter définitivement le certificat dans le navigateur. Pour plus d'informations, consultez la documentation de votre navigateur.

> **Remarque**
> Si vous utilisez Internet Explorer, l'erreur de certificat continue de s'afficher après l'acceptation du certificat. Vous devez dans ce cas fermer, puis rouvrir votre navigateur pour supprimer ce message d'erreur.

Considérations relatives à Windows 7

Si vous utilisez le système d'exploitation Windows 7, vous devez exécuter votre navigateur en tant qu'administrateur afin qu'il autorise les contrôles ActiveX.

1. Cliquez du bouton droit sur l'application du navigateur et sélectionnez **Exécuter en tant qu'administrateur**.
2. Connectez-vous à Content Gateway Manager et acceptez le certificat de sécurité selon les instructions précédentes.

Configuration de Content Gateway pour une authentification à deux facteurs

L'authentification (certificat) à deux facteurs :

- Est configurée pour la connexion à TRITON Unified Security Center et s'applique uniquement à celle-ci
- Implique que les administrateurs fournissent deux formes d'identification pour se connecter
- Peut être modifiée pour s'appliquer à Content Gateway Manager en obligeant les administrateurs à se connecter à TRITON Unified Security Center avant d'accéder à Content Gateway Manager
- Requiert la configuration de l'authentification unique pour les administrateurs autorisés à accéder à Content Gateway Manager
- Requiert la désactivation dans Content Gateway de la capacité de connexion par mot de passe, ce qui empêche les administrateurs non configurés pour l'authentification unique d'accéder à Content Gateway Manager. Lorsque Content Gateway est déployé dans un dispositif, l'accès par mot de passe est désactivé à l'aide d'une commande d'Appliance Manager. Reportez-vous à l'aide de V-Series Appliance Manager.

Pour plus d'informations sur la configuration de l'authentification à deux facteurs, reportez-vous à la section « Configuration de l'authentification des certificats » dans l'aide en ligne de la console TRITON.

Désactivation et activation de la connexion par mot de passe à Content Gateway

La connexion par mot de passe à Content Gateway Manager peut être désactivée pour n'autoriser que l'authentification à deux facteurs ou un accès via l'authentification unique depuis la console TRITON.

> **Remarque**
> Si Content Gateway est installé dans un dispositif Websense, reportez-vous à l'aide d'Appliance Manager pour plus d'informations.

Pour désactiver la connexion par mot de passe :

1. Configurez l'authentification unique dans TRITON – Web Security.
2. Si vous comptez utiliser l'authentification à deux facteurs, configurez-la dans TRITON Unified Security Center.
3. Connectez-vous au système hôte de Content Gateway et obtenez des privilèges racine.
4. Accédez au répertoire « /etc » et vérifiez qu'il contient un sous-répertoire « websense ». Si ce n'est pas le cas, créez-en un (« mkdir websense »).
5. Accédez au répertoire « websense » (le chemin d'accès est à présent /etc/websense) et voyez s'il contient le fichier « password-logon.conf ».
6. Si ce n'est pas le cas, créez-le (touch password-logon.conf).
7. Modifiez le fichier password-logon.conf.
8. Ajoutez la ligne suivante ou remplacez la ligne existante par :

   ```
   password-logon=disabled
   ```
9. Enregistrez et fermez le fichier.

Les modifications entrent immédiatement en vigueur. Il n'est pas nécessaire de redémarrer Content Gateway.

Pour réactiver la connexion par mot de passe pour tous les administrateurs :

1. Connectez-vous au système hôte de Content Gateway et obtenez des privilèges racine.
2. Accédez au répertoire /etc/websense.
3. Modifiez le fichier password-logon.conf en remplaçant :

   ```
   password-logon=disabled
   ```
   par :

   ```
   password-logon=enabled
   ```
4. Enregistrez et fermez le fichier.

Les modifications entrent immédiatement en vigueur. Il n'est pas nécessaire de redémarrer Content Gateway.

Saisie de votre clé d'abonnement

Rubrique connexe :

- *Informations système*, page 15

Lorsque Content Gateway est déployé avec Web Security Gateway ou Web Security Gateway Anywhere, il n'est pas nécessaire de saisir votre clé d'abonnement dans

Content Gateway Manager. Cette clé est automatiquement partagée lorsqu'elle est spécifiée dans TRITON –Web Security.

> **Remarque**
> L'instance de TRITON - Web Security utilisée dépend du Policy Server configuré. L'adresse IP du Policy Server configuré est indiquée dans Content Gateway Manager à la page **Monitor (Surveiller) > Mon proxy > Résumé** lorsque la vue **More Details (Plus de détails)** est sélectionnée.
>
> Pour configurer Policy Server :
>
> - Sur un dispositif V-Series, dans Appliance Manager, sélectionnez **Configuration > Web Security Components (Composants de sécurité Web)**.
> - Sur une installation logicielle, modifiez le fichier **/opt/WCG/websense.ini** en définissant la valeur de **PolicyServerIP**. Ensuite, arrêtez, puis redémarrez les processus Content Gateway :
>
> ```
> /opt/WCG/WCGAdmin stop
> /opt/WCG/WCGAdmin start
> ```

Lorsque Content Gateway est déployé avec Websense Data Security uniquement, vous devez saisir votre clé d'abonnement dans Content Gateway Manager.

1. Dans l'onglet **Configurer > Mon proxy > Abonnement > Gestion des abonnements**, saisissez la clé d'abonnement que vous a fournie Websense.
2. Cliquez sur **Appliquer**.
3. Cliquez sur **Redémarrer** dans la page **Configurer > Mon proxy > De base > Général**.

Informations système

Si Content Gateway est l'intégration proxy pour Websense Web Security (Web Security Gateway ou Web Security Gateway Anywhere), l'adresse IP et le port de Policy Server ont été définis pendant l'installation.

Pour terminer la configuration de Policy Server et des conditions d'expiration et de comportement de Filtering Service (autoriser ou bloquer le trafic), procédez comme suit :

1. Ouvrez l'onglet **Configurer > Mon proxy > Abonnement > Scanning (Analyse)**. Notez l'adresse IP et le port de Filtering Service. Il s'agit là des informations que vous avez saisies lors de l'installation de TRITON – Web Security.

> **Remarque**
> L'onglet Scanning (Analyse) ne s'affiche que si vous êtes abonné à Web Security Gateway ou à Web Security Gateway Anywhere.

2. Vérifiez le paramètre **Communication Timeout (Expiration de la communication)**. Ce paramètre définit le délai (en millisecondes) pendant lequel Content Gateway doit rester en communication avec Policy Server ou Filtering Service avant d'expirer et de déclencher le paramètre **Action for Communication Errors (Action pour erreurs de communication)**.

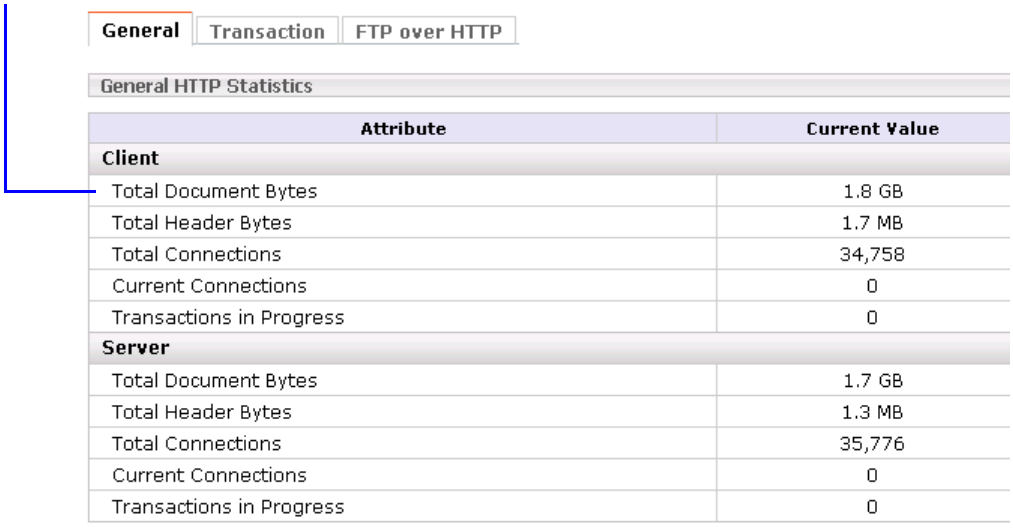
   La valeur d'expiration par défaut est 5 000 (5 secondes). Si vous modifiez cette valeur, vous devez redémarrer Content Gateway.
3. Dans la section **Action for Communication Errors (Action pour erreurs de communication)**, choisissez d'autoriser ou de bloquer le trafic lorsqu'une condition d'expiration de communication se produit. En cas d'expiration, Content Gateway applique alors le paramètre et interroge régulièrement les services afin de détecter leur remise en fonctionnement.
4. Cliquez sur **Appliquer**.

Vérification du traitement des requêtes Internet par le proxy

Après avoir installé le proxy, assurez-vous qu'il traite les demandes de contenu Web.

1. Ouvrez Content Gateway Manager. Voir *Accès à Content Gateway Manager*, page 11.
2. Ouvrez la page **Monitor (Surveiller) > Mon proxy > Résumé** pour consulter les détails de l'abonnement, l'état de l'analyse des fichiers de données et les détails des nœuds, notamment le nombre d'objets desservis, le taux d'accès et d'autres informations sur le service de proxy de base.
3. Ouvrez la page **Monitor (Surveiller) > Protocole > HTTP > Général** pour afficher le tableau General HTTP Statistics (Statistiques HTTP globales).
4. Notez la présence de la statistique **Total Document Bytes (Total des octets de documents)** dans la section **Client** de ce tableau.

Vérifiez la valeur de cette statistique.



Attribute	Current Value
Client	
Total Document Bytes	1.8 GB
Total Header Bytes	1.7 MB
Total Connections	34,758
Current Connections	0
Transactions in Progress	0
Server	
Total Document Bytes	1.7 GB
Total Header Bytes	1.3 MB
Total Connections	35,776
Current Connections	0
Transactions in Progress	0

4. Définissez votre navigateur sur le port du proxy.
5. Accédez à Internet.

6. Vérifiez à nouveau la statistique **Total Document Bytes (Total des octets de documents)**.

   Cette valeur augmente à mesure que le proxy traite les requêtes HTTP.

Utilisation de l'interface de ligne de commande

L'interface de ligne de commande est un moyen rapide d'afficher les statistiques du proxy et de configurer Content Gateway lorsque vous n'avez pas accès à un navigateur ou si vous préférez utiliser une interface de commande de type UNIX.

> **Remarque**
> L'interface de ligne de commande n'est pas disponible lorsque Content Gateway est installé dans un dispositif Websense. Servez-vous dans ce cas de Content Gateway Manager et de l'outil Appliance Manager Command Line Utility.

Vous pouvez exécuter des commandes individuelles ou un script de plusieurs commandes dans une invite de commande. Voir *Commandes de Websense Content Gateway*, page 259.

1. Devenez utilisateur racine :

   ```
   su
   ```

2. Accédez au répertoire **bin** de Content Gateway (/opt/WCG/bin). Exécutez les commandes Content Gateway dans ce répertoire.

   Les commandes prennent la forme suivante :

   ```
   content_line -argument de commande
   ```

3. Pour obtenir la liste des commandes **content_line**, saisissez :

   ```
   content_line -h
   ```

   > **Remarque**
   > Si le répertoire **bin** de Content Gateway ne fait pas partie de votre chemin, précédez la commande de : ./
   >
   > Par exemple :
   >
   > ```
   > ./content_line -h
   > ```

Démarrage et arrêt de Content Gateway via la ligne de commande

Pour arrêter ou démarrer Content Gateway à partir de la ligne de commande :

1. Devenez utilisateur racine :

   ```
   su
   ```

2. Accédez au répertoire d'installation de Content Gateway (/opt/WCG).

Pour démarrer le proxy :

```
./WCGAdmin start
```

Pour arrêter le proxy :

```
./WCGAdmin stop
```

Pour redémarrer le proxy :

```
./WCGAdmin restart
```

Pour identifier les services Content Gateway en cours d'exécution :

```
./WCGAdmin status
```

> **Remarque**
> Servez-vous systématiquement de la commande `./WCGAdmin stop` pour arrêter Content Gateway à partir de la ligne de commande.

Après avoir installé Content Gateway, ouvrez Content Gateway Manager (son interface de gestion) afin de vérifier que le proxy s'exécute. Voir *Accès à Content Gateway Manager*, page 11, et *Vérification du traitement des requêtes Internet par le proxy*, page 16.

3 Mise en cache du proxy Web

La mise en cache du proxy Web permet de stocker des copies des objets Web fréquemment consultés (par exemple les documents, images et articles) à proximité des utilisateurs pour pouvoir ensuite leur fournir ce contenu. Les utilisateurs d'Internet obtiennent dans ce cas leur contenu plus rapidement et la bande passante Internet peut servir à d'autres tâches.

Les utilisateurs d'Internet envoient leurs requêtes aux serveurs Web situés sur Internet. Pour qu'un serveur de mise en cache réponde à ces requêtes, il doit pouvoir jouer le rôle de proxy Web. Un serveur de proxy Web reçoit les demandes d'objets Web envoyées par les utilisateurs et y répond ou les transmet au *serveur d'origine* (serveur Web contenant la copie d'origine du contenu demandé).

Content Gateway prend à la fois en charge le *déploiement de proxy transparent*, dans lequel le logiciel client de l'utilisateur (en général un navigateur) n'a pas conscience de communiquer avec un proxy, et le *déploiement de proxy explicite*, dans lequel le logiciel client de l'utilisateur est configuré pour envoyer directement les requêtes au proxy.

Mise en cache des requêtes

Rubriques connexes :

- *Vérification de l'actualité des objets mis en cache*, page 20
- *Planification des mises à jour du contenu du cache local*, page 25
- *Épinglage du contenu dans le cache*, page 27
- *Mettre en cache ou non ?*, page 28
- *Mise en cache des objets HTTP*, page 29
- *Mise en cache obligatoire des objets*, page 35
- *Mise en cache des alternatives HTTP*, page 35
- *Mise en cache des objets FTP*, page 37

La présentation suivante montre comment Content Gateway répond à la requête d'un utilisateur.

1. Content Gateway reçoit une demande d'objet Web de la part d'un utilisateur.

2. Via l'adresse Web, le proxy tente de localiser l'objet demandé dans son magasin d'objets (cache).
3. Si cet objet est présent dans le cache, le proxy s'assure qu'il est suffisamment récent pour être envoyé à l'utilisateur (voir *Vérification de l'actualité des objets mis en cache*, page 20). Si l'objet est récent, le proxy l'envoie à l'utilisateur sous forme d'*accès au cache.*
4. Si les données du cache sont périmées, le proxy se connecte au serveur d'origine et vérifie que l'objet en question est encore actuel (revalidation). Dans l'affirmative, le proxy envoie immédiatement la copie mise en cache à l'utilisateur.
5. Si l'objet n'est pas dans le cache (absence dans le cache) ou si le serveur signale que la copie mise en cache n'est plus valide, le proxy récupère l'objet sur le serveur d'origine, et l'envoie simultanément à l'utilisateur et au cache. Les requêtes suivantes du même objet sont alors desservies plus rapidement puisque l'objet provient directement du cache.

Vérification de l'actualité des objets mis en cache

À réception d'une demande d'objet Web, Content Gateway tente de localiser l'objet demandé dans son cache. Si cet objet est présent dans le cache, le proxy s'assure qu'il est suffisamment récent pour être envoyé à l'utilisateur.

Le protocole détermine comment le proxy gère le caractère actualisé des objets présents dans le cache :

- Les objets HTTP reconnaissent les dates d'expiration définies par l'auteur. Le proxy respecte alors ces dates d'expiration. Sinon, il choisit une date d'expiration en fonction de la fréquence de modification de l'objet et des instructions définies par l'administrateur en matière d'actualité des objets. Par ailleurs, les objets peuvent être à nouveau validés via la vérification de leur caractère actualisé au niveau du serveur d'origine. Voir *Actualité d'un objet HTTP*, page 20.
- Les objets FTP restent dans le cache pendant une période définie. Voir *Actualité d'un objet FTP*, page 24.

Actualité d'un objet HTTP

Pour déterminer le caractère actuel d'un objet HTTP présent dans le cache, Content Gateway procède comme suit :

- Vérification de l'en-tête **Expires** ou **max-age**

  Certains objets HTTP contiennent des en-têtes **Expires** ou **max-age** qui définissent le délai pendant lequel l'objet peut être mis en cache. En comparant l'heure en cours à l'heure d'expiration, le proxy peut savoir si l'objet est récent ou non.
- Vérification des en-têtes **Last-Modified / Date**

  Lorsqu'un objet HTTP n'a pas d'en-tête **Expires** ni **max-age**, le proxy peut utiliser la formule suivante pour calculer la limite d'actualisation :

  ```
  freshness_limit =(date - dernière_modification) * 0.10
  ```

où *date* correspond à la date indiquée dans l'en-tête de réponse du serveur de l'objet, et *dernière_modification* à la date indiquée dans l'en-tête **Last-Modified**. En l'absence d'un en-tête **Last-Modified**, le proxy utilise la date à laquelle l'objet a été écrit dans le cache. Vous pouvez augmenter ou réduire la valeur de 0,10 (10 pour-cent). Voir *Modification du facteur de vieillissement associé au calcul de l'actualité des objets*, page 21.

La limite d'actualité calculée est liée aux limites minimale et maximale. Voir *Définition d'une limite d'actualité absolue*, page 22.

- Vérification de la limite d'actualité absolue

  Lorsque les objets HTTP n'ont pas d'en-tête **Expires** ou n'ont pas à la fois les en-têtes **Last-Modified** et **Date**, le proxy utilise une limite d'actualité maximale et minimale. Voir *Définition d'une limite d'actualité absolue*, page 22.

- Vérification des règles de revalidation dans le fichier **cache.config**

  Les règles de revalidation appliquent les limites d'actualité à des objets HTTP spécifiques. Vous pouvez par exemple définir les limites d'actualité des objets provenant de domaines ou d'adresses IP spécifiques, des objets associés à des URL contenant des expressions standard définies et des objets demandés par des clients particuliers. Voir *Fichier de configuration cache.config*, page 352.

Modification du facteur de vieillissement associé au calcul de l'actualité des objets

Lorsqu'un objet ne contient pas d'informations sur son expiration, Content Gateway peut utiliser les en-têtes **Last-Modified** et **Date** pour en estimer le caractère récent. Par défaut, le proxy stocke un objet pendant un délai correspondant à 10 % du temps écoulé depuis sa dernière modification. Vous pouvez augmenter ou réduire ce pourcentage.

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway.
2. Modifiez la variable suivante :

Variable	Description
proxy.config.http.cache.heuristic_lm_factor	Définissez le facteur de vieillissement associé aux calculs de l'actualité des objets. La valeur par défaut est 0,10 (10 pour-cent).

3. Enregistrez et fermez le fichier.
4. Pour appliquer vos modifications, exécutez la commande suivante dans le répertoire **bin** de Content Gateway :

```
content_line -x
```

Définition d'une limite d'actualité absolue

Certains objets ne présentent pas d'en-tête **Expires** ou n'ont pas à la fois les en-têtes **Last-Modified** et **Date**. Vous pouvez définir pendant combien de temps ces objets sont considérés comme récents dans le cache en spécifiant une limite d'actualité absolue. Une durée de vie plus longue implique que les objets sont conservés plus longtemps dans le cache. Le fait de récupérer les pages dans le cache plutôt que via le réseau peut améliorer les performances.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la zone **Minimum Heuristic Lifetime (Durée de vie heuristique minimale)** de la section **Freshness (Actualité)**, définissez le délai minimal pendant lequel les objets HTTP présents dans le cache et non associés à une date d'expiration peuvent être considérés comme récents avant d'être considérés comme périmés. La valeur par défaut est 3 600 secondes (1 heure).
3. Dans le champ **Maximum Heuristic Lifetime (Durée de vie heuristique maximale)**, définissez le délai maximal pendant lequel les objets HTTP présents dans le cache et non associés à une date d'expiration peuvent être considérés comme récents avant d'être considérés comme périmés. La valeur par défaut est 86 400 secondes (1 jour).
4. Cliquez sur **Appliquer**.

Définition des conditions d'en-tête

Pour garantir le caractère récent des objets présents dans le cache, configurez Content Gateway de telle sorte qu'il mette uniquement en cache les objets présentant des en-têtes spécifiques.

Avertissement

Par défaut, proxy met tous les objets en cache (y compris ceux sans en-tête). Websense vous conseille de ne modifier cette configuration par défaut que dans les cas de proxy spéciaux. Si vous configurez le proxy pour qu'il ne mette en cache que les objets HTTP présentant des en-têtes **Expires** ou **max-age**, le taux d'accès au cache sera fortement réduit. En effet, très peu d'objets présentent des informations d'expiration explicites.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la zone **Required Headers (En-têtes obligatoires)** de la section **Behavior (Comportement)**, sélectionnez l'une des options suivantes :
   - **An Explicit Lifetime Header (Un en-tête de durée de vie explicite)** pour ne mettre en cache que les objets HTTP présentant des en-têtes **Expires** ou **Cache-Control**
   - **An Last-Modified Header (Un en-tête de dernière modification)** pour ne mettre en cache que les objets HTTP présentant des en-têtes **Expires** ou **Last-Modified**

- **No Required Headers (Aucun en-tête obligatoire)** pour mettre en cache tous les objets HTTP (aucun en-tête spécifique n'est requis). Il s'agit là du paramètre par défaut.

3. Cliquez sur **Appliquer**.

En-têtes Cache-Control

Même lorsqu'un objet du cache est récent, certains clients ou serveurs peuvent présenter des contraintes qui les empêchent de le récupérer dans le cache. Un client peut par exemple demander à ce que l'objet ne provienne pas du cache ou, si oui, à ce qu'il ne soit pas resté dans le cache plus de 10 minutes.

Content Gateway base la possibilité de récupération d'un objet mis en cache sur les en-têtes **Cache-Control**. Les en-têtes **Cache-Control** peuvent à la fois apparaître dans les requêtes des clients et dans les réponses des serveurs.

Les en-têtes **Cache-Control** suivants affectent le mode de récupération des objets dans le cache :

- L'en-tête **no-cache**, envoyé par les clients, indique au proxy de ne récupérer *aucun* objet directement dans le cache, mais uniquement sur le serveur d'origine. Vous pouvez configurer le proxy pour qu'il ignore les en-têtes **no-cache** des clients (voir *Configuration du proxy pour qu'il ignore les en-têtes no-cache des clients*, page 30).
- L'en-tête **max-age**, envoyé par les serveurs, est comparé à l'âge de l'objet. Si l'age en question est plus récent que **max-age**, l'objet est récent et peut être récupéré.
- L'en-tête **min-fresh**, envoyé par les clients, est une *tolérance d'actualité acceptable*. Le client souhaite que l'objet soit au moins aussi récent. Lorsqu'un objet mis en cache ne reste pas ensuite récent pour cette durée au moins, il est revalidé.
- L'en-tête **max-stale**, envoyé par les clients, autorise le proxy à récupérer les objets périmés à condition qu'ils ne soient pas trop anciens. Certains navigateurs peuvent accepter de récupérer des objets légèrement périmés pour améliorer les performances, en particulier pendant les périodes de faible disponibilité d'Internet.

Le proxy applique les critères de possibilité de récupération de Cache-Control *après* les critères d'actualité des objets HTTP. Par exemple, lorsqu'un objet est considéré comme récent, mais que son âge dépasse celui indiqué dans `max-age`, il n'est pas récupéré.

Revalidation des objets HTTP

Lorsqu'un client demande un objet HTTP présent dans le cache mais périmé, Content Gateway valide à nouveau cet objet en interrogeant le serveur d'origine pour savoir si l'objet n'a pas été modifié. Cette revalidation entraîne l'un des résultats suivants :

- Lorsque l'objet est encore récent, le proxy en redéfinit la limite d'actualité et le récupère.
- Lorsqu'une nouvelle copie de l'objet est disponible, le proxy met le nouvel objet en cache (en remplaçant sa copie périmée) et l'envoie simultanément à l'utilisateur.
- Lorsque l'objet n'existe plus dans le serveur d'origine, le proxy ne récupère pas la copie mise en cache.
- Si le serveur d'origine ne répond pas à la demande de revalidation, le proxy n'effectue aucune validation, mais envoie à l'utilisateur l'objet périmé présent dans le cache.

Par défaut, le proxy revalide un objet HTTP demandé et présent dans le cache s'il estime que cet objet est périmé. Le proxy évalue le caractère récent de l'objet selon la procédure détaillée à la section *Actualité d'un objet HTTP*, page 20. Vous pouvez configurer la fréquence à laquelle le proxy doit revalider un objet HTTP.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la zone **When to Revalidate (Fréquence de revalidation)** de la section **Behavior (Comportement)**, sélectionnez :
   - **Never Revalidate (Ne jamais revalider)** pour ne jamais vérifier le caractère récent d'un objet HTTP auprès du serveur d'origine.
   - **Always Revalidate (Toujours revalider)** pour vérifier systématiquement le caractère récent d'un objet HTTP auprès du serveur d'origine.
   - **Revalidate if Heuristic Expiration (Revalider en cas d'expiration heuristique)** pour vérifier le caractère récent d'un objet HTTP auprès du serveur d'origine lorsque cet objet ne contient pas d'en-tête **Expires** ou **Cache-Control**. Content Gateway considère que tous les objets HTTP dépourvus d'en-têtes **Expires** ou **Cache-Control** sont périmés.
   - **Use Cache Directive or Heuristic (Utiliser les directives du cache ou les règles heuristiques)** pour vérifier le caractère récent d'un objet HTTP demandé auprès du serveur d'origine lorsque Content Gateway considère l'objet présent dans le cache comme périmé. Il s'agit là du paramètre par défaut.
3. Cliquez sur **Appliquer**.

> **Remarque**
>
> Vous pouvez également définir des règles de revalidation spécifiques dans le fichier **cache.config**. Voir *Fichier de configuration cache.config*, page 352.

Actualité d'un objet FTP

Les objets FTP ne contiennent pas d'informations d'horodatage ou de date et restent dans le cache en étant considérés comme récents pour la durée que vous définissez (de 15 minutes à 2 semaines), après quoi ils sont considérés comme périmés.

Les objets FTP peuvent être demandés par un client HTTP (par exemple un navigateur) ou un client FTP (tel que WS_FTP). Content Gateway met uniquement en cache les objets FTP demandés par des clients HTTP.

Objets FTP demandés par des clients HTTP

Vous pouvez définir la limite d'actualité absolue des objets FTP demandés par les clients HTTP (objets FTP sur HTTP).

> **Remarque**
> En plus de définir la limite d'actualité absolue de tous les objets FTP demandés par des clients HTTP, vous pouvez définir les règles d'actualité pour des objets FTP spécifiques dans le fichier **cache.config** (voir *Fichier de configuration cache.config*, page 352).

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la zone **FTP Document Lifetime (Durée de vie des documents FTP)** de la section **Freshness (Actualité)**, définissez la durée pendant laquelle les objets FTP demandés par des clients HTTP peuvent demeurer dans le cache et être considérés comme récents avant d'être considérés comme périmés. La valeur par défaut est 259 200 secondes (3 jours).
3. Cliquez sur **Appliquer**.

Planification des mises à jour du contenu du cache local

Pour encore améliorer les performances et être certain que les objets HTTP et FTP (demandés par des clients HTTP) présents dans le cache sont récents, vous pouvez utiliser l'option Scheduled Update (Mise à jour planifiée) pour configurer le proxy de sorte qu'il ne charge des objets spécifiques dans le cache qu'aux moments programmés.

Pour utiliser l'option Scheduled Update (Mise à jour planifiée) :

- Définissez la liste des URL contenant les objets dont la mise à jour doit être planifiée, l'heure à laquelle la mise à jour doit être effectuée et la profondeur de récursion de l'URL.
- Activez l'option Scheduled Update (Mise à jour planifiée) et configurez les paramètres facultatifs de nouvelle tentative.

Pour plus d'informations, consultez *Configuration de l'option Scheduled Update (Mise à jour planifiée)*, page 26.

Content Gateway utilise les informations que vous définissez pour identifier les URL dont il est responsable et, pour chaque URL, déduit éventuellement toutes les URL récursives. Il génère ensuite une seule liste d'URL. À l'aide de cette liste, le proxy déclenche une

opération HTTP **GET** pour chaque URL n'ayant pas fait l'objet d'un accès, en s'assurant de respecter à tout moment les limites de simultanéité HTTP définies par l'utilisateur.

> **Remarque**
> Le système enregistrant la fin de toutes les opérations HTTP **GET** dans un journal, vous pouvez surveiller les performances de cette fonction.

L'option Force Immediate Update (Imposer une mise à jour immédiate) vous permet d'actualiser les URL sans attendre l'heure de mise à jour définie. Vous pouvez l'utiliser pour tester votre configuration des mises à jour planifiées. Voir *Mise à jour immédiate imposée*, page 27.

Configuration de l'option Scheduled Update (Mise à jour planifiée)

1. Sélectionnez **Configurer > Protocoles > HTTP Scheduled Update (Mise à jour planifiée des URL HTTP) > Update URLs (Mettre à jour les URL)**.
2. Dans la zone **Scheduled Object Update (Mise à jour planifiée des objets)**, cliquez sur **Edit File (Modifier le fichier)** afin d'ouvrir l'éditeur de fichier de configuration pour le fichier **update.config**.
3. Entrez les informations suivantes :
   - Dans le champ **URL**, saisissez l'URL dont vous souhaitez planifier la mise à jour.
   - *Facultatif*. Dans le champ **Request Headers (En-têtes des requêtes)**, entrez la liste séparée par des points-virgules des en-têtes transmis dans chaque requête **GET**. Vous pouvez définir tout en-tête de requête respectant les spécifications du protocole HTTP.
   - Dans le champ **Offset Hour (Heure de décalage)**, saisissez l'heure de base à partir de laquelle les périodes de mises à jour doivent découler. Vous pouvez définir une valeur de la plage 00 à 23.
   - Dans le champ **Intervalle**, saisissez l'intervalle (en secondes) d'exécution des mises à jour, à partir de l'heure de décalage.
   - Dans le champ **Recursion Depth (Profondeur de récursion)**, saisissez la profondeur à laquelle les URL référencées sont mises à jour de façon récursive, à partir de l'URL donnée. Par exemple, une profondeur récursive de 1 met à jour l'URL donnée, ainsi que toutes les URL immédiatement référencées par les liens de l'URL d'origine.
4. Cliquez sur **Ajouter**, puis sur **Appliquer**.
5. Cliquez sur **Fermer**.
6. Ouvrez l'onglet **Général**.
7. Activez **Scheduled Update (Mise à jour planifiée)**.
8. Dans le champ **Maximum Concurrent Updates (Mises à jour simultanées maximales)**, saisissez le nombre maximal de requêtes de mises à jour simultanées autorisées à un moment donné de sorte que le processus de mise à jour planifiée ne surcharge pas l'hôte. La valeur par défaut est 100.

9. Dans le champ **Count (Nombre)** de la section **Retry on Update Error (Nouvelle tentative en cas d'erreur de mise à jour)**, saisissez le nombre de nouvelles tentatives de mise à jour d'une URL à réeffectuer en cas d'échec. La valeur par défaut est 10.
10. Dans le champ **Intervalle** de la section **Retry on Update Error (Nouvelle tentative en cas d'erreur de mise à jour)**, saisissez le délai (en secondes) devant s'écouler après chaque nouvelle tentative de mise à jour d'une URL en cas d'échec. La valeur par défaut est 2.
11. Cliquez sur **Appliquer**.

Mise à jour immédiate imposée

L'option Force Immediate Update (Imposer une mise à jour immédiate) vous permet de vérifier immédiatement les URL répertoriées dans le fichier **update.config**. Cette option ignore l'intervalle et l'heure de décalage définis dans le fichier **update.config** et actualise les URL de la liste.

Important

Lorsque vous activez l'option Force Immediate Update (Imposer une mise à jour immédiate), le proxy met continuellement à jour les URL spécifiées dans le fichier **update.config** jusqu'à ce que cette option soit désactivée.

1. Sélectionnez **Configurer > Protocoles > HTTP Scheduled Update (Mise à jour planifiée des URL HTTP) > Général**.
2. Vérifiez que l'option **Scheduled Update (Mise à jour planifiée)** est activée.
3. Ouvrez l'onglet **Update URLs (Mettre les URL à jour)**.
4. Activez l'option **Force Immediate Update (Imposer une mise à jour immédiate)**.
5. Cliquez sur **Appliquer**.

Épinglage du contenu dans le cache

L'option d'épinglage du cache configure Content Gateway de sorte qu'il conserve certains objets HTTP (et les objets FTP demandés par des clients HTTP) dans le cache pendant le délai indiqué. Servez-vous de cette option pour être certain que les objets les plus populaires restent dans le cache et que le proxy ne retire pas d'importants objets du cache.

Remarque

Le proxy examine les en-têtes Cache-Control et n'épingle un objet dans le cache que s'il peut être mis en cache.

Pour utiliser l'option d'épinglage dans le cache, procédez comme suit :

- Définissez les règles d'épinglage du cache dans le fichier **cache.config**. Voir *Définition des règles d'épinglage du cache*, page 28.
- Activez l'option d'épinglage du cache. Voir *Activation de l'épinglage du cache*, page 28.

Définition des règles d'épinglage du cache

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Cliquez sur l'option **Edit File (Modifier le fichier)** située en bas de la page pour afficher l'éditeur de fichier de configuration pour le fichier **cache.config**.
3. Saisissez les informations suivantes dans les champs fournis :
   - Dans la liste déroulante **Rule Type (Type de règle)**, sélectionnez **pin-in-cache (Épingler dans le cache)**.
   - Dans la liste déroulante **Primary Destination Type (Type de destination principale)**, sélectionnez **url_regex**.
   - Dans le champ **Primary Destination Value (Valeur de destination principale)**, spécifiez l'URL à épingler dans le cache.
   - Dans le champ **Période**, indiquez la durée pendant laquelle le proxy doit épingler cet objet dans le cache.

     Vous pouvez par ailleurs ajouter des spécificateurs secondaires (par exemple un **Préfixe** et un **Suffixe**) à la règle. L'ensemble des champs sont décris à la section *HTTP*, page 277.
4. Cliquez sur **Ajouter** pour ajouter la règle dans la liste, puis sur **Appliquer**.
5. Cliquez sur **Fermer**.

Activation de l'épinglage du cache

1. Dans **Configurer > Subsystems (Sous-systèmes) > Cache > Général**, activez **Allow Pinning (Autoriser l'épinglage)**.
2. Cliquez sur **Appliquer**.

Mettre en cache ou non ?

À réception d'une demande d'objet Web non présent dans le cache, Content Gateway récupère l'objet en question sur le serveur d'origine et l'envoie au client. Dans le même temps, le proxy vérifie que cet objet peut être mis en cache avant de le stocker dans son cache pour pouvoir répondre aux futures demandes.

Pour déterminer si un objet peut être mis en cache, Content Gateway se base sur son protocole :

- Pour les objets HTTP, le proxy respecte les directives de mise en cache des clients et des serveurs d'origine. Vous pouvez par ailleurs configurer le proxy pour qu'il

ne mette pas en cache certains objets. Voir *Mise en cache des objets HTTP*, page 29.

- Pour les objets FTP, le proxy respecte les directives de mise en cache que vous définissez via les fichiers et les options de configuration. Voir *Mise en cache des objets FTP*, page 37.

Mise en cache des objets HTTP

Content Gateway respecte les directives de mise en cache des clients et des serveurs d'origine, de même que celles que vous définissez via les options et les fichiers de configuration.

Cette section détaille les sujets suivants :

- *Directives des clients*, page 29
- *Directives des serveurs d'origine*, page 30
- *Directives de configuration*, page 33

Directives des clients

Par défaut, Content Gateway ne met *pas* en cache les objets présentant les en-têtes de requête suivants :

- **Cache-Control: no-store**
- **Cache-Control: no-cache**

> **Remarque**
> Vous pouvez configurer le proxy pour qu'il ignore l'en-tête **Cache-Control: no-cache**. Voir *Configuration du proxy pour qu'il ignore les en-têtes no-cache des clients*, page 30.

- **Cookie :** (pour les objets texte)

  Par défaut, le proxy met en cache les objets envoyés en réponse aux requêtes contenant des cookies, sauf si l'objet correspond à du texte. Vous pouvez configurer le proxy pour qu'il ne mette *pas* en cache le contenu avec cookies quel qu'en soit le type, pour qu'il mette en cache tout le contenu avec cookies ou pour qu'il mette uniquement en cache le contenu avec cookies de type image. Voir *Mise en cache des objets avec cookies*, page 34.

- **Authorization :**

> **Remarque**
> Les objets FTP demandés par des clients HTTP peuvent également contenir des en-têtes **Cache-Control: no-store, Cache-Control: no-cache** ou **Authorization**. Lorsque l'objet FTP demandé par un client HTTP contient un tel en-tête, le proxy ne le met pas en cache, sauf lorsqu'il a été explicitement configuré pour le faire.

Configuration du proxy pour qu'il ignore les en-têtes no-cache des clients

Par défaut, Content Gateway respecte les directives **Cache Control:no-cache** des clients. Lorsque l'objet demandé contient un en-tête **no-cache**, le proxy transmet la requête au serveur d'origine, y compris lorsque le cache en contient une copie récente.

Vous pouvez configurer le proxy pour qu'il ignore les directives **no-cache** des clients. Dans ce cas, le proxy ignore les en-têtes **no-cache** présents dans les requêtes des clients et utilise l'objet stocké dans son cache.

Important
Le comportement par défaut, qui consiste à respecter les directives **no-cache**, convient dans la plupart des cas. Configurez Content Gateway pour qu'il ignore les directives **no-cache** uniquement si vous maîtrisez HTTP 1.1.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la section **Behavior (Comportement)**, activez l'option **Ignore « no-cache » in Client Requests (Ignorer « no-cache » dans les requêtes des clients)**.
3. Cliquez sur **Appliquer**.

Remarque
Certaines versions de Microsoft Internet Explorer ne demandent pas un nouveau chargement du cache à partir des caches transparents lorsque l'utilisateur clique sur le bouton **Actualiser**. Il est ainsi possible que le contenu ne soit pas directement récupéré auprès du serveur d'origine. Vous pouvez configurer Content Gateway pour qu'il traite les requêtes Microsoft Internet Explorer de façon plus prudente, en proposant un contenu plus récent, quitte à envoyer moins de documents à partir du cache. Vous pouvez configurer le proxy pour qu'il ajoute des en-têtes **no-cache** dans les requêtes provenant de Microsoft Internet Explorer dans Content Gateway Manager (section **Behavior (Comportement)** onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**).

Directives des serveurs d'origine

Par défaut, Content Gateway ne met pas en cache les objets présentant les en-têtes de réponse suivants :

- **Cache-Control: no-store**
- **Cache-Control: private**

- **WWW-Authenticate:**

> **Remarque**
> Vous pouvez configurer le proxy pour qu'il ignore les en-têtes **WWW-Authenticate**. Voir *Configuration du proxy pour qu'il ignore les en-têtes WWW-Authenticate*, page 33.

- **Set-Cookie :**
- **Cache-Control: no-cache**

> **Remarque**
> Vous pouvez configurer le proxy pour qu'il ignore les en-têtes **no-cache**. Voir *Configuration du proxy pour qu'il ignore les en-têtes no-cache des serveurs*, page 31.

- **En-tête Expires:** présentant une valeur 0 (zéro) ou une date antérieure

Configuration du proxy pour qu'il ignore les en-têtes no-cache des serveurs

Par défaut, Content Gateway respecte les directives **Cache-Control:no-cache**. Les réponses provenant des serveurs d'origine et contenant un en-tête **no-cache** ne sont pas stockées dans le cache et toutes les précédentes copies de l'objet présent dans le cache sont supprimées.

> **Important**
> Si vous configurez le proxy pour qu'il ignore les en-têtes **no-cache**, il ignorera également les en-têtes **no-store**.

> **Important**
> Le comportement par défaut, qui consiste à respecter les directives **no-cache**, convient dans la plupart des cas. Configurez le proxy pour qu'il ignore les en-têtes **no-cache** des serveurs d'origine uniquement si vous maîtrisez HTTP 1.1.

Vous pouvez configurer le proxy pour qu'il ignore les en-têtes **no-cache** des serveurs d'origine.

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway.

2. Modifiez la variable suivante :

Variable	Description
proxy.config.http.cache.ignore_server_no_cache	Définissez cette variable sur 1 pour ignorer les directives des serveurs demandant de contourner le cache.

3. Enregistrez et fermez le fichier.
4. Pour appliquer vos modifications, exécutez la commande suivante dans le répertoire **bin** de Content Gateway :

```
content_line -x
```

Configuration du proxy pour qu'il ignore les en-têtes WWW-Authenticate

Par défaut, Content Gateway ne met pas en cache les objets qui contiennent des en-têtes de réponse **WWW-Authenticate**. L'en-tête **WWW-Authenticate** contient des paramètres d'authentification que le client utilise lorsqu'il prépare la réponse d'authentification pour un serveur d'origine.

Important

Le comportement par défaut, qui consiste à ne pas mettre en cache les objets contenant des en-têtes **WWW-Authenticate**, convient dans la plupart des cas. Configurez le proxy pour qu'il ignore les en-têtes **WWW-Authenticate** des serveurs uniquement si vous maîtrisez HTTP 1.1.

Vous pouvez configurer le proxy pour qu'il ignore les en-têtes **WWW-Authenticate** des serveurs d'origine, auquel cas les objets contenant des en-têtes **WWW-Authenticate** sont stockés dans le cache en vue des requêtes futures.

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway.
2. Modifiez la variable suivante :

Variable	Description
proxy.config.http.cache.ignore_ authentication	Définissez cette variable sur 1 pour mettre en cache les objets contenant des en-têtes **WWW-Authenticate**.

3. Enregistrez et fermez le fichier.
4. Pour appliquer vos modifications, exécutez la commande suivante dans le répertoire **bin** de Content Gateway :

```
content_line -x
```

Directives de configuration

Outre les directives des clients et des serveurs d'origine, Content Gateway respecte les directives que vous définissez via les options et les fichiers de configuration.

Vous pouvez configurer le proxy pour :

- Qu'il ne mette *pas* en cache les objets HTTP. Voir *Désactivation de la mise en cache des objets HTTP*, page 34.
- Qu'il mette en tâche le contenu dynamique (objets dont les URL contiennent un point d'interrogation (?), un point-virgule (;) ou cgi, ou qui se terminent par .asp). Voir *Mise en cache du contenu dynamique*, page 34.
- Qu'il mette en cachent les objets envoyés en réponse à l'en-tête **Cookie:**. Voir *Mise en cache des objets avec cookies*, page 34.
- Qu'il respecte les règles définies dans le fichier **cache.config** et consistant à ne jamais effectuer de mise en cache. Voir *Fichier de configuration cache.config*, page 352.

Désactivation de la mise en cache des objets HTTP

Par défaut, Content Gateway met en cache tous les objets HTTP, à l'exception de ceux pour lesquels vous avez défini des règles de non mise en cache dans le fichier **cache.config**. Vous pouvez désactiver la mise en cache des objets HTTP de sorte que tous ces objets soient récupérés sur le serveur d'origine et ne soient jamais mis en cache.

1. Sélectionnez **Configurer** > **Protocoles** > **HTTP > Cacheability (Capacités de mise en cache)**.
2. Désactivez l'option **HTTP Caching (Mise en cache HTTP)**.
3. Cliquez sur **Appliquer**.

Mise en cache du contenu dynamique

Une URL est considérée comme dynamique lorsqu'elle contient un point d'interrogation (?), un point-virgule (;) ou cgi, ou lorsqu'elle se termine par .asp. Par défaut, Content Gateway ne met *pas* en cache le contenu dynamique. Vous pouvez toutefois configurer le proxy pour qu'il mette ce contenu en cache.

Avertissement

Il est recommandé de ne configurer le proxy pour qu'il mette en cache le contenu dynamique que dans des cas particuliers.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la section **Dynamic Caching (Mise en cache du contenu dynamique)**, activez l'option **Caching Documents with Dynamic URLs (Mise en cache des documents présentant des URL dynamiques)**.
3. Cliquez sur **Appliquer**.

Mise en cache des objets avec cookies

Par défaut, Content Gateway met en cache les objets envoyés en réponse aux requêtes contenant des cookies, *sauf* si l'objet correspond à du texte. Le proxy ne met pas en cache le contenu texte avec cookie, car les en-têtes des objets sont stockés, de même que l'objet, et les valeurs d'en-tête de cookie personnalisées pourraient être enregistrées en même temps que l'objet.

Dans le cas des objets non texte, il est peu probable que des en-têtes personnalisés soient envoyés ou utilisés.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la zone **Caching Response to Cookies (Mise en cache des réponses dans des cookies)** de la section **Dynamic Caching (Mise en cache du contenu dynamique)**, sélectionnez une option de mise en cache :
   - Sélectionnez **Cache All but Text (Tout mettre en cache sauf le texte)** pour mettre en cache l'ensemble du contenu avec cookie, sauf celui correspondant à du texte (il s'agit là du paramètre par défaut).

- Sélectionnez **Cache Only Image Types (Mettre en cache les types Image uniquement)** pour ne mettre en cache que le contenu avec cookies correspondant à une image.
- Sélectionnez **Cache Any Content Type (Mettre en cache tous les types de contenu)** pour mettre en cache le contenu avec cookies quel que soit son type.
- Sélectionnez **No Cache on Cookies (Aucun cache pour les cookies)** pour ne *pas* mettre en cache le contenu avec cookies quel que soit son type.

3. Cliquez sur **Appliquer**.

Mise en cache obligatoire des objets

Vous pouvez obliger Content Gateway à mettre en cache des URL spécifiques (y compris des URL dynamiques) pendant une durée définie, quels que soient les en-têtes de réponse **Cache-Control**.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Cliquez sur l'option **Edit File (Modifier le fichier)** située en bas de la page pour afficher l'éditeur de fichier de configuration pour le fichier **cache.config**.
3. Saisissez les informations suivantes dans les champs fournis :
   - Dans la liste déroulante **Rule Type (Type de règle)**, sélectionnez **ttl-in-cache**.
   - Dans la liste déroulante **Primary Destination Type (Type de destination principale)**, sélectionnez **url_regex**.
   - Dans le champ **Primary Destination Value (Valeur de destination principale)**, spécifiez l'URL à mettre obligatoirement dans le cache.
   - Dans le champ **Période**, indiquez la durée pendant laquelle le proxy doit récupérer cette URL dans le cache.

     Vous pouvez par ailleurs ajouter des spécificateurs secondaires (par exemple un **Préfixe** et un **Suffixe**) à la règle. L'ensemble des champs sont décris à la section *HTTP*, page 277.
4. Cliquez sur **Ajouter**, puis sur **Appliquer**.
5. Cliquez sur **Fermer**.

Mise en cache des alternatives HTTP

Certains serveurs d'origine répondent aux requêtes correspondant à la même URL par divers objets. Le contenu de ces objets peut varier, selon si le serveur fournit un contenu différent selon les langues, cible les différents navigateurs par des styles de présentation différents ou fournit des formats de document distincts (HTML, PDF). Les différentes versions d'un même objet sont appelées *alternatives* et sont mises en cache par Content Gateway en fonction des en-têtes de réponse **Vary**.

Configuration de la mise en cache des alternatives par Content Gateway

Vous pouvez définir d'autres en-têtes de requête et de réponse pour des types de contenu spécifiques que le proxy identifiera comme des alternatives lors de la mise en cache.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la section **Vary Based on Content Type (Varie en fonction du type de contenu)**, cliquez sur **Enabled (Activé)** pour mettre en cache les versions alternatives des documents HTTP qui ne contiennent pas l'en-tête **Vary**.
3. Définissez les autres en-têtes de requête et de réponse que le serveur proxy doit identifier :
   - Dans le champ **Vary by Default on Text (Varie par défaut pour le texte)**, entrez le champ d'en-tête HTTP en fonction duquel la variation doit être effectuée lorsque la requête correspond à du texte (par exemple, un document HTML).
   - Dans le champ **Vary by Default on Images (Varie par défaut pour les images)**, entrez le champ d'en-tête HTTP en fonction duquel la variation doit être effectuée lorsque la requête correspond à des images (par exemple, un fichier **.gif**).
   - Dans le champ **Vary by Default on Other Document Types (Varie par défaut pour les autres types de documents)**, entrez le champ d'en-tête HTTP en fonction duquel la variation doit être effectuée lorsque la requête correspond à autre chose qu'à du texte ou des images.

   Remarque

   Si vous spécifiez que la variation doit être effectuée en fonction du champ d'en-tête **Cookie** dans les champs ci-dessus, assurez-vous que l'option appropriée soit activée dans la zone **Caching Response to Cookies (Mise en cache des réponses dans des cookies)** de la section **Dynamic Caching (Mise en cache du contenu dynamique)**. Par exemple, si vous activez l'option **Cache Only Image Types (Mettre en cache les types Image uniquement)** de la zone **Caching Response to Cookies (Mise en cache des réponses dans des cookies)** et que vous activez l'option **Vary by Default on Text (Varie par défaut pour le texte)** de la section **Vary Based on Content Type (Varie en fonction du type de contenu)**, les alternatives par cookie ne s'appliqueront pas au texte.

4. Cliquez sur **Appliquer**.

Limitation du nombre d'alternatives pour un objet

Vous pouvez limiter le nombre d'alternatives mises en cache par objet par Content Gateway. Le nombre d'alternatives par défaut est 3.

> **Remarque**
> Un plus grand nombre d'alternatives peut affecter les performances du proxy, car toutes les alternatives ont la même URL. Bien que Content Gateway puisse rapidement rechercher l'URL dans l'index, il doit analyser en séquence les différentes alternatives disponibles dans le magasin d'objets.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans le champ **Maximum Alternates (Nombre maximal d'alternatives)**, entrez le nombre maximal de versions alternatives d'un objet que le proxy doit mettre en cache. La valeur par défaut est 3.
3. Cliquez sur **Appliquer**.

Mise en cache des objets FTP

Les objets FTP peuvent être demandés par un client HTTP (par exemple un navigateur) ou un client FTP (tel que WS_FTP).

Dans le cas des objets FTP demandés par des clients HTTP (FTP sur HTTP), appliquez la configuration suivante pour déterminer ce que le proxy stocke dans le cache :

- Désactivez la mise en cache FTP sur HTTP afin que le proxy ne mettent pas en cache les objets FTP demandés par des clients HTTP (voir *Désactivation de la mise en cache FTP sur HTTP*, page 38).
- Définissez les règles de non mise en cache dans le fichier **cache.config** (voir *Fichier de configuration cache.config*, page 352).
- Configurez le proxy pour qu'il ignore les en-têtes **Cache-Control: no-store** ou **Cache-Control: no-cache** (voir *Configuration du proxy pour qu'il ignore les en-têtes no-cache des clients*, page 30).

La mise en cache des objets FTP demandés par des clients FTP n'est pas prise en charge.

Désactivation de la mise en cache FTP sur HTTP

Vous pouvez configurer Content Gateway pour qu'il ne mette pas en cache les objets FTP demandés par des clients HTTP en désactivant l'option FTP sur HTTP. Le proxy traite les requêtes en les transmettant au serveur FTP, mais ne met pas en cache les objets demandés.

1. Ouvrez l'onglet **Configurer > Protocoles > HTTP > Cacheability (Capacités de mise en cache)**.
2. Dans la section **Caching (Mise en cache)**, désactivez l'option **FTP over HTTP Caching (Mise en cache FTP sur HTTP)**.
3. Cliquez sur **Appliquer**.

4 Proxy explicite

Si les requêtes Internet ne sont pas acheminées de manière transparente vers Content Gateway via un commutateur ou un routeur de Niveau 4 (voir *Proxy transparent et module ARM*, page 47), le trafic doit être **explicitement** acheminé vers Content Gateway en configurant le navigateur Web des clients. (On appelle parfois cette opération un *déploiement de proxy explicite*.)

Les clients peuvent configurer leurs navigateurs Web de l'une des 3 manières suivantes :

- En configurant leur navigateur pour qu'il envoie les requêtes directement au proxy. Voir *Configuration manuelle du navigateur*, page 39.
- En configurant leur navigateur pour qu'il télécharge les instructions de configuration du proxy à partir d'un fichier PAC (Proxy Auto-Config). Voir *Utilisation d'un fichier PAC*, page 40.
- En utilisant le protocole WPAD (Web Proxy Auto-Discovery Protocol) pour télécharger les instructions de configuration du proxy à partir d'un serveur WPAD (pour Microsoft Internet Explorer uniquement). Voir *Utilisation du protocole WPAD*, page 42.

En outre, si Content Gateway est configuré pour envoyer le trafic FTP par proxy, les clients FTP, tels que FileZilla ou WS_FTP, doivent être configurés pour envoyer explicitement les requêtes au proxy. Voir *Configuration des clients FTP dans un environnement de proxy explicite*, page 43.

Configuration manuelle du navigateur

Pour configurer un navigateur de sorte qu'il envoie les requêtes à Content Gateway, les clients doivent fournir les informations suivantes pour chacun des protocoles pour lesquels le proxy doit desservir leurs navigateurs :

- Nom d'hôte ou adresse IP du proxy

> **Important**
> Si l'Authentification Windows intégrée est configurée pour l'authentification des utilisateurs, vous devez utiliser le nom de domaine qualifié complet. Si vous indiquez une adresse IP, l'authentification échouera. Voir *Authentification Windows intégrée*, page 179.

- Port du serveur proxy. Le numéro de port par défaut du serveur proxy de Content Gateway est 8080.

> **Important**
> Ne définissez pas l'adresse IP du proxy de Content Gateway sous forme d'adresse IP virtuelle.
>
> Bien que Content Gateway Manager n'interdise pas la saisie d'une adresse IP virtuelle, le proxy ne fonctionne pas correctement avec ce type d'adresses.

De plus, les clients peuvent indiquer de ne pas utiliser le proxy pour certains sites. Les requêtes concernant ces sites sont acheminées directement au serveur d'origine.

Pour Microsoft Internet Explorer version 7.0 et supérieur, les paramètres de configuration du proxy se trouvent dans **Outils > Options Internet > Connexions > Paramètres réseau**. Par défaut, Microsoft Internet Explorer définit tous les protocoles sur le même serveur proxy. Pour configurer chaque protocole séparément, cliquez sur **Avancé** dans la section **Paramètres réseau**. Pour obtenir des instructions complètes sur la configuration du proxy, consultez la documentation de votre navigateur.

Pour Mozilla Firefox 4.0 et ultérieur, les paramètres de configuration du proxy se trouvent dans **Outils > Options > Avancé > Réseau > Paramètres > Paramètres de connexion > Configuration manuelle du proxy**. Par défaut, vous devez configurer chaque protocole séparément. Toutefois, vous pouvez définir tous les protocoles sur le même serveur proxy en cochant la case **Utiliser ce serveur proxy pour tous les protocoles**.

Nous n'avez pas besoin de définir les options de configuration au niveau du proxy pour accepter les requêtes des navigateurs configurés manuellement.

Utilisation d'un fichier PAC

Le fichier PAC est une définition des fonctions JavaScript que le navigateur appelle pour savoir comment traiter les requêtes. Dans les paramètres de leur navigateur, les clients doivent spécifier l'URL qui permet de charger le fichier PAC.

Vous pouvez stocker un fichier PAC dans le proxy et fournir l'URL de ce fichier à vos clients. Si vous disposez d'un fichier **proxy.pac**, copiez-le dans le répertoire **config** de Content Gateway.

> **Remarque**
> Le fichier PAC peut résider dans tout serveur de votre réseau.
>
> Si vous utilisez SSL Manager, consultez la section *Exécution en mode proxy explicite*, page 131, pour plus d'informations sur l'utilisation d'un fichier PAC avec du trafic HTTPS.

1. Si vous avez déjà un fichier **wpad.dat**, remplacez le fichier **wpad.dat** situé dans le répertoire **config** de Content Gateway par votre fichier existant.

2. Naviguez jusqu'à l'onglet **Configurer** > **Content Routing (Acheminement du contenu)** > **Browser Auto-Config (Auto-configuration du navigateur) > PAC**.
3. Dans le champ **Auto-Configuration Port (Port d'auto-configuration)**, indiquez le numéro du port utilisé par Content Gateway pour fournir le fichier PAC. Le port par défaut est le 8083.
4. Le volet Paramètres PAC affiche le fichier **proxy.pac** :
   - Si vous avez copié un fichier PAC existant dans le répertoire **config** de Content Gateway, le fichier **proxy.pac** contient les paramètres de configuration de votre proxy. Vérifiez ces paramètres et procédez à toute modification nécessaire.
   - Si vous n'avez pas copié un fichier PAC existant dans le répertoire **config** de Content Gateway, le volet Paramètres PAC est vide. Entrez le script qui fournit les paramètres de configuration de votre serveur proxy. Vous trouverez un exemple de script à la section *Exemple de fichier PAC*, page 41. Consultez également l'article intitulé « PAC File Best Practices » (Meilleures pratiques d'utilisation d'un fichier PAC) dans la Bibliothèque technique de Websense.
5. Cliquez sur **Appliquer**.
6. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.
7. Informez vos utilisateurs qu'ils doivent configurer leurs navigateurs de sorte qu'ils pointent vers ce fichier PAC.

   Par exemple, si le fichier PAC est stocké dans le serveur proxy avec le nom d'hôte **proxy1** et que Content Gateway utilise le port par défaut 8083 pour fournir ce fichier, les utilisateurs doivent spécifier l'URL suivante dans les paramètres de configuration du proxy :

   ```
   http://proxy1.entreprise.com:8083/proxy.pac
   ```

Les procédures qui permettent de spécifier l'emplacement du fichier PAC varient d'un navigateur à l'autre. Par exemple, pour Microsoft Internet Explorer, vous définissez l'emplacement du fichier PAC dans le champ **Utiliser un script de configuration automatique** sous **Outils > Options Internet > Connexions > Paramètres réseau**. Pour Mozilla Firefox, les paramètres de configuration du proxy se trouvent dans **Outils > Options > Avancé > Réseau > Paramètres > Paramètres de connexion > Adresse de configuration automatique du proxy**. Consultez la documentation de votre navigateur pour obtenir plus de détails.

Exemple de fichier PAC

L'exemple de fichier PAC suivant indique aux navigateurs de se connecter directement à tous les hôtes sans nom de domaine complet et à tous les hôtes du domaine local. Toutes les autres requêtes sont dirigées vers le serveur proxy appelé **myproxy.entreprise.com**.

```
function FindProxyForURL(url, host)
{
if (isPlainHostName(host) || dnsDomainIs(host,
".entreprise.com"))
return "DIRECT";
else
return "PROXY myproxy.entreprise.com:8080; DIRECT";
}
```

Utilisation du protocole WPAD

Le protocole WPAD permet à Internet Explorer version 7 et ultérieure de détecter automatiquement le serveur qui lui fournira les paramètres de configuration du serveur proxy. Les clients n'ont pas besoin de configurer leurs navigateurs pour envoyer les requêtes à un serveur proxy : un seul serveur fournit les paramètres à tous les clients du réseau.

> **Remarque**
> WPAD est incompatible avec les déploiements de proxy transparents.

Lorsqu'un navigateur Internet Explorer version 7 ou ultérieur démarre, il recherche un serveur WPAD qui lui fournira les paramètres de configuration du serveur proxy. II ajoute le nom d'hôte WPAD au début du nom de domaine complet actuel. Par exemple, un client de la société **x.y.entreprise.com** recherche un serveur WPAD à l'adresse **wpad.x.y.entreprise.com**. Si cette recherche échoue, le navigateur retire le domaine le plus bas et recommence la recherche ; par exemple, il essaie avec **wpad.y.entreprise.com**. Le navigateur cesse ses recherches dès qu'il détecte un serveur WPAD ou lorsqu'il atteint le domaine de troisième niveau, **wpad.entreprise.com**. L'algorithme s'arrête au troisième niveau afin que le navigateur ne recherche pas à l'extérieur du réseau actuel.

> **Remarque**
> Par défaut, Microsoft Internet Explorer version 7 et ultérieur est défini pour détecter automatiquement les serveurs WPAD. Toutefois, les utilisateurs peuvent désactiver ce paramètre.

Vous pouvez configurer Content Gateway pour qu'il joue le rôle de serveur WPAD :

1. Si vous avez déjà un fichier **wpad.dat**, remplacez le fichier **wpad.dat** situé dans le répertoire **config** de Content Gateway par votre fichier existant.
2. Connectez-vous à Content Gateway Manager et naviguez jusqu'à **Configurer** > **Content Routing (Acheminement du contenu)** > **Browser Auto-Config (Auto-configuration du navigateur) > WPAD** pour afficher le fichier **wpad.dat**.
3. Le volet Paramètres WPAD affiche le fichier **wpad.dat** :
   - Si vous avez copié un fichier **wpad.dat** existant dans le répertoire **config** de Content Gateway, ce fichier contient les paramètres de configuration de votre proxy. Vérifiez ces paramètres et procédez à toute modification nécessaire.
   - Si vous n'avez pas copié de fichier **wpad.dat** existant dans le répertoire **config** de Content Gateway (/opt/WCG/config), le volet Paramètres WPAD est vide. Entrez un script qui fournira les paramètres de configuration de votre serveur proxy. Vous trouverez un exemple de script à la section *Exemple de fichier PAC*, page 41 (tout fichier **wpad.dat** peut contenir le même script que le fichier **proxy.pac**).
4. Cliquez sur **Appliquer**.
5. Naviguez jusqu'à **Configurer** > **Networking (Mise en réseau) > ARM**.

6. Dans la section **Network Address Translation (Traduction d'adresses réseau) (NAT)**, cliquez sur **Edit File (Modifier le fichier)** pour ajouter une règle spéciale de redéfinition des correspondances au fichier **ipnat.conf**.
7. Entrez les informations dans les champs fournis, puis cliquez sur **Ajouter** :
   - Dans le champ **Interface Ethernet**, entrez l'interface réseau qui reçoit les requêtes WPAD des navigateurs (par exemple hme0 ou eth0).
   - Dans la liste déroulante **Type de connexion**, sélectionnez **tcp**.
   - Dans le champ **Adresse IP de destination**, entrez l'adresse IP du serveur Content Gateway qui sera convertie en nom du serveur WPAD par les serveurs de noms locaux, suivi de /32. Par exemple : 123.456.7.8/32.
   - Dans le champ **Port de destination**, entrez **80**.
   - Dans le champ **Adresse IP de destination redirigée**, entrez la même adresse IP que celle saisie dans le champ **Adresse IP de destination**, mais sans /32.
   - Dans le champ **Port de destination redirigé**, entrez **8083**.
8. Cliquez sur **Ajouter**.
9. Utilisez les touches fléchées sur la gauche pour placer cette nouvelle règle à la première ligne du fichier.
10. Cliquez sur **Appliquer**, puis sur **Fermer**.
11. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Configuration des clients FTP dans un environnement de proxy explicite

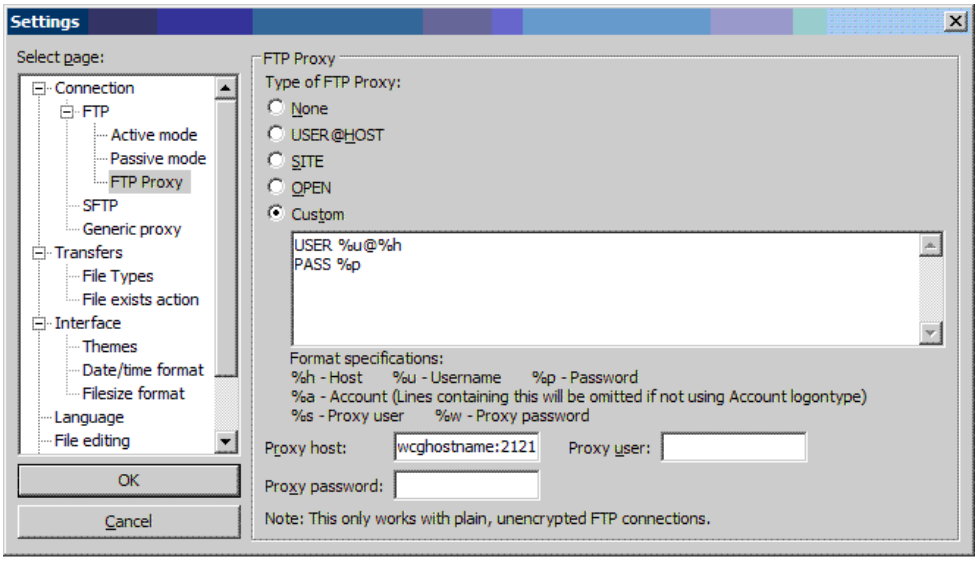
Lorsque Content Gateway est configuré pour envoyer le trafic FTP par proxy (voir *FTP*, page 288), les clients FTP, tels que FileZilla ou WS_FTP, doivent être configurés pour envoyer les requêtes au proxy. Après cette configuration, l'utilisateur travaille avec son client FTP comme s'il n'y avait pas de proxy.

Pour se connecter à un serveur FTP, 4 éléments d'informations sont généralement nécessaires. Ces éléments sont répartis comme suit :

De :	À :
Nom d'hôte du serveur FTP	Nom d'hôte du ***proxy*** FTP
N° de port du serveur FTP	N° de port du ***proxy*** FTP (2121 par défaut)
Nom d'utilisateur du serveur FTP	nomUtilisateur_serveur_FTP@nomHôte_serveur_FTP Par exemple : anon@ftp.abc.com
Mot de passe du serveur FTP	Mot de passe du serveur FTP

Certains clients FTP disposent d'une page de configuration pour spécifier les informations du proxy FTP. Mettez ces paramètres à jour afin qu'ils pointent vers le proxy FTP de Content Gateway. Consultez la documentation de votre client FTP.

Voici un exemple de configuration dans une version récente du client FileZilla.



Dans la zone **FTP Proxy (Proxy FTP)** :

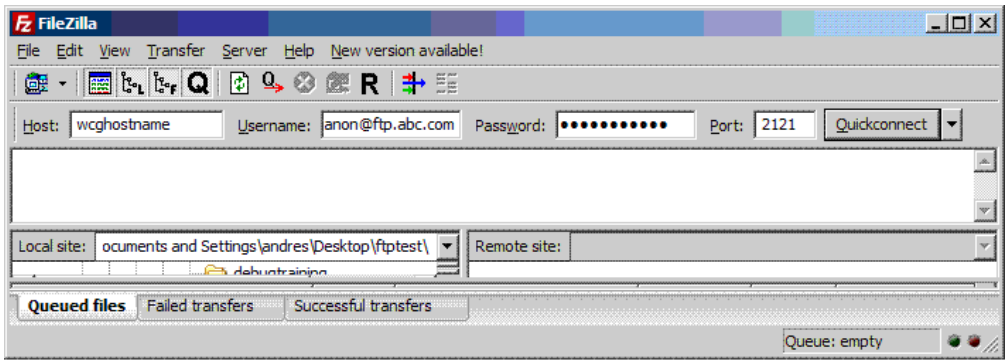
1. Définissez **Proxy FTP** sur **Custom (Personnalisé)** et définissez les valeurs USER et PASS comme indiqué.
2. Définissez **Proxy host (Hôte du proxy)** sur le nom d'hôte et le numéro de port du proxy FTP de Content Gateway.
3. Acceptez ces paramètres en cliquant sur **OK**.

L'utilisateur peut alors saisir ses informations de connexion FTP comme d'habitude, comme en l'absence d'un proxy. Par exemple :

Hôte :	ftp.abc.com
Nom d'utilisateur :	anon
Mot de passe :	123abc

Si le client FTP n'est **pas** configuré, l'utilisateur doit entrer ses requêtes FTP comme suit :

Hôte :	Nom d'hôte du proxy de Content Gateway
Nom d'utilisateur :	anon@ftp.abc.com
Mot de passe :	123acb
Port :	2121



Prise en charge d'IPv6 par Content Gateway version 7.7.0

La version 7.7 de TRITON Enterprise, y compris le composant proxy de Content Gateway, fournit une prise en charge incrémentielle d'IPv6.

> **Important**
> Cette prise en charge est fournie uniquement aux déploiements avec proxy explicite.

La prise en charge d'IPv6 par Content Gateway comprend :

- IPv6 sur interfaces Ethernet à double pile IP
- Prise en charge des protocoles HTTP, HTTPS, FTP, DNS
- Trafic IPv6 vers Internet, des clients et des serveurs de fichier PAC
- Adresses IP virtuelles IPv6 (vaddrs.config)
- Règles d'authentification par plages d'adresses IPv6 des clients
- Adresses de clients et plages d'adresses IPv6 pour autoriser ou limiter l'accès au proxy (ip_allow.config)
- Adresses de clients et plages d'adresses IPv6 pour autoriser ou limiter l'accès à Content Gateway Manager (mgmt_allow.config)
- Valeur de destination principale IPv6 et valeurs d'adresses IP source dans les règles de filtrages du proxy (filter.config), les règles du cache (cache.config) et les serveurs proxy parents dans une chaîne (parent.config)
- Adresses IPv6 dans la Liste des incidents de SSL
- Interruptions et compteurs SNMP pour les données IPv6

Limites et restrictions :

- Les réseaux internes uniquement en IPv6 ne sont pas pris en charge.
- Vous devez utiliser IPv4 pour communiquer avec tous les composants de TRITON, y compris avec les autres membres d'un cluster Content Gateway (adresse de multidiffusion).

> **Remarque**
> Contrairement au texte descriptif que l'on trouve dans Content Gateway Manager, les **Multicast Group Address (Groupes d'adresses en multidiffusion)** doivent être définis sur IPv4 (**Configurer > Mon proxy > De base > Clustering (Mise en cluster)**).

- Pour l'authentification de tous les utilisateurs, le ou les contrôleurs de domaine doivent pouvoir être contactés par une adresse IPv4.
- Le module ARM ne prend pas en charge les adresses IPv6, y compris pour les règles de redirection (ipnat.config) et les règles de contournement statique (bypass.config).
- Dans une chaîne, le proxy parent ne peut pas être en IPv6.
- L'usurpation d'adresse IP n'est pas prise en charge.
- Le proxy SOCKS n'est pas pris en charge.

Statistiques IPv6 du proxy :

Content Gateway surveille le trafic IPv6. Pour afficher ces statistiques, ouvrez la page **Monitor (Surveiller) > Networking (Mise en réseau) > System (Système)**.

Impact d'IPv6 sur les journaux d'événements :

Lorsqu'IPv6 est activé, les entrées du journal des événements sont normalisées au format IPv6. Par exemple, l'entrée « 10.10.41.200 » est journalisée sous la forme « ::ffff:10.10.41.200 ».

Pour récupérer le client « 10.10.41.200 » dans un journal personnalisé, utilisez le filtre suivant :

```
<LogFilter>
   <Name = "Machine_Test_IPv6"/>
   <Condition = "chi MATCH ::ffff:10.10.41.200"/>
   <Action = "ACCEPT"/>
</LogFilter>
```

Résumé de la configuration IPv6

La prise en charge d'IPv6 est désactivée par défaut.

Si Content Gateway est déployé dans un dispositif Websense, commencez par activer IPv6 dans Appliance Manager, dans l'onglet **Configuration > Interfaces réseau > IPv6**.

IPv6 est activé dans Content Gateway Manager, à la section **Réseau** de la page **Configurer > Mon proxy > De base**. Lorsqu'IPv6 est activé, sa prise en charge fonctionne dans toutes les zones opérationnelles, tel qu'indiqué dans la section précédente.

Dans tout champ qui accepte des adresses IPv6, vous pouvez saisir ces adresses dans tout format conforme au standard. Par exemple :

- Vous pouvez omettre les zéros non significatifs (en en-tête) dans une valeur de 16 bits.
- Toute série de zéros consécutifs peut être remplacée par un caractère deux points (:).

Lorsqu'IPv6 est désactivé, les champs de saisie IPv6 sont masqués et les valeurs IPv6 sont supprimées des fichiers de configuration.

Lorsque vous utilisez la résolution DNS (**DNS Resolver**), ouvrez la page **Configurer > Réseau > DNS Resolver** pour définir votre préférence : IPv4 ou IPv6. IPv4 est la valeur par défaut.

5 Proxy transparent et module ARM

L'option de proxy transparent permet à Content Gateway de répondre aux requêtes Internet des clients sans que les utilisateurs ne soient obligés de reconfigurer leur navigateur. Pour ce faire, il redirige le flux des requêtes vers le proxy après l'interception du trafic, en général par le biais d'un commutateur ou d'un routeur de Niveau 4 (L4).

Dans un déploiement de proxy transparent :

1. Le proxy intercepte les requêtes des clients destinées aux serveurs d'origine par le biais d'un commutateur ou d'un routeur. Voir *Stratégies d'interception transparente*, page 48.
2. Le module Adaptive Redirection Module (ARM) remplace l'adresse IP de destination du paquet entrant par l'adresse IP du proxy, ainsi que le port de destination du paquet par le port du proxy lorsque celui-ci diffère. (Le module ARM est toujours actif.)
3. Le proxy reçoit les requêtes de clients interceptées et commence à les traiter. Lorsque la requête correspond à un objet présent dans le cache, le proxy envoie l'objet demandé. Lorsque la requête ne correspond pas à un élément du cache, le proxy récupère l'objet sur le serveur d'origine et l'envoie au client.
4. Sur le trajet de retour vers le client, le module ARM remplace l'adresse IP et le port sources par l'adresse IP et le port du serveur d'origine.

Important

Dans le cas des configurations de proxy transparent dotées de plusieurs interfaces ou passerelles, Content Gateway doit utiliser les itinéraires appropriés vers les clients et Internet, indiqués dans la table de routage du système d'exploitation.

Pour HTTP, le proxy peut identifier les clients et serveurs présentant un problème et le module ARM peut désactiver l'interception de ces clients et servers pour transmettre directement le trafic correspondant au serveur d'origine. Vous pouvez également créer des règles de contournement statique ARM de sorte que certains clients et serveurs ne soient pas redirigés vers le proxy. Voir *Contournement de l'interception*, page 67.

Rubriques connexes :

- *Stratégies d'interception transparente*, page 48
- *Contournement de l'interception*, page 67
- *Délestage de la charge de connexion*, page 70
- *Réduction des recherches DNS*, page 71
- *Usurpation d'adresse IP*, page 72

Module ARM

Le module ARM de Content Gateway examine les paquets entrants avant que la couche IP ne les voit et les envoie ensuite à Content Gateway pour leur traitement.

Le module ARM peut apporter deux modifications à l'adresse d'un paquet entrant. Il peut modifier son adresse IP de destination et son port de destination. Par exemple, l'adresse IP de destination d'un paquet HTTP est remplacée par l'adresse IP du proxy et le port HTTP de destination par le port du proxy HTTP de Content Gateway (généralement le port 8080).

Sur le trajet de retour vers le client, le module ARM remplace l'adresse IP et le port sources par l'adresse IP et le port du serveur d'origine.

Le composant ARM est constitué de plusieurs fichiers et d'un module noyau, installés en même temps que le produit. Le programme d'installation crée également les règles de redirection des paquets via l'adresse IP de l'ordinateur proxy et des affectations de ports par défaut. Le module ARM est toujours actif.

Pour que le proxy desserve les requêtes HTTP, HTTPS, FTP ou DNS en toute transparence, vous devez vérifier les règles de redirection dans le fichier **ipnat.conf** et au besoin les modifier. Si vous utilisez WCCP pour l'interception transparente, une règle de redirection doit exister pour chaque port dans chaque groupe de services actifs. Les règles des ports standard sont incluses par défaut. Pour afficher et exploiter les règles de redirection ARM, procédez comme suit.

1. Connectez-vous à Content Gateway Manager et ouvrez l'onglet **Configurer > Networking (Mise en réseau) > ARM > Général**.

   La section **Network Address Translation (NAT) (Traduction d'adresses réseau)** affiche les règles de redirection présentes dans le fichier **ipnat.conf**. Vérifiez ces règles de redirection et procédez à toute modification nécessaire.

   a. Pour modifier une règle de redirection, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **ipnat.conf** dans l'éditeur de fichier de configuration.

   b. Sélectionnez la règle à éditer et modifiez les champs appropriés. Cliquez sur **Set (Définir)**, puis sur **Appliquer** pour valider vos modifications. Cliquez sur **Fermer** pour fermer l'éditeur de fichier de configuration.

   Tous les champs sont décris à la section *ARM*, page 321.

2. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Stratégies d'interception transparente

Websense Content Gateway prend en charge les solutions d'interception transparente suivantes :

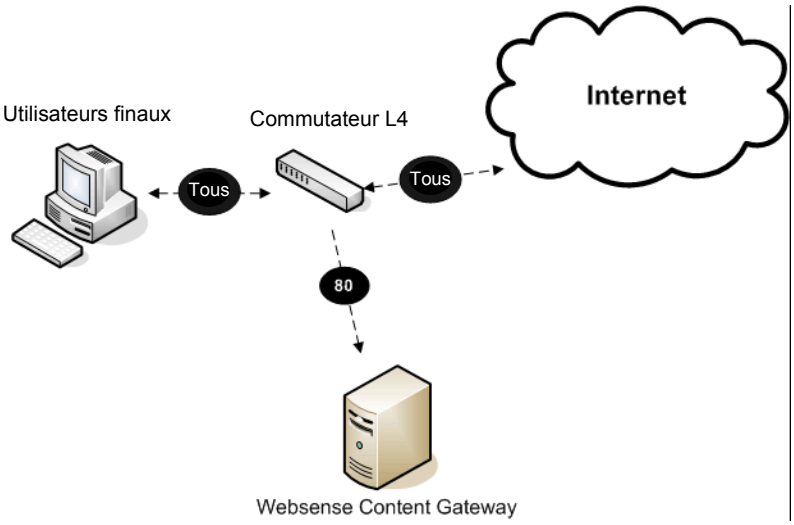
- Un commutateur de niveau 4. Voir *Interception transparente par un commutateur de niveau 4*, page 49.
- Un routeur ou un commutateur prenant en charge WCCP v2. Les routeurs Cisco de type IOS sont les plus courants. Voir *Interception transparente avec dispositifs WCCP v2*, page 50.

- Un routage en fonction des stratégies. Voir *Interception transparente et mode multidiffusion*, page 64.
- Un routage logiciel. Voir *Interception transparente avec routage logiciel*, page 66.

La manière exacte dont les requêtes de clients atteignent le proxy dépend de la topologie du réseau. Dans un réseau complexe, vous devez définir les clients devant être desservis en transparence et veiller à ce que les périphériques réseau et le proxy soient positionnés de manière à intercepter leurs requêtes. Content Gateway, ou les routeurs ou commutateurs qui l'alimentent, sont souvent déployés sur une artère principale ou un canal d'agrégation vers Internet.

Interception transparente par un commutateur de niveau 4

Les commutateurs de Niveau 4 peuvent rediriger les protocoles pris en charge vers le proxy, tout en transmettant directement le reste du trafic Internet vers sa destination, comme le montre l'illustration suivante pour le trafic HTTP.



Les commutateurs de Niveau 4 offrent les fonctionnalités suivantes, en fonction de leur type :

- Un commutateur de Niveau 4 capable de détecter les hôtes en panne sur le réseau et de rediriger le trafic renforce la fiabilité du système.
- Lorsqu'un même commutateur de Niveau 4 alimente plusieurs serveurs proxy, le commutateur gère l'équilibrage de la charge entre les différents nœuds Content Gateway. Les divers commutateurs peuvent utiliser différentes méthodes d'équilibrage de la charge, par exemple la permutation circulaire (round-robin) ou le hachage. Lorsqu'un nœud devient indisponible, le commutateur redistribue la charge. Lorsque le nœud est remis en service, certains commutateurs lui réattribuent sa charge de travail précédente, de sorte que le cache du nœud doive être à nouveau alimenté. Cette fonctionnalité est appelée *affinité du cache*.

> **Remarque**
> Nous vous conseillons de ne **pas** activer le basculement IP virtuel de Content Gateway lorsqu'un commutateur assure l'équilibrage de la charge dans une configuration en cluster.

Interception transparente avec dispositifs WCCP v2

Rubriques connexes :

- *Distribution de la charge WCCP*, page 52
- *Configuration des routeurs WCCP v2*, page 54
- *Activation de WCCP v2 dans Content Gateway*, page 59
- *Contournement ARM et WCCP*, page 52

Content Gateway prend en charge l'interception transparente avec les routeurs et commutateurs de type WCCP v2.

Les protocoles HTTP, HTTPS, FTP et DNS sont pris en charge. Les règles de redirection ARM par défaut sont incluses pour les communications HTTP, HTTPS et FTP sur les ports standard.

La liste des *Fonctionnalités WCCP v2 prises en charge* suit le plan de configuration.

Important

Les clients du réseau, les serveurs proxy Content Gateway et les serveurs Web de destination (passerelle par défaut) doivent résider dans des sous-réseaux distincts.

Voici le plan de configuration d'un WCCP v2.

1. Installez et configurez vos dispositifs WCCP v2.

   Dans chaque dispositif WCCP v2 :

   - Configurez les groupes de services.
   - Configurez au besoin la sécurité par mot de passe.
   - Configurez au besoin la communication en multidiffusion.

   Voir *Configuration des routeurs WCCP v2*, page 54.
2. Configurez Content Gateway pour qu'il fonctionne avec vos dispositifs WCCP.
   - Définissez les groupes de services correspondants.

     Outre l'interface réseau, les protocoles, les ports, l'authentification (le cas échéant) et la communication en multidiffusion (le cas échéant), configurez également :

     - Les adresses IP des dispositifs WCCP v2
     - La Méthode de transmission des paquets et la Méthode de retour des paquets
     - Si Content Gateway est déployé dans un cluster, la distribution de la charge de la **méthode d'attribution** (le cas échéant)
   - Créez les règles de traduction d'adresses réseau (NAT) ARM pour les ports non standard.

   Voir *Activation de WCCP v2 dans Content Gateway*, page 59, et *Module ARM*, page 48.
3. Validez la configuration en testant le trafic.

Fonctionnalités WCCP v2 prises en charge

Content Gateway prend en charge les fonctionnalités WCCP v2 suivantes :

- Plusieurs routeurs dans un cluster avec proxy
- Plusieurs ports par groupe de services
- Plusieurs groupes de services par protocole. Il est parfois nécessaire ou pratique d'utiliser des groupes de services distincts pour les différents dispositifs WCCP. Par exemple, dans le cas d'un pare-feu Cisco ASA, des groupes de services distincts sont requis pour chaque dispositif WCCP du réseau.
- La distribution de la charge dynamique dans un cluster avec proxy via une **méthode d'attribution** HASH ou MASK et le **poids**. Voir *Distribution de la charge WCCP*, page 52.
- La négociation de Méthode de transmission des paquets et de Méthode de retour des paquets
- La sécurité par mot de passe MD5 par groupe de services
- Le mode multidiffusion

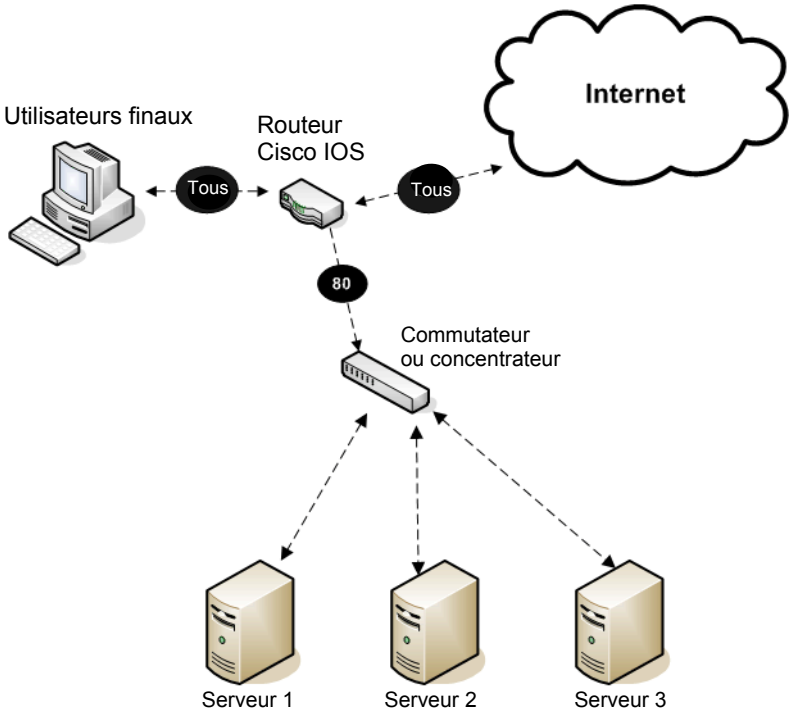
Dans un cluster Content Gateway, nous vous conseillons de ne **pas** activer le basculement IP virtuel dans les environnements WCCP. La configuration Content Gateway avec WCCP v2 gère les défaillances des nœuds et les redémarre. (Voir *Distribution de la charge WCCP*, page 52, et *Basculement IP virtuel*, page 83.)

Content Gateway prend également en charge l'affinité du cache. Lorsqu'un nœud n'est plus disponible, puis le redevient, son cache n'a pas besoin d'être à nouveau alimenté.

Fonctionnement de l'interception WCCP v2 :

1. Les dispositifs WCCP v2 envoient le trafic HTTP, HTTPS, FTP et DNS au serveur proxy ou au cluster de serveurs, conformément à la configuration du groupe de services.
2. Le module ARM réadresse le trafic. Par exemple, le trafic HTTP passant par le port 80 est réadressé au port 8080 de Content Gateway.
3. Le proxy traite la requête de la même façon que d'habitude, en renvoyant ensuite la réponse au client.

4. Le module ARM redéfinit l'adresse du port du proxy indiqué dans l'en-tête de réponse sur le port 80 (annulant le réadressage effectué sur le trajet vers le proxy). En conséquence, la réponse obtenue par l'utilisateur semble provenir directement du serveur d'origine.



Contournement ARM et WCCP

Lorsque Content Gateway dispose d'une règle de contournement ARM (présentée à la section *Contournement de l'interception*, page 67), il transmet directement les requêtes de certains clients au serveur d'origine, en contournant le proxy.

Les requêtes ignorées ne sont pas modifiées par le module ARM et conservent leur adresse IP source.

WCCP v2 vous permet d'exclure certaines interfaces de routeur de la redirection. **Les règles de contournement de Content Gateway ARM ne fonctionnent que si vous excluez l'interface du routeur auquel Content Gateway est connecté de la redirection WCCP.** Pour effectuer cette opération au niveau du routeur, sélectionnez l'interface connectée à Content Gateway et exécutez la commande de configuration du routeur **ip wccp redirect exclude in**. Le routeur exclut alors le trafic entrant sur l'interface spécifiée de toutes les règles de redirection.

Distribution de la charge WCCP

Le protocole WCCP fournit la **méthode d'attribution** pour la distribution dynamique des charges symétriques et asymétriques dans un cluster. WCCP détecte les défaillances des nœuds et effectue la redistribution en fonction de la configuration que Content Gateway lui a communiquée.

- La distribution de la charge est configurée dans Content Gateway Manager et envoyée aux dispositifs WCCP.

- La distribution de la charge est configurée **par groupe de services**.

  Pour chaque groupe de services :

  - Les membres participants du cluster doivent être enregistrés dans le groupe de services. (Le dispositif WCCP ne prend aucune décision en matière d'équilibrage de la charge.)
  - La méthode d'attribution HASH ou MASK est sélectionnée. La méthode HASH est généralement utilisée avec la méthode de transmission/retour GRE et la méthode MASK avec la méthode de transmission/retour L2.

    Important

    La méthode MASK a été développée spécialement pour les commutateurs de la gamme Cisco Catalyst et est l'une des caractéristiques clés qui permettent d'effectuer entièrement l'interception WCCP matérielle sur ces plateformes. Elle ne doit être utilisée qu'avec les dispositifs dont la prise en charge est documentée.

  - Un ou plusieurs **attributs de distribution** sont sélectionnés. En général, l'adresse IP de destination est utilisée.
  - Lorsque la charge doit être répartie entre les divers membres du cluster dans des proportions différentes, une valeur de **poids** est définie pour chaque membre du cluster. Cette valeur détermine la proportion de requêtes reçues par chaque membre du cluster par rapport aux autres.

    Une distribution de charge asymétrique utilisant la valeur **poids** se révèle utile dans les cas suivants :

    - Lorsque plusieurs serveurs Content Gateway présentent des capacités de performances inégales, par exemple un V-Series V10000 et un V10000 G2.
    - Lorsque le profil du trafic Internet n'autorise pas une distribution égale du fait des préférences de certains serveurs d'origine (et de ce fait des adresses IP de destination).

Fonctionnement de la redistribution dynamique :

Une redistribution dynamique est effectuée lorsque le dispositif WCCP détecte qu'un membre du cluster est hors ligne. Il redistribue alors automatiquement la charge aux membres restants du cluster en fonction de la configuration de la distribution de la charge. Lorsqu'un membre du cluster est remis en service et est détecté par le dispositif WCCP, la distribution de la charge est là encore ajustée automatiquement en fonction de la configuration.

Vous trouverez la procédure de configuration à la section *Configuration des groupes de services dans Content Gateway Manager*, page 60.

Prise en charge de la distribution asymétrique de la charge par la valeur du poids :

Lorsqu'elle est utilisée, la valeur du poids doit être définie dans chaque nœud du cluster. La valeur du poids est unique pour chaque groupe de services et chaque nœud. La valeur du poids ne se propage pas au sein du cluster.

Par rapport aux paramètres des autres membres du cluster, la valeur du poids détermine la proportion de trafic dirigée vers ce nœud par WCCP.

Par défaut, le poids est défini sur 0, c'est-à-dire pour une distribution identique entre tous les membres du cluster.

Pour obtenir une distribution asymétrique, le poids est défini par rapport aux autres membres du cluster. Par exemple, en supposant qu'un cluster comprenne 3 nœuds :

Nœud	Valeur du poids	Distribution de la charge
Nœud1	50	50%
Nœud2	25	25%
Nœud3	25	25%

Si Nœud1 est hors ligne, Nœud2 et Nœud3 récupèrent un volume égal de trafic. Si Nœud3 est hors ligne, Nœud1 obtient les deux tiers du trafic et Nœud2 le tiers restant.

La valeur du poids étant relative aux paramètres des autres nœuds du cluster, la distribution obtenue ci-dessus peut également être obtenue avec les valeurs 10, 5, 5. (La plage de poids valides va de 0 à 255.)

Lorsque le poids est à nouveau défini sur la valeur par défaut (0), cette valeur doit être configurée dans tous les nœuds du cluster.

Configuration des routeurs WCCP v2

Il est fortement recommandé de consulter la documentation et le site de support du fabricant afin d'obtenir des informations sur la configuration et les performances de votre dispositif WCCP v2. La plupart des périphériques doivent être configurés pour tirer pleinement parti de la redirection matérielle. Avec les dispositifs Cisco, la version la plus récente d'IOS est généralement la meilleure.

Pour préparer vos dispositifs WCCP v2 en vue de leur utilisation avec le proxy :

1. Configurez un ou plusieurs groupes de services pour les protocoles que vous prévoyez d'utiliser. Un même groupe de services peut gérer un ou plusieurs protocoles. Voir *Configuration des groupes de services dans le dispositif WCCP*, page 55.
2. Configurez le routeur de manière à activer le traitement WCCP pour ces groupes de services. Voir *Activation du traitement WCCP pour un groupe de services*, page 56.
3. Activez éventuellement la sécurité du routeur. La sécurité du routeur doit également être activée pour le groupe de services dans Content Gateway. Voir *Activation de la sécurité WCCP v2 dans le routeur*, page 58.

> **Remarque**
> Pour obtenir des instructions sur la configuration de votre propre routeur, reportez-vous à la documentation du fournisseur de votre matériel. Dans le cas des routeurs Cisco, consultez la page http://www.cisco.com/univercd/cc/td/doc/product/core/ et recherchez la version de votre IOS et de votre dispositif, par exemple, IOS 12.4.

4. Une fois la configuration du routeur terminée, vous devez également activer WCCP dans Content Gateway Manager. Voir *Activation de WCCP dans Content Gateway Manager*, page 59.

Configuration des groupes de services dans le dispositif WCCP

WCCP utilise des **groupe de services** pour définir le trafic redirigé vers Content Gateway (et d'autres dispositifs).

Un groupe de services peut intercepter le trafic passant par :

- Un ou plusieurs protocoles
- Un ou plusieurs ports

Un identifiant unique entier (ID) compris entre 0 et 255 est attribué aux groupes de services.

Les ID de groupe de services sont définis par l'utilisateur. Ils ne sont pas associés à un type de trafic ni à un port par défaut.

Le tableau suivant présente les définitions des groupes de services fréquemment utilisés dans les réseaux. Si vous configurez l'usurpation d'adresse IP, reportez-vous au tableau de la section *Usurpation d'adresse IP*, page 72, pour obtenir les ID de groupes de services inverses courants.

ID de service	Port	Type de trafic
0	80	HTTP
5	21	FTP
70	443	HTTPS (requiert SSL Manager)

Les groupes de services doivent être configurés dans le routeur et dans Content Gateway.

La meilleure pratique consiste à configurer d'abord le(s) routeur(s), puis Content Gateway.

Suivez les instructions fournies dans la documentation de votre propre routeur, mais d'une manière générale :

1. Pour identifier la configuration effectuée dans le routeur pour WCCP, entrez :

   ```
   show running-config | include wccp
   ```

2. Pour activer WCCP v2, entrez :

   ```
   ip wccp version 2
   ```

3. Si vous utilisez un autre cache de proxy avec votre routeur avant Content Gateway, désactivez l'ID de service précédemment utilisé. Par exemple, si vous utilisez un routeur Cisco, désactivez l'ID de service **web-cache** via la commande suivante :

   ```
   no ip wccp web-cache
   ```

4. Spécifiez les ID de groupes de services à utiliser avec Content Gateway. Pour savoir quelle commande utiliser, reportez-vous à la documentation de votre routeur.

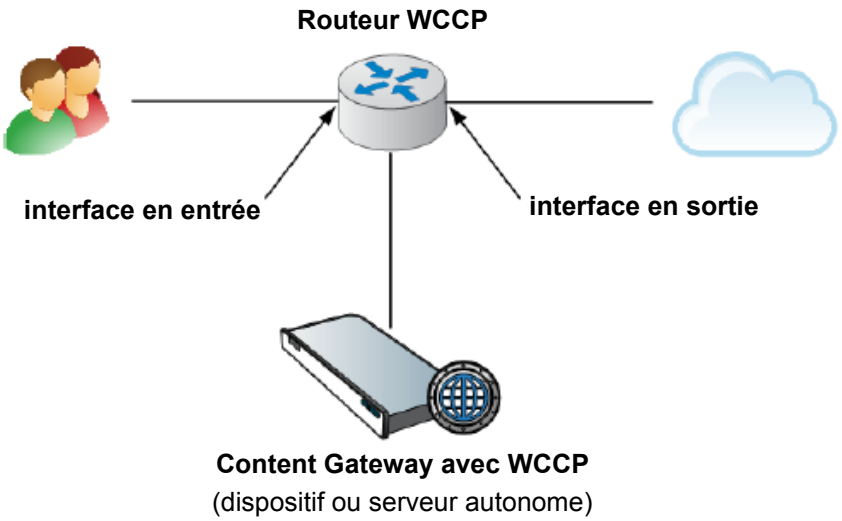
   Vous devez configurer chaque groupe de services pris individuellement en charge par le routeur. Vous ne pouvez pas configurer un routeur globalement.

Activation du traitement WCCP pour un groupe de services

Vous devez activer le traitement WCCP pour chaque groupe de services WCCP v2 configuré.

Les routeurs WCCP v2 contiennent plusieurs interfaces réseau, y compris :

- Une ou plusieurs interfaces recevant le trafic client entrant (en entrée)
- Une ou plusieurs interfaces connectées à Content Gateway
- Une interface dédiée au trafic sortant (en sortie) destiné à Internet



Voici quelques directives relatives à l'activation du traitement WCCP pour un groupe de services dans un routeur. Pour des instructions précises, consultez la documentation de votre propre routeur.

1. Activez la fonctionnalité WCCP :

   ```
   ip wccp <ID groupe de services> password [0-7] <motdepasse>
   ```

2. Dans l'interface du routeur ou du commutateur, activez la redirection des paquets entrants (en entrée) ou sortants (en sortie).

> **Remarque**
> Si votre matériel et votre topologie réseau l'autorisent, il est préférable d'effectuer la redirection au niveau de l'interface en entrée (à l'aide des commandes « redirect in »).

Voici quelques exemples. N'oubliez pas de remplacer les ID de groupe de services par ceux que vous avez définis dans votre ou vos routeurs.

Pour commencer, sélectionnez l'interface à configurer :

```
interface <type> <numéro>
```

Ensuite, définissez vos règles de redirection :

```
ip wccp <ID groupe de services> redirect in
```

Exemples de redirection du trafic entrant :

Exécutez les commandes suivantes pour chaque protocole que vous souhaitez prendre en charge, **mais uniquement sur la ou les interfaces dédiées au trafic** *entrant* **(en entrée)**.

Par exemple, pour activer la redirection du trafic passant par le port de destination HTTP, entrez :

```
ip wccp 0 redirect in
```

Pour activer la redirection du trafic passant par le port de destination HTTPS, entrez :

```
ip wccp 70 redirect in
```

Pour activer la redirection du trafic passant par le port de destination FTP, entrez :

```
ip wccp 5 redirect in
```

Pour activer la redirection du trafic passant par le port HTTP source, ce qui est requis pour l'usurpation d'adresse IP, entrez :

```
ip wccp 20 redirect in
```

Exemples de redirection du trafic *sortant* (en sortie) :

Exécutez les commandes suivantes pour chaque protocole que vous souhaitez prendre en charge, **mais uniquement sur la ou les interfaces dédiées au trafic** *sortant* **(en sortie)**.

Pour commencer, sélectionnez l'interface à configurer :

```
interface <type> <numéro>
```

Ensuite, définissez vos règles de redirection :

```
ip wccp <ID groupe de services> redirect out
```

Par exemple, pour activer la redirection du trafic pour HTTP, entrez :

```
ip wccp 0 redirect out
```

Pour activer la redirection du trafic pour HTTPS, entrez :

```
ip wccp 70 redirect out
```

Pour activer la redirection du trafic pour FTP, entrez :

```
ip wccp 5 redirect out
```

3. **IMPORTANT : lorsque le contournement ARM dynamique ou statique est activé, ou lorsque l'usurpation d'adresse IP est activée,** *et* **que la redirection s'effectue sur l'interface** *sortante* **(en sortie)**, excluez la redirection des paquets sortants de Content Gateway dans l'interface du routeur qui gère le trafic sortant de Content Gateway. Reportez-vous à l'illustration ci-dessous.

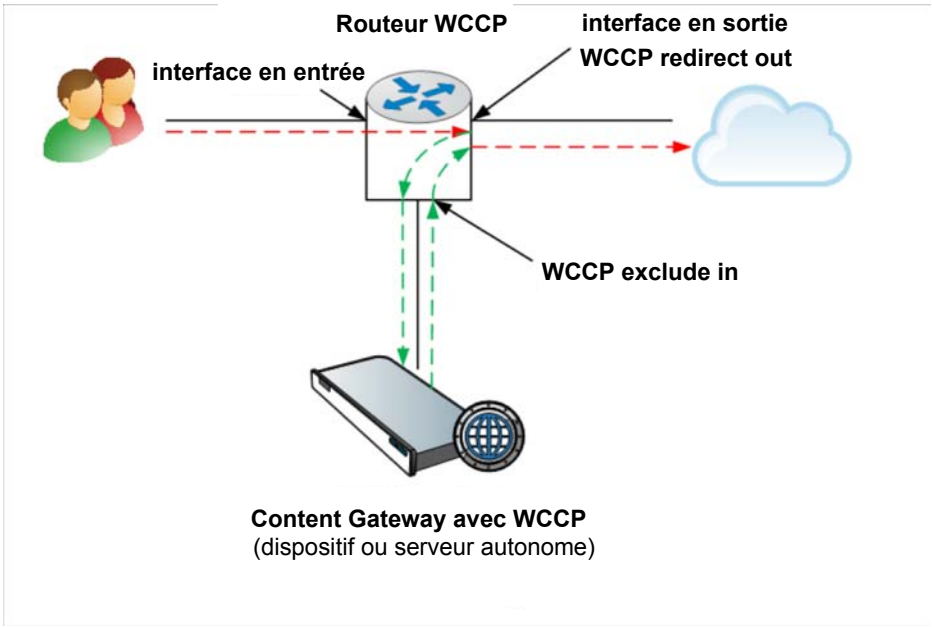
   a. Sélectionnez l'interface qui gère le trafic sortant de Content Gateway :

      ```
      interface <type> <numéro>
      ```

   b. Excluez le trafic sortant de Content Gateway sur l'interface de toutes les règles de redirection définies dans le routeur :

      ```
      ip wccp redirect exclude in
      ```

Lorsqu'un contournement ARM ce produit, ou si l'usurpation d'adresse IP est activée, le proxy envoie le trafic vers Internet en utilisant l'adresse IP source d'origine. La commande « redirect exclude in » empêche le routeur de retransmettre en boucle le trafic vers Content Gateway.



Désactivation du traitement WCCP pour un groupe de services

Si, pour une raison quelconque, vous devez désactiver le traitement WCCP, servez-vous de la commande suivante pour désactiver la fonctionnalité WCCP :

```
no ip wccp <ID groupe de services> password [0-7] <motdepasse>
```

Activation de la sécurité WCCP v2 dans le routeur

Si vous exécutez WCCP v2, vous devez activer la sécurité dans le nœud Content Gateway de sorte que le proxy et vos routeurs puissent s'authentifier mutuellement. Vous devez activer la sécurité de chaque groupe de services pris en charge par le routeur individuellement. Vous ne pouvez pas configurer un routeur globalement comme dans le cas de Content Gateway.

L'activation de l'option de sécurité et la fourniture du mot de passe d'authentification s'effectuent dans Content Gateway Manager.

Le mot de passe d'authentification que vous spécifiez doit correspondre au mot de passe d'authentification configuré dans le routeur pour chaque groupe de services intercepté. La procédure suivante présente un exemple de définition d'un mot de passe d'authentification pour des groupes de services différents.

1. Utilisez Telnet pour vous connecter au routeur et passez en mode Activé.
2. À l'invite, saisissez la commande suivante pour configurer le routeur à partir du terminal :

   ```
   configure terminal
   ```

3. Si vous avez défini un mot de passe lorsque vous avez activé WCCP dans le routeur, ignorez l'étape 4. Autrement, entrez la commande suivante pour chaque groupe de services intercepté par le routeur :

   ```
   nomhôte(config)# ip wccp groupe_service password motdepasse
   ```

   où *nomhôte* correspond au nom d'hôte du routeur que vous configurez, *groupe_service* à l'ID du groupe de services (par exemple, 0 pour HTTP) et *motdepasse* au mot de passe utilisé pour l'authentification de Content Gateway. Ce mot de passe doit correspondre à celui défini pour ce groupe de services dans la configuration de Content Gateway.

4. Fermez et enregistrez la configuration du routeur.

Activation de WCCP v2 dans Content Gateway

Rubriques connexes :

- *Configuration des routeurs WCCP v2*, page 54
- *Configuration des groupes de services dans le dispositif WCCP*, page 55
- *Activation du traitement WCCP pour un groupe de services*, page 56
- *Activation de la sécurité WCCP v2 dans le routeur*, page 58

Après avoir configuré vos routeurs WCCP v2, il vous reste à effectuer les étapes suivantes :

1. *Activation de WCCP dans Content Gateway Manager*
2. *Configuration des groupes de services dans Content Gateway Manager*
3. Redémarrage de Content Gateway

Important

Avant de redémarrer Content Gateway, vérifiez que votre configuration respecte les conditions suivantes :

- Les dispositifs Cisco IOS exécutent bien une version très récente d'IOS et tous les correctifs appropriés ont bien été appliqués.
- Les routeurs WCCP sont programmés avec les groupes de services et les autres fonctionnalités appropriés.

Activation de WCCP dans Content Gateway Manager

1. Accédez à **Configurer** > **Mon proxy > De base > Général**.
2. Dans la section **Networking (Mise en réseau)** du tableau **Features (Fonctions)**, localisez **WCCP** et cliquez sur **On (Activer)**, puis sur **Appliquer**. Ne redémarrez **pas** Content Gateway.

Configuration des groupes de services dans Content Gateway Manager

Chaque groupe de services WCCP qui redirige le trafic vers un serveur Content Gateway doit être associé à un groupe de services correspondant défini dans le cluster ou le serveur Content Gateway.

Important

Tous les attributs du groupe de services se propagent au sein du cluster, **à l'exception** de l'état **activé/désactivé**, de l'**interface réseau** spécifiée et du **poids** du groupe de services.

En conséquence :

- Les groupes de services ne doivent être configurés qu'une seule fois au sein du cluster.
- **A l'exception** du paramètre **activé/désactivé**, de l'**interface réseau** et du **poids** (le cas échéant) qui doivent être définis dans chaque nœud.

Ce fonctionnement permet d'exclure de façon spécifique l'activité de chaque groupe de services dans un nœud donné. De la même façon, l'exclusion du **poids** permet de distribuer la charge de façon proportionnelle (voir *Distribution de la charge WCCP*).

- Pour définir les groupes de services, sélectionnez **Configurer** > **Networking (Mise en réseau)** > **WCCP**.

  Le tableau des **Groupes de services** présente la liste des groupes de services configurés et un sous-ensemble de leurs paramètres de configuration.

  Les entrées sont stockées dans le fichier **wccp.config**.

  Le bouton **Actualiser** lit à nouveau le fichier **wccp.config** et actualise le tableau.
- Pour ajouter, modifier, supprimer ou réorganiser des groupes de services, cliquez sur **Edit File (Modifier le fichier)**.

Configuration d'un groupe de services (modification du fichier wccp.config)

1. Dans **Configurer** > **Networking (Mise en réseau)** > **WCCP**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **wccp.config** dans l'éditeur.

   Les groupes de services définis sont répertoriés en haut de la page.

   Cliquez sur une entrée de la liste pour en afficher les détails complets, la modifier ou la repositionner.

   Lorsqu'une entrée est sélectionnée, les flèches vers le bas et vers le haut situées à gauche de la liste permettent de déplacer l'entrée dans la liste.

   Pour supprimer une entrée sélectionnée, cliquez sur le « X ».
2. **Informations du groupe de services**
   a. **Service Group Status (État du groupe de services)** : pour activer un groupe de services, sélectionnez **Enabled (Activé)**. Un groupe de services peut être défini sans être actif. L'état **activé/désactivé** ne se propage pas au sein du cluster.
   b. **Service Group Name (Nom du groupe de services)** : spécifiez un nom de groupe de services unique. Le nom du groupe de services facilite l'administration.

c. **Service Group ID (ID du groupe de services)** : spécifiez un numéro d'identification de groupe de services WCCP compris entre 0 et 255. Cet identifiant doit correspondre à l'ID de groupe de services configuré dans le routeur. Voir *Configuration des groupes de services dans le dispositif WCCP*.

d. **Protocole** : spécifiez le protocole réseau applicable au groupe de services (TCP ou UDP).

e. **Ports** : spécifiez les ports que ce groupe de services doit utiliser. Vous pouvez spécifier jusqu'à 8 ports dans une liste séparée par des virgules.

> **Important**
> Chaque port du groupe de services doit être associé à une règle de traduction d'adresses réseau (NAT) ARM pour rediriger le trafic vers Content Gateway. Voir *Module ARM*.

f. **Network Interface (Interface réseau) :** dans la liste déroulante, sélectionnez l'interface réseau du système hôte Content Gateway que ce groupe de services doit utiliser. La valeur de **Network Interface (Interface réseau)** ne se propage pas au sein du cluster et, comme la valeur **Service Group Status (État du groupe de services)**, elle doit par conséquent être spécifiée pour chaque membre du cluster.

3. **Négociation du mode**

Le mode doit être sélectionné de manière à correspondre aux capacités et à la position du routeur ou du commutateur.

L'option **Packet Forward Method (Méthode de transmission des paquets)** détermine comment le trafic intercepté est transmis à partir du routeur WCCP vers le proxy.

L'option **Packet Return Method (Méthode de retour des paquets)** définit la méthode utilisée pour renvoyer le trafic intercepté au routeur WCCP.

En général, le routeur ne prend en charge qu'une seule méthode.

Le plus souvent, les méthodes de transmission et de retour correspondent.

a. **Packet Forward Method (Méthode de transmission des paquets)** : sélectionnez L2 ou GRE.

b. Si sous sélectionnez L2, la méthode de retour est automatiquement définie sur L2 (GRE n'est pas une option).

c. **Packet Return Method (Méthode de retour des paquets)** : sélectionnez L2 ou GRE.

> **Important**
> La sélection de L2 implique que le routeur ou le commutateur soit adjacent au Niveau 2 (dans le même sous-réseau que Content Gateway).
>
> L'option GRE ne peut pas être utilisée avec le mode multidiffusion WCCP.

Si Content Gateway est configuré avec une méthode de transmission/retour non prise en charge par le routeur, le proxy tente d'utiliser une méthode que ce routeur prend en charge.

4. **Paramètres avancés**

   a. **Assignment Method (Méthode d'attribution)** : spécifiez les paramètres utilisés pour distribuer le trafic intercepté entre les différents nœuds d'un cluster. Ces paramètres peuvent être combinés à la valeur du **poids** pour autoriser une distribution dynamique de la charge. La description de la fonctionnalité de distribution de la charge WCCP est disponible à la section *Distribution de la charge WCCP*, page 52.

   HASH applique une opération de hachage aux attributs de distribution sélectionnés.

   - L'option HASH permet de sélectionner plusieurs attributs de distribution.
   - Le résultat de l'opération de hachage identifie le membre du cluster devant recevoir le trafic.

   MASK applique une opération de masquage aux attributs de distribution sélectionnés.

   - Un seul attribut de distribution peut être sélectionné, en général l'adresse IP de destination.
   - Le résultat de l'opération de masquage identifie le membre du cluster devant recevoir le trafic.

   Les attributs de distribution suivants peuvent être sélectionnés :

   - Adresse IP de destination
   - Port de destination
   - Adresse IP source
   - Port source

   La valeur de MASK s'applique au maximum à 6 bits significatifs (dans un cluster, 64 compartiments sont créés au total). Pour plus d'informations sur la méthode d'attribution des opérations HASH et MASK, consultez votre documentation WCCP. Pour votre dispositif, utilisez la valeur recommandée dans la documentation du fabricant.

   b. **Weight (Poids)** : pour obtenir une distribution proportionnelle de la charge, spécifiez une valeur comprise entre 0 et 255. Cette valeur détermine la distribution proportionnelle de la charge entre les différents serveurs d'un cluster.

   Tous les membres du cluster sont définis par défaut sur la valeur 0, c'est-à-dire sur une distribution équilibrée du trafic. Si le poids est défini sur 1 ou sur une valeur supérieure, cette valeur régit la distribution proportionnelle entre les différents nœuds. Par exemple, lorsqu'un cluster comprend 3 nœuds, si le poids de Proxy1 est défini sur 20 et les poids de Proxy2 et Proxy3 sur 10, Proxy1 obtient la moitié du trafic et Proxy2 et Proxy3 obtiennent chacun un quart.

Important

Lorsque la valeur du **poids** est supérieure à 0 dans l'un des membres du cluster, tous les autres membres du cluster dont le poids est défini sur 0 ne reçoivent **aucun** trafic. Si vous envisagez d'utiliser le poids, assurez-vous de le définir pour chaque membre du cluster.

Remarque

La valeur du **poids** déterminant la distribution proportionnelle en fonction de la valeur définie dans les autres membres du cluster, elle ne se propage pas au sein du cluster.

Pour plus d'informations sur la distribution de la charge, consultez la section *Distribution de la charge WCCP*, page 52.

c. **Reverse Service Group ID (ID du groupe de services inverse)** : permet de définir un ID de groupe de services inverse.

Lorsque l'usurpation d'adresses IP est activée, vous devez définir un groupe de services inverse pour chaque groupe de services HTTP et HTTPS (le cas échéant) de transmission.

> **Remarque**
> Seuls HTTP et HTTPS sont pris en charge pour l'usurpation d'adresses IP.

Content Gateway utilise l'ID spécifié pour créer un groupe de services inverse correspondant au miroir du groupe de services de transmission. Par exemple, lorsque la méthode d'attribution du groupe de services de transmission est basée sur une adresse IP de destination, la méthode d'attribution du service inverse est basée sur l'adresse IP source.

> **Remarque**
> L'usurpation d'adresses IP n'est pas prise en charge avec les groupes de services qui utilisent une méthode d'attribution de hachage et des attributs source et de destination. Lorsque l'usurpation d'adresses IP est activée sur un tel groupe de services, une alarme se déclenche et l'usurpation d'adresses IP est désactivée.

5. **Informations sur le routeur**

> **Remarque**
> Quelques secondes sont nécessaires au routeur pour signaler qu'un nouveau serveur proxy a rejoint le groupe de services.

a. **Sécurité** : pour utiliser l'authentification WCCP facultative, sélectionnez **Enabled (Activé)** et saisissez le mot de passe utilisé pour l'authentification de ce groupe de services sur le routeur. Voir *Activation de la sécurité WCCP v2 dans le routeur*, page 58.

b. **Multicast (Multidiffusion)** : Pour une exécution en mode multidiffusion, sélectionnez **Enabled (Activé)** et saisissez l'adresse IP de multidiffusion. L'adresse IP de multidiffusion doit être la même que celle définie dans le routeur. Voir *Interception transparente et mode multidiffusion*, page 64.

> **Important**
> La méthode de transmission/retour de paquets GRE ne peut pas être utilisée avec le mode multidiffusion.

c. **WCCP Routers (Routeurs WCCP)** : spécifiez jusqu'à 10 adresses IP de routeurs WCCP. Ces routeurs doivent être configurés avec un groupe de services correspondant. Si la méthode de transmission ou de retour des paquets GRE est sélectionnée, spécifiez également l'adresse IP virtuelle de chaque routeur et l'adresse IP d'une passerelle. Les adresses IP virtuelles doivent être uniques.

> **Remarque**
> Si le routeur WCCP est configuré avec plusieurs adresses IP, par exemple lorsque le routeur est configuré pour prendre en charge plusieurs réseaux VLAN, l'adresse IP indiquée dans les statistiques **Monitor (Surveiller) > Networking (Mise en réseau) > WCCP** et dans les captures de paquets peut ne pas être la même que l'adresse IP configurée ici. En effet, le routeur signale systématiquement le trafic de l'adresse IP active la plus élevée.
>
> Pour que le routeur indique systématiquement la même adresse IP, une méthode consiste à définir l'adresse de bouclage sur une valeur supérieure à l'adresse IP du routeur. Il s'agit là de la configuration recommandée.

6. Cliquez sur **Ajouter** pour ajouter une entrée ou sur **Set (Définir)** pour enregistrer les modifications apportées à une entrée existante.
7. Cliquez sur **Fermer** pour quitter l'éditeur.
8. Dans la page **Configurer** > **Networking (Mise en réseau)** > **WCCP**, cliquez sur **Appliquer** pour valider vos modifications. Si vous quittez la page avant de cliquer sur **Appliquer**, vous perdrez toutes les modifications effectuées.
9. Pour que les modifications prennent effet, redémarrez le proxy. Sélectionnez **Configurer** > **Mon proxy** > **De base > Général**, puis cliquez sur **Redémarrer**.

> **Remarque**
> Pour vérifier que le routeur envoie le trafic au proxy, examinez les statistiques du volet **Monitor (Surveiller)** dans Content Gateway Manager. Par exemple, vérifiez que la valeur de la statistique **Objects Served (Objets desservis)** augmente dans la section **Mon proxy > Summary (Résumé)**.

Interception transparente et mode multidiffusion

Pour configurer l'exécution de Content Gateway en mode multidiffusion, vous devez activer le mode multidiffusion et spécifier l'adresse IP de multidiffusion dans Content Gateway Manager.

> **Important**
> La méthode de transmission/retour de paquets GRE ne peut pas être utilisée avec le mode multidiffusion.

Par ailleurs, vous devez définir l'adresse de multidiffusion dans vos routeurs pour chaque groupe de services intercepté (HTTP, FTP, DNS et SOCKS). La procédure suivante présente un exemple de définition d'une adresse de multidiffusion pour des groupes de services différents dans un routeur de type WCCP v2.

1. Utilisez Telnet pour vous connecter au routeur et passez en mode Activé.
2. À l'invite, saisissez la commande suivante pour configurer le routeur à partir du terminal :

   ```
   configure terminal
   ```

3. À l'invite, saisissez la commande suivante pour configurer chaque groupe de services intercepté par le routeur :

   ```
   nomhôte(config)# ip wccp groupe_service group-address
   adresse_multidiffusion
   ```

   où *nomhôte* correspond au nom d'hôte du routeur configuré, *groupe_service* à l'ID du groupe de services (par exemple, 0 pour HTTP) et *adresse_multidiffusion* à l'adresse de multidiffusion.
4. À l'invite, saisissez la commande suivante pour configurer l'interface réseau :

   ```
   interface nom_interface
   ```

   où *nom_interface* correspond à l'interface réseau dans le routeur intercepté et redirigé.
5. À l'invite, saisissez la commande suivante pour configurer chaque groupe de services intercepté par le routeur :

   ```
   nomhôte(config-if)# ip wccp groupe_service group-listen
   ```

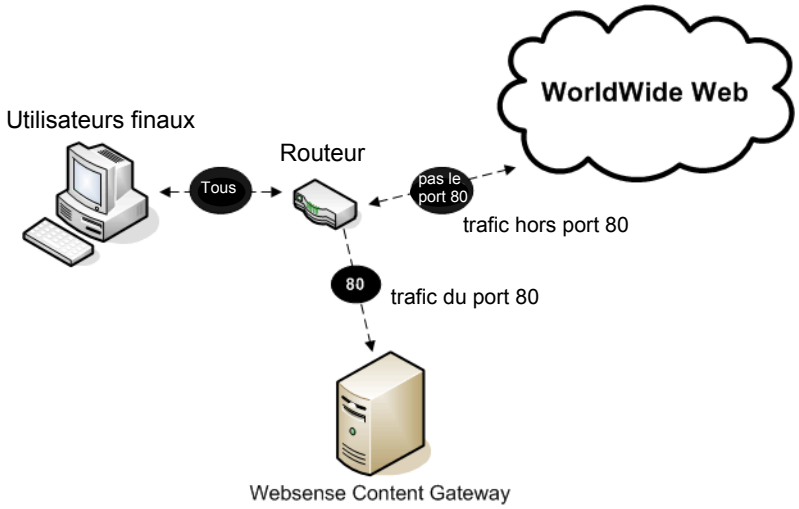
6. Fermez et enregistrez la configuration du routeur.

Interception transparente avec routage à base de stratégie

À la place du protocole WCCP, vous pouvez utiliser les capacités de routage stratégique d'un routeur pour envoyer le trafic vers Content Gateway. WCCP ou un commutateur de Niveau 4 sont généralement préférables dans cette configuration, car le routage à base de stratégie affecte les performances du routeur et ne prend pas en charge l'équilibrage de la charge ni les requêtes de pulsation.

- L'ensemble du trafic Internet des clients est envoyé à un routeur qui alimente Content Gateway.
- Le routeur envoie le trafic passant par le port 80 (HTTP) au proxy et le reste du trafic au routeur du prochain saut.
- Le module ARM traduit les requêtes interceptées en requêtes Content Gateway.
- Les requêtes traduites sont envoyées au proxy.
- Les objets Web à desservir de manière transparente sont réadressés par le module ARM sur le trajet de retour conduisant au client, de sorte que les documents semblent provenir du serveur d'origine.

Un cluster Content Gateway avec basculement IP virtuel renforce la fiabilité du système. En cas de défaillance d'un nœud, un autre peut récupérer ses requêtes en toute transparence. Voir *Basculement IP virtuel*, page 83.



Interception transparente avec routage logiciel

Vous pouvez déployer Content Gateway sans ajouter de routeurs ni de commutateurs en exploitant le routage logiciel au niveau du nœud Content Gateway. Dans ce cas, Content Gateway se comporte comme un routeur logiciel et achemine l'ensemble du trafic par l'intermédiaire du serveur proxy. Cette solution peut se révéler utile lorsque le trafic est faible, si le coût lié à l'utilisation du serveur proxy en tant que routeur n'est pas trop élevé en termes de performances.

Dans les systèmes Linux, vous pouvez utiliser les démons **routed** et **gated** comme solution de routage logiciel. Le démon **routed** fait partie intégrante de toutes les distributions Linux standard. Le démon **gated** est un package logiciel commercial extensible du Merit GateD Consortium.

Lorsque vous utilisez le routage logiciel avec Content Gateway :

- L'ensemble du trafic Internet provenant des ordinateurs situés derrière Content Gateway sur le réseau passe par Content Gateway.
- Le logiciel de routage achemine toutes les requêtes non transparentes vers Internet et les requêtes HTTP passant par le port 80 vers le cache du proxy.
- Le module ARM convertit les requêtes interceptées en requêtes du proxy.
- Les requêtes traduites sont envoyées au proxy.

- Les objets Web à desservir de manière transparente sont réadressés par le module ARM sur le trajet de retour conduisant au client, de sorte que les objets semblent provenir du serveur d'origine.

> **Remarque**
> Bien que les ordinateurs Content Gateway puissent jouer le rôle de routeurs, ils ne sont pas expressément conçus pour cela. Pour plus de fiabilité, vous pouvez utiliser un cluster Content Gateway avec l'option de basculement IP virtuel. En cas de défaillance d'un nœud, un autre nœud du cluster prend le relais. Voir *Basculement IP virtuel*, page 83. Le mécanisme de basculement de cluster de Content Gateway est similaire au protocole HSRP (Hot Standby Router Protocol).

Contournement de l'interception

Un nombre restreint de clients et de serveurs ne fonctionne pas correctement avec les proxy Web. Les raisons à ces limites comprennent notamment :

- Les anomalies logicielles des clients (navigateurs personnalisés, non commerciaux)
- Les anomalies logicielles des serveurs
- Les applications qui envoient du trafic non HTTP via des ports HTTP pour contourner les restrictions de sécurité
- L'authentification de l'adresse IP du serveur (le serveur d'origine restreint l'accès à quelques adresses IP de clients seulement, mais l'adresse IP de Content Gateway n'étant pas la même, l'accès n'est pas possible). Cette situation est peu fréquente, car la plupart des FAI allouent dynamiquement les adresses IP des clients et des protocoles cryptographiques plus sécurisés sont désormais généralement utilisés.

Les proxy Web étant très courants au sein des entreprises et sur Internet, les problèmes d'interopérabilité sont rares. Toutefois, Content Gateway contient un module d'apprentissage adaptatif qui détecte les problèmes d'interopérabilité dus au traitement du proxy transparent et ignore automatiquement le trafic au niveau du serveur proxy sans intervention de l'opérateur.

Content Gateway respecte deux types de règles de contournement :

- Les règles de contournement *dynamique* (également appelé adaptatif) sont générées de façon dynamique si vous configurez Content Gateway pour qu'il ignore le cache lorsqu'il détecte du trafic non HTTP sur le port 80 ou lorsqu'il rencontre certaines erreurs HTTP. Voir *Règles de contournement dynamique*, page 68.

- Les règles de contournement *statique* doivent être configurées manuellement dans le fichier **bypass.config**. Voir *Règles de contournement statique*, page 69.

> **Remarque**
> Ne confondez pas les règles de contournement ARM avec les listes de contrôle d'accès (ACL) des clients. Les règles de contournement sont créées pour répondre à des problèmes d'interopérabilité. Le contrôle de l'accès des clients restreint simplement les adresses IP des clients pouvant accéder au proxy, comme l'explique la section *Contrôle de l'accès des clients au proxy*, page 163.

Règles de contournement dynamique

Rubriques connexes :

- *Définition des règles de contournement dynamique*, page 69
- *Affichage des statistiques du contournement dynamique*, page 69

Lorsqu'il est configuré pour cela, le proxy surveille les erreurs d'interopérabilité entre les protocoles. Lorsqu'il détecte des erreurs, il configure le module ARM de sorte qu'il ignore le proxy pour les clients et serveurs à l'origine de ces erreurs.

Les quelques clients ou serveurs qui ne fonctionnent pas correctement via les proxy sont donc détectés automatiquement et acheminés de manière à contourner le serveur proxy de mise en cache pour qu'ils continuent à fonctionner (mais sans mise en cache).

Vous pouvez configurer le proxy pour qu'il ignore lui-même dynamiquement les erreurs suivantes :

Code d'erreur	Description
N/A	Trafic non HTTP passant par le port 80
400	Requête incorrecte
401	Non autorisé
403	Interdit (échec d'authentification)
405	Méthode non autorisée
406	Non acceptable (accès)
408	Expiration de la requête
500	Erreur interne du serveur

Par exemple, lorsque Content Gateway est configuré pour ignorer un échec d'authentification (**403 Refusé**), il génère une règle de contournement de destination pour l'adresse IP du serveur d'origine lorsqu'une requête destinée à un serveur d'origine renvoie une erreur 403. Toutes les requêtes destinées au serveur d'origine sont ignorées jusqu'au redémarrage du proxy.

Dans un autre exemple, lorsque le module ARM détecte qu'un client envoie une requête non HTTP à un serveur d'origine spécifique via le port 80, Content Gateway génère une règle de source/destination. Toutes les requêtes provenant de ce client et destinées au serveur d'origine sont ignorées, mais pas celles qui proviennent des autres clients.

Les règles de contournement générées dynamiquement sont purgées lorsque Content Gateway redémarre. Pour conserver les règles générées dynamiquement, vous pouvez enregistrer un instantané de l'ensemble des règles de contournement actuelles. Voir *Affichage des règles de contournement définies*, page 70.

Pour empêcher Content Gateway de contourner dynamiquement certaines adresses IP, vous pouvez définir des règles de refus de contournement dynamique dans le fichier **bypass.config**. Les règles de refus de contournement peuvent empêcher le proxy de se contourner lui-même. Pour plus d'informations sur la définition de règles de refus de contournement dynamique, consultez la section *Fichier de configuration bypass.config*, page 350.

Définition des règles de contournement dynamique

Par défaut, Content Gateway n'est pas configuré pour s'ignorer lui-même lorsqu'il rencontre des erreurs HTTP ou un trafic non HTTP sur le port 80. Vous devez activer les règles de contournement dynamique en définissant les options appropriées.

1. Accédez à **Configurer** > **Networking (Mise en réseau)** > **ARM > Dynamic Bypass (Contournement dynamique)**.
2. Activez l'option **Dynamic Bypass (Contournement dynamique)**.
3. Dans la section **Behavior (Comportement)**, sélectionnez les règles de contournement dynamique que vous souhaitez utiliser.
4. Cliquez sur **Appliquer**.
5. Cliquez sur **Redémarrer** dans l'onglet **Configurer** > **Mon proxy > De base > Général**.

Affichage des statistiques du contournement dynamique

Content Gateway tient le compte des requêtes ignorées pour chaque type de déclencheur du contournement dynamique. Par exemple, Content Gateway compte toutes les requêtes ignorées en réponse à une erreur 401.

- Sélectionnez **Monitor (Surveiller)** > **Networking (Mise en réseau)** > **ARM**.

Les statistiques s'affichent dans la section **HTTP Bypass Statistics (Statistiques de contournement HTTP)** du tableau.

Règles de contournement statique

Vous pouvez configurer des règles de contournement pour acheminer les requêtes de certains clients ou destinées à des serveurs d'origine spécifiques sans passer par le proxy. Contrairement aux règles de contournement dynamique qui sont purgées au

redémarrage du proxy, ces règles de contournement statique sont enregistrées dans un fichier de configuration.

Vous pouvez configurer trois types de règles de contournement statique :

- Le contournement de la source, qui permet à Content Gateway d'ignorer une adresse IP source ou une plage d'adresses IP spécifique. Vous pouvez par exemple exploiter cette solution pour ignorer les clients qui ne veulent pas utiliser une solution de mise en cache.
- Le contournement de la destination, qui permet à Content Gateway d'ignorer une adresse IP ou une plage d'adresses IP de destination spécifique. Il peut par exemple s'agir de serveurs d'origine qui utilisent l'authentification IP en se basant sur l'adresse IP réelle du client. Les règles de contournement de la destination empêchent Content Gateway de mettre en cache la totalité d'un site. Si le site contourné est populaire, l'impact sera important en termes de taux d'accès.
- Le contournement de paires source/destination qui permet à Content Gateway d'ignorer les requêtes provenant de la source indiquée et destinées à la destination spécifiée. Par exemple, vous pouvez détourner certaines paires de client/serveur qui rencontrent des problèmes d'authentification IP rompue ou de trafic HTTP hors bande.

  Les règles de contournement de source/destination sont parfois préférables aux règles de destination, car elles ne bloquent un serveur de destination que pour les utilisateurs qui rencontrent des problèmes.

Pour configurer des règles de contournement statique, modifiez le fichier **bypass.config** (voir *Fichier de configuration bypass.config*, page 350).

Affichage des règles de contournement définies

Le module ARM dispose d'un utilitaire de support appelé **print_bypass** qui vous permet d'afficher les règles de contournement dynamique et statique existantes.

Pour afficher l'ensemble des règles de contournement dynamique et statique existantes :

1. Connectez-vous à un nœud Content Gateway, puis accédez au répertoire **bin** de Content Gateway (/opt/WCG/bin).
2. À l'invite, saisissez la commande suivante, puis appuyez sur la touche **Retour** :

   ```
   ./print_bypass
   ```

   Toutes les règles de contournement statique et dynamique existantes s'affichent à l'écran. Les règles sont classées par adresse IP. Vous pouvez envoyer le résultat de la commande **print_bypass** dans un fichier et enregistrer ce dernier.

Délestage de la charge de connexion

La fonctionnalité de délestage de la charge prévient également les surcharges de requêtes des clients. Lorsque le nombre de connexions client dépasse la limite définie, le module ARM transmet directement les requêtes entrantes au serveur d'origine. Par défaut, le nombre de connexions de clients est limité à 1 million.

1. Sélectionnez **Configurer** > **Networking (Mise en réseau)** > **Connection Management (Gestion des connexions) > Load Shedding (Délestage de la charge)**.
2. Dans le champ **Maximum Connections (Nombre maximal de connexions)**, définissez le nombre maximal de connexions de clients autorisées avant que le module ARM ne commence à transmettre directement les requêtes au serveur d'origine.
3. Cliquez sur **Appliquer**.
4. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Réduction des recherches DNS

Si vous exécutez Content Gateway en mode proxy transparent, vous pouvez activer l'option *Always Query Destination (Demander systématiquement la destination)* pour réduire le nombre de recherches DNS et améliorer les délais de réponse. Lorsqu'elle est activée, cette option configure le proxy pour qu'il obtienne systématiquement l'adresse IP de destination originale des requêtes entrantes issues du module ARM. Content Gateway utilise alors cette adresse IP pour identifier le serveur d'origine, au lieu d'effectuer une recherche DNS en se basant sur le nom d'hôte de la requête. Le client ayant déjà effectué une recherche DNS, Content Gateway n'a pas besoin de le faire.

Remarque

Il est recommandé de ne pas activer l'option Always Query Destination (Demander systématiquement la destination) lorsque Content Gateway s'exécute à la fois en mode proxy explicite et transparent. Pour plus d'informations sur l'exécution de Content Gateway en mode proxy transparent uniquement, consultez la section *Comment configurer Content Gateway pour qu'il ne desserve que les requêtes transparentes ?*, page 470. En mode proxy explicite, le client n'effectue pas de recherche DNS basée sur le nom d'hôte du serveur d'origine ; cette opération doit donc être effectuée par le proxy. De même, la recherche de catégorie est basée sur l'adresse IP, ce qui n'est pas toujours aussi précis qu'une recherche d'URL.

Par ailleurs, n'activez pas l'option Always Query Destination (Demander systématiquement la destination) lorsque vous souhaitez capturer les noms de domaine dans le serveur de journalisation et non pas les adresses IP.

Pour activer l'option Always Query Destination (Demander systématiquement la destination) :

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway (/opt/WCG/config).

2. Modifiez la variable suivante :

Variable	Description
proxy.config.arm.always_query_dest	Pour désactiver l'option Always Query Destination (Demander systématiquement la destination), définissez cette valeur sur 0. Les noms de domaine sont capturés. Pour activer l'option Always Query Destination (Demander systématiquement la destination), définissez cette valeur sur 1. Les adresses IP sont capturées et non plus les noms de domaine.

3. Enregistrez et fermez le fichier.
4. Pour appliquer vos modifications, exécutez la commande suivante dans le répertoire **bin** de Content Gateway :

```
content_line -x
```

Usurpation d'adresse IP

L'usurpation d'adresse IP configure le proxy pour qu'il utilise l'adresse IP du client lorsqu'il communique avec le serveur d'origine, au lieu d'utiliser la propre adresse IP du proxy. En conséquence, les requêtes semblent provenir du client et non plus du proxy.

- L'usurpation d'adresse IP est prise en charge pour le trafic HTTP et HTTPS uniquement.
- Lorsque l'usurpation d'adresse IP est activée, elle s'applique à la fois au trafic HTTP et HTTPS. Elle ne peut pas être configurée pour ne s'appliquer qu'à un seul protocole.
- L'usurpation d'adresse IP est prise en charge pour le trafic transparent uniquement.

- L’usurpation d’adresse IP s’appuie sur le module ARM.

Avertissement

Le déploiement de l’usurpation d’adresse IP requiert un contrôle précis des itinéraires de routage sur le réseau, car il remplace le processus de routage standard du trafic s’exécutant sur les ports TCP 80 et 443.

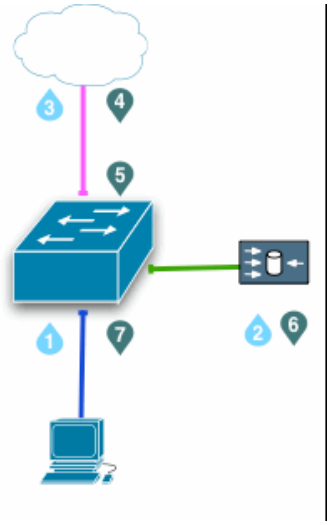
Lorsque l’usurpation d’adresse IP est activée, les outils de débogage traditionnels tels que **traceroute** et **ping** ont une utilité limitée.

Important

Pour plus d’informations sur l’impact de la table de routage du noyau du proxy sur le déploiement du proxy transparent, consultez l’article du Centre de solutions intitulé « Web sites in the Static or Dynamic bypass list fail to connect (« Échec de connexion des sites Web de la liste de contournement statique ou dynamique »).

Usurpation d’adresse IP et flux du trafic

La section suivante décrit le flux de trafic HTTP et HTTPS lorsque l’usurpation d’adresse IP est utilisée avec WCCP. L’implémentation d’un routage à base de stratégie permet d’obtenir le même résultat. Les chiffres indiqués dans le diagramme correspondent aux actions décrites dans la liste numérotée.



1. Une requête de client parvient à un port routé ou à une interface SVI (Switched Virtual Interface), à la recherche du trafic destiné à un port HTTP (80) ou HTTPS (443).

2. Le commutateur redirige la requête du client vers Content Gateway (le proxy) et ce dernier achemine en interne le trafic vers le port 8080 (HTTP) ou 8070 (HTTPS) de sa propre adresse IP.

   Au besoin, le proxy crée une connexion au serveur Web d'origine en utilisant l'adresse IP d'origine du client.
3. La requête est envoyée au serveur Web d'origine via le commutateur, la traduction d'adresses réseau (NAT) et/ou le pare-feu.
4. Lorsque la réponse du serveur d'origine est renvoyée, le paquet IP contient l'adresse IP du client comme destination.
5. La réponse du serveur d'origine parvient à un port routé ou à une interface SVI (Switched Virtual Interface), à la recherche du trafic provenant d'un port source HTTP (80) ou HTTPS (443). Voir la remarque ci-dessous.
6. Le commutateur redirige la réponse du serveur d'origine vers le proxy, pour terminer la connexion TCP proxy vers serveur Web.
7. La réponse du proxy destinée au client est générée et renvoyée au client sur la connexion TCP proxy vers client.

> **Remarque**
> Lorsque l'usurpation d'adresse IP est activée, le proxy annonce un groupe de services inverse pour chaque service WCCP activé. Le groupe de services inverse doit être appliqué tout au long de l'itinéraire de retour du proxy.

Les ID de groupe de services WCCP sont définis par l'utilisateur et doivent être programmés dans le(s) dispositif(s) et dans Content Gateway (voir *Configuration des groupes de services dans le dispositif WCCP* et *Configuration des groupes de services dans Content Gateway Manager*).

Voici quelques suggestions de définition.

ID de service	Port	Type de trafic
0	Port de destination 80	HTTP
20	Port source 80	HTTP
70	Port de destination 443	HTTPS (requiert SSL Manager)
90	Port source 443	HTTPS

Le **routage à base de stratégie** (Policy-based routing, ou PBR) utilise des listes de contrôle d'accès (ACL) pour identifier et rediriger les flux. Dans un déploiement PBR, toute la configuration s'effectue au niveau du routeur et il n'existe pas de configuration Content Gateway correspondante. Les déploiements PBR doivent rediriger le trafic revenant des serveurs d'origine via les ports 80 et 443 vers Content Gateway.

Activation de l'usurpation d'adresse IP :

1. Sélectionnez **Configurer** > **Networking (Mise en réseau)** > **ARM > Général**.
2. Sélectionnez **IP Spoofing (Usurpation d'adresse IP)**.
3. Cliquez sur **Appliquer**.
4. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Avertissement

Le module ARM est un composant essentiel de Content Gateway et ne doit jamais être désactivé. S'il est désactivé alors que l'usurpation d'adresse IP est activée, les requêtes des clients reçoivent une erreur d'échec d'affichage de la page Web et un message d'erreur est enregistré dans /var/log/messages.

Pour plus d'informations sur la configuration des routeurs WCCP, consultez la section *Configuration des routeurs WCCP v2*, page 54.

6 Clusters

Rubriques connexes :

- *Mise en cluster de SSL Manager*, page 78
- *Modification de la configuration du clustering*, page 80
- *Ajout de nœuds à un cluster*, page 81
- *Retrait de nœuds dans un cluster*, page 82
- *Basculement IP virtuel*, page 83

Websense Content Gateway peut évoluer d'un seul nœud jusqu'à un cluster de 15 nœuds ou plus, ce qui vous permet de rapidement augmenter vos capacités et d'améliorer les performances et la fiabilité du système.

- Content Gateway détecte l'ajout et la suppression des nœuds dans le cluster. Il peut également détecter l'interruption d'un nœud.
- À tout moment, vous pouvez ajouter ou supprimer un nœud dans le cluster.
- Lorsque vous retirez un nœud du cluster, Content Gateway supprime toutes les références au nœud manquant.
- Le redémarrage d'un nœud dans le cluster entraîne le redémarrage de tous les nœuds de ce cluster.
- Lorsque la fonction *Basculement IP virtuel* est activée, les nœuds actifs d'un cluster peuvent assurer le trafic d'un nœud défaillant.
- Les nœuds d'un même cluster partagent automatiquement leurs informations de configuration.

Remarque

Les adresses IP de Filtering Service et de Policy Service ne sont pas propagées au niveau du cluster.

Dans les déploiements de proxy transparent avec WCCP, les paramètres de poids et d'état Activé/Désactivé du groupe de services ne sont pas propagés. Voir *Interception transparente avec dispositifs WCCP v2*, page 50.

Content Gateway utilise un protocole propriétaire pour la mise en cluster. Ce protocole est multidiffusé pour la détection et les requêtes de pulsation des nœuds, et à diffusion point à point pour tous les échanges de données au sein du cluster.

Important

Il est recommandé d'utiliser une interface réseau dédiée pour les communications du cluster Content Gateway, **sauf** lorsque l'hôte est un dispositif V-Series, auquel cas l'interface P1 (eth0) est recommandée.

Important

Dans une hiérarchie de serveurs proxy, les nœuds du cluster ne peuvent pas être une combinaison de parents et d'enfants HTTP. Vous devez configurer chaque nœud dans un cluster Content Gateway en tant que nœud unique dans la hiérarchie, car ils partagent tous la même configuration.

Gestion de la mise en cluster

En mode Gestion de la mise en cluster, vous pouvez administrer tous les nœuds Content Gateway simultanément, car tous les nœuds du cluster partagent les mêmes informations de configuration.

Remarque

Dans un cluster, vous pouvez avoir 15 nœuds ou plus.

Pour obtenir de l'aide lors de la mise à l'échelle de votre déploiement, contactez votre représentant Websense.

- Content Gateway utilise un protocole de gestion en multidiffusion pour conserver une seule image système de tous les nœuds du cluster.
- Les informations sur l'appartenance, la configuration et les exceptions du cluster sont partagées par tous les nœuds.
- Le processus **content_manager** propage les modifications de la configuration aux nœuds du cluster.
- Lorsque SSL Manager est activé, la configuration SSL peut être propagée au niveau du cluster. Toutefois, un mécanisme distinct est utilisé pour ce faire. Voir la section suivante.

Mise en cluster de SSL Manager

Lorsque SSL Manager est activé dans un cluster, la configuration SSL peut être propagée au niveau de ce cluster. Toutefois, elle utilise un mécanisme distinct qui exige une configuration séparée.

Pour configurer SSL Manager de sorte qu'il propage les informations de configuration au niveau du cluster, un nœud doit être sélectionné en tant que nœud **primaire** au niveau duquel s'effectueront toutes les modifications de la configuration SSL. Ce nœud primaire est appelé **Serveur de configuration de SSL Manager**. Tous les autres nœuds sont **secondaires**.

- Les paramètres définis dans le nœud primaire sont propagés dans les nœuds secondaires.
- Ces nœuds secondaires interrogent périodiquement le nœud primaire pour savoir si des modifications sont en attente. Si c'est le cas, chaque nœud secondaire récupère ces modifications.
- Si des modifications de la configuration interviennent dans un nœud secondaire, elles seront remplacées lors de la récupération de la configuration principale auprès du nœud primaire.
- Si le nœud primaire tombe en panne, une alarme est générée et les nœuds secondaires continuent de fonctionner avec leur configuration actuelle jusqu'à la remise en service du nœud primaire ou la configuration d'un nouveau nœud primaire.

Lorsque la mise en cluster de SSL Manager est configurée, les paramètres de configuration suivants sont propagés :

- L'adresse IP du nœud primaire
- Configurer > SSL > Certificats > Autorités de certification
- Configurer > SSL > Certificats > Add Root CA (Ajouter une autorité de certification racine)
- Configurer > SSL > Certificats > Restore Certificates (Restaurer les certificats)
- Configurer > SSL > Décryptage / Cryptage : tous les paramètres
- Configurer > SSL > Validation : tous les paramètres
- Configurer > SSL > Client Certificates (Certificats clients) : tous les paramètres
- Configurer > SSL > Journalisation : tous les paramètres
- Configurer > SSL > Internal Root CA (Autorité de certification racine interne) > Import Root CA (Importer une autorité de certification racine)
- Configurer > SSL > Internal Root CA (Autorité de certification racine interne) > Create Root CA (Créer une autorité de certification racine)
- Certificats et incidents générés dynamiquement

Configuration de la mise en cluster de SSL Manager

1. Configurez et démarrez Management Clustering. Voir *Modification de la configuration du clustering*.
2. Dans tout nœud du cluster, connectez-vous à Content Gateway Manager.
3. Ouvrez l'onglet **Configurer > Mon proxy > De base > Clustering**.
4. Dans le champ **SSL Manager Configuration Server (Serveur de configuration de SSL Manager)**, entrez l'adresse IP du Serveur de configuration de SSL Manager (le nœud primaire). Si ce champ ne peut pas être modifié, le système auquel vous êtes connecté n'est pas membre du cluster.
5. Cliquez sur **Appliquer**, puis redémarrez Content Gateway. Notez que tous les nœuds Content Gateway sont redémarrés également. Ce redémarrage permet à tous les membres du cluster d'identifier le nœud primaire et d'activer le clustering SSL.

Cette configuration peut être confirmée dans la page **Monitor (Surveiller) > Mon proxy > Résumé**, en bas de la section **Node Details (Détails des nœuds)**. Si l'adresse IP du **Serveur de configuration de SSL Manager** est un lien, ce serveur est un autre nœud du cluster. Cliquez sur ce lien pour vous connecter au **Serveur de configuration de SSL Manager**.

Modification de la configuration du clustering

Le clustering est généralement configuré lors de l'installation du proxy. Toutefois, vous pouvez le configurer ultérieurement ou à tout moment dans Content Gateway Manager.

1. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Mon proxy > De base > Clustering**.
2. Dans la zone **Type de cluster**, sélectionnez le mode de clustering :
   - Sélectionnez **Management Clustering** pour inclure ce proxy dans un cluster.
   - Sélectionnez **Single Node (Nœud unique)** si ce nœud n'est pas membre d'un cluster.
3. Dans la zone **Interface du cluster**, entrez le nom de l'interface réseau. Il s'agit de l'interface utilisée par Content Gateway pour communiquer avec les autres nœuds du cluster, par exemple : eth0.

   Il est recommandé d'utiliser une interface secondaire dédiée.

   Les informations de configuration des nœuds sont multidiffusées, en texte brut, vers les autres nœuds Content Gateway du même sous-réseau. C'est pourquoi Websense recommande de placer les clients dans un sous-réseau différent de celui des nœuds Content Gateway. En effet, les communications en multidiffusion ne sont pas acheminées pour le clustering.

   Pour les dispositifs V-Series, P1 (eth0) est l'interface conseillée. Vous pouvez cependant utiliser également P2 (eth1) si vous souhaitez isoler le trafic de gestion du cluster.
4. Dans la zone **Cluster Multicast Group Address (Adresse du groupe en multidiffusion pour le cluster)**, entrez l'adresse du groupe en multidiffusion qui est partagée par tous les membres du cluster.
5. Si vous utilisez **SSL Manager** et que vous souhaitez que les informations de la configuration SSL se propagent au niveau du cluster, entrez l'adresse IP du Serveur de configuration de SSL Manager. Dans un cluster, les informations de la configuration SSL sont gérées par un mécanisme distinct. Pour exploiter efficacement cette fonction, vous devez vous familiariser avec ce mécanisme. Voir *Mise en cluster de SSL Manager*.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Important

Content Gateway n'applique pas le changement de mode de clustering à tous les nœuds du cluster. Vous devez modifier le mode de clustering dans chaque nœud individuellement.

Ajout de nœuds à un cluster

Content Gateway détecte les nouveaux nœuds Content Gateway dans votre réseau et les ajoute au cluster, en propageant les dernières informations de configuration aux nouveaux arrivants. Vous disposez ainsi d'une méthode pratique pour amorcer de nouvelles machines.

Pour connecter un nœud à un cluster Content Gateway, il vous suffit d'installer le logiciel Content Gateway dans le nouveau nœud. Pendant ce processus, assurez-vous que le nom du cluster et les ports attribués soient bien ceux du cluster existant. Ainsi, Content Gateway reconnaîtra automatiquement le nouveau nœud.

> **Important**
> Les nœuds d'un cluster doivent être homogènes. Chacun d'eux doit résider dans la même plateforme matérielle, avec la même version de système d'exploitation, et Content Gateway doit être installé dans le même répertoire (**/opt/WCG**).

1. Installez le matériel approprié et connectez-le à votre réseau. (Pour obtenir des instructions d'installation, consultez la documentation de votre matériel.)
2. Installez le logiciel Content Gateway à l'aide de la procédure appropriée pour l'installation d'un nœud de cluster. Consultez le *Guide d'installation de Content Gateway*. Pendant la procédure d'installation, les conditions suivantes doivent être respectées :
   - Le nom de cluster que vous affectez au nouveau nœud est bien celui du cluster existant.
   - Les ports affectés au nouveau nœud sont bien les mêmes que ceux utilisés par les autres nœuds du cluster.
   - Vous devez ajouter des adresses en multidiffusion et des paramètres d'itinéraire en multidiffusion.
3. Redémarrez Content Gateway. Voir *Démarrage et arrêt de Content Gateway via la ligne de commande*, page 17.

Si vous avez déjà une installation Content Gateway et que vous souhaitez ajouter ce serveur au cluster, il est inutile de réinstaller Content Gateway dans le nœud. Il suffit de modifier les variables de configuration dans le nœud Content Gateway existant.

1. Dans le nœud à ajouter au cluster, ouvrez le fichier **records.config** situé dans le répertoire **/opt/WCG/config**.

2. Modifiez les variables suivantes :

Variable	Description
proxy.local.cluster.type	Spécifiez le mode de clustering : 2 = mode gestion 3 = aucun clustering
proxy.config.proxy_name	Spécifiez le nom du cluster Content Gateway. Tous les nœuds de ce cluster doivent utiliser le même nom.
proxy.config.cluster. mc_group_addr	Spécifiez l'adresse de multidiffusion pour les communications du cluster. Tous les nœuds de ce cluster doivent utiliser la même adresse de multidiffusion.
proxy.config.cluster.rsport	Spécifiez le port de service fiable. Ce port sert à échanger des données entre les nœuds du cluster. Tous les nœuds de ce cluster doivent utiliser le même port de service fiable. La valeur par défaut est 8087.
proxy.config.cluster.mcport	Spécifiez le port de multidiffusion. Ce port est utilisé pour l'identification des nœuds. Tous les nœuds du cluster doivent utiliser le même port de multidiffusion. Le numéro de port par défaut est le 8088.
proxy.config.cluster. ethernet_interface	Spécifiez l'interface réseau à utiliser pour le trafic du cluster. Tous les nœuds de ce cluster doivent utiliser la même interface réseau.

3. Enregistrez et fermez le fichier.
4. Redémarrez Content Gateway (**/opt/WCG/WCGAdmin restart**).

Pour passer du mode Gestion au mode Nœud unique et vice versa :

1. Accédez à Content Gateway Manager.
2. Ouvrez l'onglet **Configurer> Mon proxy> De base> Clustering**.
3. Dans la zone **Type de cluster**, sélectionnez le type approprié (**Single (Unique)** ou **Management (Gestion)**).
4. Cliquez sur **Appliquer**.
5. Cliquez sur **Redémarrer** dans **Configurer> Mon proxy> De base> Général**.

Retrait de nœuds dans un cluster

Dans le nœud que vous souhaitez retirer du cluster :

1. Ouvrez l'onglet **Configurer > Mon proxy > De base > Clustering**.
2. Dans la zone **Type de cluster**, sélectionnez **Single Node (Nœud unique)**.
3. Cliquez sur **Appliquer**.
4. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Basculement IP virtuel

Grâce à la fonction Basculement IP virtuel, Content Gateway conserve un pool d'adresses IP virtuelles qu'il affecte aux nœuds du cluster en fonction des besoins. Ces adresses sont virtuelles seulement parce qu'elles ne sont pas liées à un ordinateur spécifique ; Content Gateway peut les affecter à n'importe lequel de ses nœuds. Pour le monde extérieur, ces adresses IP virtuelles sont les adresses des serveurs Content Gateway.

Le basculement IP virtuel garantit que, si un nœud du cluster tombe en panne, les autres nœuds peuvent prendre le relais et assumer les tâches de celui qui est défaillant. Content Gateway gère le basculement IP virtuel de plusieurs manières :

- Le processus **content_manager** entretient la communication avec le cluster. Les nœuds échangent automatiquement des statistiques et les informations de configuration via une communication en multidiffusion. Si les requêtes de pulsation multidiffusées ne parviennent pas jusqu'à l'un des nœuds du cluster, les autres nœuds s'aperçoivent que ce nœud n'est pas disponible.
- Le processus **content_manager** réaffecte les adresses IP du nœud défaillant aux autres nœuds opérationnels en environ 30 secondes. Ainsi, le service continue de fonctionner sans interruption.
- Les adresses IP sont affectées aux nouvelles interfaces réseau, et ces nouvelles affectations sont diffusées au réseau local. Cette réaffectation s'effectue via un processus appelé *ARP rebinding* ou Reliaison ARM.

Adresses IP virtuelles - Définition

Rubriques connexes :

- *Activation et désactivation de l'adressage IP virtuel*, page 84
- *Ajout et modification d'adresses IP virtuelles*, page 84

Les adresses IP virtuelles sont des adresses IP qui ne sont pas attribuées à des ordinateurs spécifiques. Elles peuvent passer d'un nœud à l'autre au sein d'un cluster Content Gateway.

Il est courant d'avoir un seul ordinateur pour plusieurs adresses IP dans le même sous-réseau. Cet ordinateur doit avoir une adresse IP principale ou réelle reliée à sa carte d'interface, et il dessert également de nombreuses autres adresses virtuelles.

Vous pouvez faire en sorte que votre base d'utilisateurs se serve d'un mécanisme de pointage DNS circulaire pour accéder aux adresses IP virtuelles, au lieu d'utiliser les véritables adresses IP des ordinateurs Content Gateway.

Les adresses IP virtuelles n'étant pas reliées aux ordinateurs, tout cluster Content Gateway peut récupérer les adresses des nœuds inactifs et les redistribuer aux nœuds restants qui sont actifs.

À l'aide d'un protocole de gestion propriétaire, les nœuds Content Gateway échangent leur statut avec leurs pairs. Si un nœud tombe en panne, ses pairs s'en aperçoivent et négocient pour savoir lequel des nœuds restants va masquer cette défaillance en récupérant l'interface virtuelle du nœud en panne.

Activation et désactivation de l'adressage IP virtuel

1. Ouvrez l'onglet **Configurer > Mon proxy > De base > Général**.
2. Sous la section Networking (Mise en réseau), dans le tableau Features (Fonctions), sélectionnez **On (Activé)** ou **Off (Désactivé)** pour **Virtual IP (IP virtuelle)** afin d'activer ou de désactiver l'adressage IP virtuel.
3. Cliquez sur **Appliquer**.
4. Cliquez sur **Restart (Redémarrer)** dans **Configurer > Mon proxy > De base > Général** afin de redémarrer Content Gateway dans tous les nœuds du cluster.

Ajout et modification d'adresses IP virtuelles

Comme toutes les adresses IP, les adresses IP virtuelles doivent être réservées au préalable, avant de pouvoir être affectées à Content Gateway.

Avertissement

Un adressage IP incorrect peut désactiver votre système. Assurez-vous de bien comprendre le fonctionnement des adresses IP virtuelles avant de les modifier.

1. Accédez à **Configurer** > **Networking (Mise en réseau)** > **Virtual IP (IP virtuelle)**.

   La zone **Virtual IP Addresses (Adresses IP virtuelles)** affiche toutes les adresses IP virtuelles gérées par Content Gateway.

Remarque

Le bouton Virtual IP (IP virtuelle) s'affiche uniquement si vous avez activé l'option Virtual IP (IP virtuelle) dans le tableau des fonctions dans **Configurer > Mon proxy > De base > Général**.

2. Cliquez sur **Edit File (Modifier le fichier)** pour ajouter de nouvelles adresses IP virtuelles ou modifier celles qui existent déjà.
3. Pour modifier une adresse IP virtuelle, sélectionnez-la dans le tableau situé en haut de la page, modifiez les champs fournis, puis cliquez sur **Set (Définir)**.

   Pour supprimer l'adresse IP sélectionnée, cliquez sur **Clear Fields (Effacer les champs)**.

   Pour ajouter une adresse IP virtuelle, spécifiez-la, ainsi que son interface Ethernet et sa sous-interface, dans les champs fournis, puis cliquez sur **Ajouter**.
4. Cliquez sur **Appliquer**, puis sur **Fermer**.
5. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

7 Mise en cache hiérarchique

Websense Content Gateway peut participer aux *Hiérarchies de caches HTTP*, page 85, qui permet aux requêtes non satisfaites par un cache d'être acheminées aux autres caches régionaux, tirant ainsi parti des contenus et de la proximité des autres caches.

Une hiérarchie de caches est composée de plusieurs niveaux de caches qui communiquent entre eux. Content Gateway prend en charge plusieurs types de hiérarchies de caches. Toutes les hiérarchies de caches reconnaissent le concept de *parent* et *enfant*. Un cache parent est un cache plus élevé dans la hiérarchie, auquel le proxy peut transmettre des requêtes. Un cache enfant est un cache pour lequel le proxy est un parent.

Hiérarchies de caches HTTP

Dans une hiérarchie de caches HTTP, si un nœud Content Gateway ne parvient pas à trouver dans son cache l'objet demandé, il peut le rechercher dans un cache parent, qui à son tour peut le rechercher dans les autres caches, avant d'effectuer un nouveau tri pour récupérer cet objet auprès du serveur d'origine.

Vous pouvez configurer un nœud Content Gateway pour qu'il utilise un ou plusieurs caches parents HTTP, de sorte que, si un parent est indisponible, un autre parent peut desservir les requêtes. On appelle ce comportement le basculement des caches parents. Il est décrit à la section *Basculement des caches parents*, page 86.

> **Remarque**
>
> Si vous ne souhaitez pas que toutes les requêtes passent par le cache parent, vous pouvez configurer le proxy pour qu'il achemine certaines requêtes directement au serveur d'origine (par exemple, celles qui contiennent des URL spécifiques). Pour ce faire, définissez des règles de proxy parent dans le fichier de configuration **parent.config**, décrit à la section *Fichier de configuration parent.config*, page 373).

> **Remarque**
>
> Si l'objet demandé est absent du cache parent, ce dernier récupère ce contenu auprès du serveur d'origine (ou dans un autre cache, selon la configuration du cache parent). Le parent met le contenu en cache et en envoie une copie au proxy (son enfant), où ce contenu est mis en cache et envoyé au client.

Basculement des caches parents

Lorsque vous configurez le proxy pour qu'il utilise plusieurs caches parents, il détecte lorsqu'un parent n'est pas disponible et envoie les requêtes non satisfaites à un autre cache parent. Si vous spécifiez plus de deux caches parents, l'ordre dans lequel ils sont interrogés dépend des règles de proxy parent configurées dans le fichier de configuration des parents, décrit à la section *Fichier de configuration parent.config*, page 373. Par défaut, les caches parents sont interrogés dans l'ordre dans lequel ils apparaissent dans le fichier de configuration.

Configuration de Content Gateway pour l'utilisation d'un cache parent HTTP

1. Dans la page **Configurer > Content Routing (Acheminement du contenu) > Hiérarchies > Parenting (Caches parents)**, activez **Parent Proxy (Proxy parent)**.
2. Cliquez sur **Edit File (Modifier le fichier)** pour ouvrir l'éditeur de fichiers de configuration avec le fichier *Fichier de configuration parent.config*.
3. Renseignez les champs fournis, puis cliquez sur **Ajouter**. L'ensemble des champs sont décris à la section *Hiérarchies*, page 290.
4. Cliquez sur **Appliquer**, puis sur **Fermer**.
5. Dans l'onglet **Parenting (Caches parents)**, cliquez sur **Appliquer** pour enregistrer votre configuration.

> **Important**
>
> Exécutez cette procédure dans le proxy *enfant*. Ne modifiez pas le parent.

8 Configuration du cache

Le cache est constitué d'une base de données d'objets haut débit appelée **magasin d'objets**. Ce magasin indexe les objets en fonction de leurs URL et des en-têtes associés, ce qui permet à Websense Content Gateway de stocker, récupérer et desservir des pages Web, et également des portions de pages Web, pour réaliser des économies optimales en termes de bande passante. À l'aide de la gestion des objets, le magasin d'objets peut mettre en cache d'autres versions du même objet, selon la langue utilisée ou le type d'encodage, et stocker des documents de petite ou grande taille, évitant ainsi le gaspillage d'espace disponible. Lorsque le cache est saturé, Content Gateway en retire les données périmées.

Content Gateway tolère les défaillances des disques mis en cache. En cas de panne d'un disque, Content Gateway le désigne comme endommagé et continue à utiliser les disques restants. Une alarme est envoyée à Content Gateway Manager, indiquant quel disque est en panne. En cas de défaillance de la totalité des disques mis en cache, Content Gateway passe en mode proxy uniquement.

Pour la configuration du cache, vous pouvez effectuer les tâches suivantes :

- Ajoutez un disque de cache après l'installation. Voir *Ajout d'un disque de cache après l'installation*, page 88.
- Changez le volume total d'espace disque alloué au cache. Voir *Modification des capacités de mise en cache*, page 89.
- Partitionnez le cache en réservant de l'espace disque pour certains protocoles, serveurs d'origine et domaines. Voir *Partitionnement du cache*, page 91.
- Spécifiez une taille limite pour les objets autorisés dans le cache. Voir *Configuration de la limite de taille des objets mis en cache*, page 93.
- Supprimez tout le contenu du cache. Voir *Effacement du contenu du cache*, page 93.
- Changez la taille du cache de mémoire RAM. Voir *Modification de la taille du cache de mémoire RAM*, page 94.

Cache de mémoire RAM

Content Gateway gère un petit cache de mémoire RAM destiné aux objets populaires. Ce cache de mémoire RAM dessert rapidement la plupart des objets populaires et réduit la charge des disques, en particulier pendant les périodes de fort trafic temporaire. La taille du cache de mémoire RAM peut être configurée. Voir *Modification de la taille du cache de mémoire RAM*, page 94.

Ajout d'un disque de cache après l'installation

Pour ajouter un disque de cache, vous avez besoin des éléments suivants :

- Un disque physique non formaté (créé par l'installation du système d'exploitation). Notez sa taille en octets.
- Un périphérique de caractères brut (créé avec la commande mknod)

L'ajout du périphérique implique de mapper le disque physique avec le périphérique de caractères brut.

La plupart des exemples ci-dessous présentent des commandes pour un disque HP DL360 et son contrôleur RAID. (Tous les disques sont RAID 0.)

1. Configurez le périphérique brut et modifiez ses autorisations :

   ```
   mknod /etc/udev/devices/raw c 162 0

   chmod 600 /etc/udev/devices/raw
   ```

2. Identifiez le nom du périphérique du disque physique qui doit servir de cache, et notez sa taille en octets (vous en aurez besoin ultérieurement) :

   ```
   fdisk -l | grep "^Disk"

   Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
   ```

3. Créez un nœud, changez son propriétaire, puis mappez le nœud brut avec un disque physique. Notez que l'argument final s'incrémente de 1 à chaque ajout de disque :

   ```
   mknod /etc/udev/devices/raw_c0d1 c 162 1 Vous pouvez
   remplacer le nom du périphérique par celui renvoyé par la
   commande fdisk -l.

   chown Websense /etc/udev/devices/raw_c0d1 Utilisez le nom
   de périphérique employé dans l'instruction mknod.

   /usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
   Utilisez le nom de périphérique employé dans
   l'instruction mknod.
   ```

4. Pour que vos modifications prennent effet au redémarrage, ajoutez les mêmes commandes /usr/bin/raw à **/etc/init.d/content_gateway** à la ligne 6 :

   ```
   ...

   case "$1" in

   'start')

   /usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
   Utilisez le nom de périphérique employé dans
   l'instruction mknod.

   ...
   ```

5. Ajoutez ces périphériques au fichier de configuration **/opt/WCG/config/storage.conf** en utilisant le nœud brut et la taille en blocs renvoyée par la commande **fdisk -l** :

   ```
   /etc/udev/devices/raw_c0d1 146778685440
   Utilisez le nom de périphérique employé dans
   l'instruction mknod.
   ```

6. Vérifiez que la mise en cache est bien activée. Si l'installation n'a configuré aucun disque de cache, la mise en cache sera désactivée :
   a. Dans Content Manager, accédez à **Configurer > Protocoles > HTTP**, puis ouvrez l'onglet **Cacheability (Capacités de mise en cache)**.
   b. Sous **HTTP Caching (Mise en cache HTTP)**, sélectionnez **Enabled (Activé)**.
   c. Cliquez sur **Appliquer**, puis redémarrez Content Gateway.

Modification des capacités de mise en cache

La taille de cache disque maximale agrégée est limitée à 147 Go. Cette taille permet une exploitation optimale des ressources système, tout en fournissant un excellent confort d'utilisation.

La taille minimale d'un cache disque est de 2 Go.

Rubriques connexes :

- *Interrogation de la taille du cache*, page 89
- *Augmentation des capacités de mise en cache*, page 89
- *Réduction des capacités de mise en cache*, page 90

Interrogation de la taille du cache

Pour afficher la taille configurée du cache agrégé, ouvrez Content Manager et accédez à **Monitor (Surveiller) > Subsystems (Sous-systèmes) > Cache**. La taille du cache s'affiche, en octets, dans la colonne **Current Value (Valeur actuelle)** du champ **Cache Size (Taille du cache)**.

Vous pouvez également afficher la taille du cache avec la commande suivante, exécutée à partir du répertoire **bin** de Content Gateway (**/opt/WCG/bin**).

```
content_line -r proxy.process.cache.bytes_total
```

Augmentation des capacités de mise en cache

Pour augmenter l'espace disque total alloué à la mise en cache dans les disques existants, ou pour ajouter de nouveaux disques à un nœud Content Gateway, procédez comme suit :

1. Arrêtez Content Gateway. Voir *Démarrage et arrêt de Content Gateway via la ligne de commande*, page 17.
2. Ajoutez du matériel, si nécessaire.
   a. Configurez le périphérique brut et modifiez ses autorisations. Par exemple :

      ```
      mknod /etc/udev/devices/raw c 162 0
      ```

      ```
      chmod 600 /etc/udev/devices/raw
      ```

b. Identifiez le nom du périphérique physique qui doit servir de cache, et notez sa taille en octets (vous en aurez besoin ultérieurement). Par exemple :

```
fdisk -l | grep "^Disk"

Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
```

c. Pour chaque disque physique, créez un nœud, changez son propriétaire, puis mappez le nœud brut avec un disque physique. Notez que l'argument final s'incrémente de 1 à chaque ajout de disque.

Pour créer un nœud :

```
mknod /etc/udev/devices/raw_c0d1 c 162 1
```

Vous pouvez remplacer le nom du périphérique par celui renvoyé par la commande **fdisk -l** à l'étape b.

Pour modifier le propriétaire :

```
chown Websense /etc/udev/devices/raw_c0d1
```

Le propriétaire est l'utilisateur de l'installation (Websense par défaut). Utilisez le nom de périphérique employé dans l'instruction mknod.

Pour mapper le nœud brut avec un disque physique :

```
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

Utilisez le nom de périphérique employé dans l'instruction mknod.

d. Ajoutez les mêmes commandes **/usr/bin/raw** au fichier **/etc/init.d/content_gateway** afin que vos modifications prennent effet au redémarrage. Par exemple, à la ligne 6, ajoutez :

```
...
case "$1" in
'start')
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

3. Modifiez le fichier **storage.config** dans le répertoire **config** de Content Gateway (**/opt/WCG/config**) pour augmenter le volume d'espace disque alloué au cache dans les disques existants, ou pour ajouter de nouveaux disques. Voir *Fichier de configuration storage.config*, page 447.
4. Redémarrez Content Gateway.

Réduction des capacités de mise en cache

Vous pouvez réduire le volume total d'espace disque alloué au cache dans un disque existant, ou retirer des disques d'un nœud Content Gateway.

1. Arrêtez Content Gateway.
2. Retirez du matériel, si nécessaire.
3. Modifiez le fichier **storage.config** pour réduire le volume d'espace disque alloué au cache dans les disques existants, ou supprimer la référence au matériel que vous retirez du système. Voir *Fichier de configuration storage.config*, page 447.
4. Si vous retirez un disque, vous devez modifier le fichier **/etc/rc.d/init.d/content_gateway** pour supprimer le disque brut relié à ce disque.

5. Redémarrez Content Gateway.

> **Important**
> Dans le fichier **storage.config**, tout disque brut ou formaté doit avoir une capacité minimale de 2 Go.

Partitionnement du cache

Vous pouvez gérer l'espace dédié au cache plus efficacement et limiter l'exploitation des disques en créant des partitions de cache de différentes tailles pour chaque protocole. Vous pouvez encore configurer davantage ces partitions pour y stocker des données provenant de certains serveurs d'origine et de certains domaines.

> **Important**
> HTTP est le seul protocole pris en charge pour l'instant.

> **Important**
> La configuration du partitionnement doit être identique dans tous les nœuds d'un cluster.

Création de partitions de cache pour certains protocoles

Vous pouvez créer des partitions distinctes pour votre cache. Leur taille de stockage peut varier en fonction du protocole. Cette configuration garantit qu'un certain volume d'espace disque est toujours disponible pour un protocole donné.

> **Important**
> HTTP est le seul protocole pris en charge pour l'instant.

Dans Content Gateway Manager :

1. Accédez à l'onglet **Configurer** > **Subsystems (Sous-systèmes)** > **Cache** > **Partition**.
2. Dans la zone **Cache Partition (Partition du cache)**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir l'éditeur de fichiers de configuration avec le fichier **partition.config**.
3. Renseignez les champs fournis, puis cliquez sur **Ajouter**. L'ensemble des champs sont décris à la section *Cache*, page 313.
4. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis cliquez sur **Fermer**.

Modification de la taille des partitions et protocoles

Après avoir configuré vos partitions de cache en fonction du protocole, vous pouvez modifier cette configuration à tout moment. Avant de procéder à des modifications, notez les éléments suivants :

- Vous devez arrêter Content Gateway avant de changer la taille des partitions de cache et les attributions de protocole.
- Lorsque vous augmentez la taille d'une partition, son contenu n'est **pas** supprimé. Toutefois, lorsque vous réduisez la taille d'une partition, son contenu **est** supprimé.
- Vous pouvez modifier le numéro d'une partition. Elle est alors supprimée, puis recréée, même si sa taille et son type de protocole restent identiques.
- Lorsque vous ajoutez de nouveaux disques à votre nœud Content Gateway, les tailles des partitions spécifiées en pourcentage augmentent proportionnellement.
- Trop de changements de la taille des partitions peut entraîner une fragmentation des disques, ce qui altère les performances et les taux d'accès au cache. Il est recommandé d'effacer le contenu du cache (voir *Effacement du contenu du cache*, page 93) avant de modifier radicalement la taille de ses partitions.

Partitionnement du cache en fonction du serveur d'origine ou du domaine

Après avoir partitionné le cache en fonction de sa taille et de son protocole, vous pouvez affecter les partitions créées à certains serveurs d'origine et domaines.

Vous pouvez affecter une partition à un seul serveur d'origine ou à plusieurs. Cependant, si une partition est affectée à plusieurs serveurs d'origine, le volume d'espace disponible pour chaque serveur d'origine n'est pas garanti dans cette partition. Du contenu est stocké dans la partition en fonction de sa popularité.

Outre l'affectation de partitions à certains serveurs d'origine et domaines, vous pouvez affecter une partition générique pour stocker le contenu provenant de tous les serveurs d'origine et domaines qui ne sont pas énumérés dans la liste. Cette partition générique est également utilisée en cas de corruption des partitions d'un serveur d'origine ou d'un domaine particulier.

Important

Si vous n'affectez pas de partition générique, Content Gateway s'exécute en mode proxy uniquement.

Remarque

Avant d'affecter des partitions à certains hôtes ou domaines, vous n'avez **pas** besoin d'arrêter Content Gateway. Toutefois, ce type de configuration prend beaucoup de temps et peut provoquer un pic d'exploitation de la mémoire. Il est recommandé de configurer l'affectation des partitions pendant les périodes de faible trafic.

Vous pouvez partitionner le cache en fonction du nom d'hôte et du domaine dans Content Gateway Manager.

Dans Content Gateway Manager :

1. Configurez les partitions du cache selon la taille et le protocole, comme décrit à la section *Fichier de configuration partition.config*, page 376.

   Vous devez créer une partition distincte en fonction du protocole (HTTP uniquement) de chaque hôte et domaine, et une partition générique supplémentaire à utiliser pour le contenu n'appartenant pas à ces serveurs d'origine et domaines. Par exemple, si vous souhaitez isoler les contenus provenant de deux différents serveurs d'origine, vous devez avoir au moins trois partitions distinctes : une partition HTTP pour chaque serveur d'origine et une partition générique pour tous les autres serveurs d'origine non énumérés dans la liste (ces partitions ne doivent pas obligatoirement être de la même taille).
2. Dans l'onglet **Configurer**, cliquez sur **Subsystems (Sous-systèmes)**, puis sur **Cache**.
3. Ouvrez l'onglet **Hosting (Hébergement)** et, dans la zone **Cache Hosting (Hébergement du cache)**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir l'éditeur de fichiers de configuration avec le fichier **hosting.config**.
4. Renseignez les champs fournis, puis cliquez sur **Ajouter**. L'ensemble des champs sont décris à la section *Cache*, page 313.
5. Cliquez sur **Appliquer**, puis sur **Fermer**.

Configuration de la limite de taille des objets mis en cache

Par défaut, Content Gateway autorise des objets de toutes tailles dans le cache. Vous pouvez modifier ce comportement par défaut et spécifier une taille limite pour les objets mis en cache.

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Cache > Général**.
2. Dans le champ **Maximum Object Size (Taille maximale des objets)**, entrez la taille maximale autorisée (en octets) pour les objets mis en cache. Si vous ne souhaitez pas fixer de limite de taille, entrez 0 (zéro).
3. Cliquez sur **Appliquer**.

Effacement du contenu du cache

Lorsque vous effacez le cache, vous retirez toutes les données de la totalité du cache, ce qui inclut le contenu de la base de données des hôtes. Effacez le cache avant d'exécuter certaines tâches de configuration du cache, telles que son partitionnement.

> **Remarque**
> Vous ne pouvez pas effacer le contenu du cache lorsque Content Gateway est en exécution.

1. Arrêtez Content Gateway. Voir *Démarrage et arrêt de Content Gateway via la ligne de commande*, page 17.

2. Pour effacer le cache, entrez la commande suivante :

   ```
   content_gateway -Cclear
   ```

   Avertissement
   La commande **clear** supprime toutes les données présentes dans le magasin d'objets et la base de données des hôtes. Content Gateway ne vous invite **pas** à confirmer cette suppression.

3. Redémarrez Content Gateway.

Modification de la taille du cache de mémoire RAM

Content Gateway fournit un cache de mémoire RAM dédié à la récupération rapide des petits objets populaires. La taille par défaut de ce cache de mémoire RAM est calculée en fonction du nombre et de la taille des partitions configurées pour le cache. Vous pouvez augmenter la taille du cache de mémoire RAM afin d'améliorer les performances des taux d'accès au cache.

Avertissement
Si vous augmentez la taille du cache de mémoire RAM et que vous constatez une baisse des performances de Content Gateway (par exemple de plus longs délais d'attente), le système d'exploitation peut avoir besoin de plus de mémoire pour ses ressources réseau. Ramenez la taille du cache de mémoire RAM à sa précédente valeur.

Remarque
Si vous avez partitionné votre cache en fonction du protocole ou des hôtes, la taille du cache de mémoire RAM de chaque partition est proportionnelle à la taille de cette partition.

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Cache > Général**.
2. Dans le champ **Ram Cache Size (Taille du cache de mémoire RAM)**, entrez le volume d'espace (en méga-octets) à allouer au cache de mémoire RAM. Bien que l'interface utilisateur accepte des valeurs supérieures, **ne dépassez pas les 512 Mo**.

   La taille par défaut est de 104 857 600 (100 Mo).

   Remarque
   La valeur « -1 » indique à Content Gateway de dimensionner automatiquement le cache de mémoire RAM sur environ 1 Mo par Go de cache disque.

3. Cliquez sur **Appliquer**.
4. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

9 Mise en cache du proxy DNS

Généralement, pour résoudre les noms d'hôte, les clients envoient des requêtes DNS à un serveur DNS. Toutefois, ces serveurs DNS sont souvent surchargés ou éloignés géographiquement des clients ; c'est pourquoi les recherches DNS peuvent être lentes et provoquer des goulots d'étranglement au lieu de satisfaire les requêtes.

L'option de mise en cache du proxy DNS permet à Content Gateway de résoudre les requêtes DNS au nom des clients. Cette option décharge les serveurs DNS distants et réduit les délais de réponse des recherches DNS.

> **Important**
> Vous ne pouvez utiliser l'option de mise en cache du proxy DNS qu'avec un commutateur de niveau 4 ou un routeur Cisco exécutant WCCP v2.

La présentation suivante montre comment Content Gateway répond à une requête DNS.

1. Un client envoie une requête DNS. Cette requête est interceptée par un routeur ou un commutateur de niveau 4 qui est configuré pour rediriger tout le trafic DNS vers Content Gateway via le port 53.
2. Le module ARM examine le paquet DNS. Si la requête DNS est de **type A** (une réponse), le module ARM transmet la requête à Content Gateway. Le module ARM transmet toutes les requêtes DNS qui ne sont pas de **type A** au serveur DNS.
3. Content Gateway vérifie le contenu de son cache DNS pour savoir s'il dispose du nom d'hôte correspondant à l'adresse IP de cette requête DNS. Si cette correspondance est présente dans son cache DNS, Content Gateway envoie l'adresse IP au client. Si cette correspondance est absente de son cache DNS, Content Gateway contacte le serveur DNS pour résoudre ce nom d'hôte. Lorsque Content Gateway reçoit la réponse du serveur DNS, il met en cache le nom d'hôte correspondant à l'adresse IP et envoie cette adresse au client. Si la recherche circulaire (round-robin) est utilisée, Content Gateway envoie la liste complète des correspondances d'adresses IP au client et respectant à la lettre l'ordre de la recherche circulaire.

> **Remarque**
> Si le nom d'hôte correspondant à l'adresse IP est absent du cache DNS, Content Gateway contacte le serveur DNS désigné dans le fichier **/etc/resolv.conf**. Il ne doit pas s'agir du même serveur DNS que celui destiné à recevoir la requête DNS à l'origine.

Le cache DNS est conservé en mémoire et sauvegardé sur disque. Content Gateway met les données sur disque à jour toutes les 60 secondes. La durée de vie (TTL, time-to-live) est strictement respectée pour chaque correspondance nom d'hôte/adresse IP.

Configuration de la mise en cache du proxy DNS

Pour configurer Content Gateway en tant que cache du proxy DNS :

- Ajoutez une règle de redéfinition des correspondances dans le fichier **ipnat.conf**.
- Activez l'option du proxy DNS et spécifiez le port que Content Gateway utilisera pour le trafic du proxy DNS.

Important

Vous ne pouvez utiliser l'option de mise en cache du proxy DNS qu'avec un commutateur de niveau 4 ou un routeur Cisco exécutant WCCP v2.

Dans Content Gateway Manager :

1. Accédez à l'onglet **Configurer > Networking (Mise en réseau) > ARM > Général**.
2. Dans la section **Network Address Translation (NAT) (Traduction d'adresses réseau)**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **ipnat.conf** dans l'éditeur de fichiers de configuration.
3. Renseignez les champs fournis :
   - Dans le champ **Interface Ethernet**, entrez l'interface Ethernet Content Gateway qui doit recevoir les requêtes DNS des clients. Par exemple, eth0.
   - Dans la liste déroulante **Type de connexion**, sélectionnez **udp**.
   - Dans le champ **Original Destination IP (Adresse IP de destination originale)**, entrez **0.0.0.0** pour accepter les requêtes DNS de tous les clients.
   - Dans le champ **Original Destination CIDR (CIDR de destination originale)** (facultatif), entrez la valeur du masque CIDR (Classless Internet Domain Routing). Si vous avez spécifié 0.0.0.0 dans le champ Adresse IP de destination originale, entrez '0' ici.
   - Dans le champ **Original Destination Port (Port de destination originale)**, entrez le numéro du port via lequel les requêtes DNS sont envoyées à Content Gateway. Le port par défaut est le 53.
   - Dans le champ **Local Client IP (Adresse IP locale du client)**, entrez l'adresse IP de Content Gateway.
   - Dans le champ **Local Client Port (Port local du client)**, entrez le numéro du port utilisé par Content Gateway pour communiquer avec le serveur DNS. Le port par défaut est le 5353.
   - Dans la liste déroulante **User Protocol (Protocole utilisateur)**, sélectionnez **dns**.

4. Cliquez sur **Ajouter**, sur **Appliquer**, puis sur **Fermer**.
5. Accédez à **Mon proxy** > **De base** et, dans le tableau **Features (Fonctions)**, activez l'option **Proxy DNS** dans la section **Networking (Mise en réseau)**, puis cliquez sur **Appliquer**.
6. Accédez à **Networking (Mise en réseau)** > **Proxy DNS**.
7. Dans le champ **DNS Proxy Port (Port du proxy DNS)**, entrez le numéro du port du proxy DNS. Le port par défaut est le 5353.
8. Cliquez sur **Appliquer**, puis redémarrez Content Gateway.

10 Configuration du système

Plusieurs options de Websense Content Gateway permettent de configurer le système :

- *Content Gateway Manager*, page 99
- *Interface de ligne de commande*, page 103
- *Fichiers de configuration*, page 104
- *Enregistrement et restauration des configurations*, page 105

Il est préférable de redémarrer Content Gateway à chaque modification de la configuration.

Content Gateway Manager

Content Gateway Manager offre une interface de type Web qui permet de configurer Content Gateway.

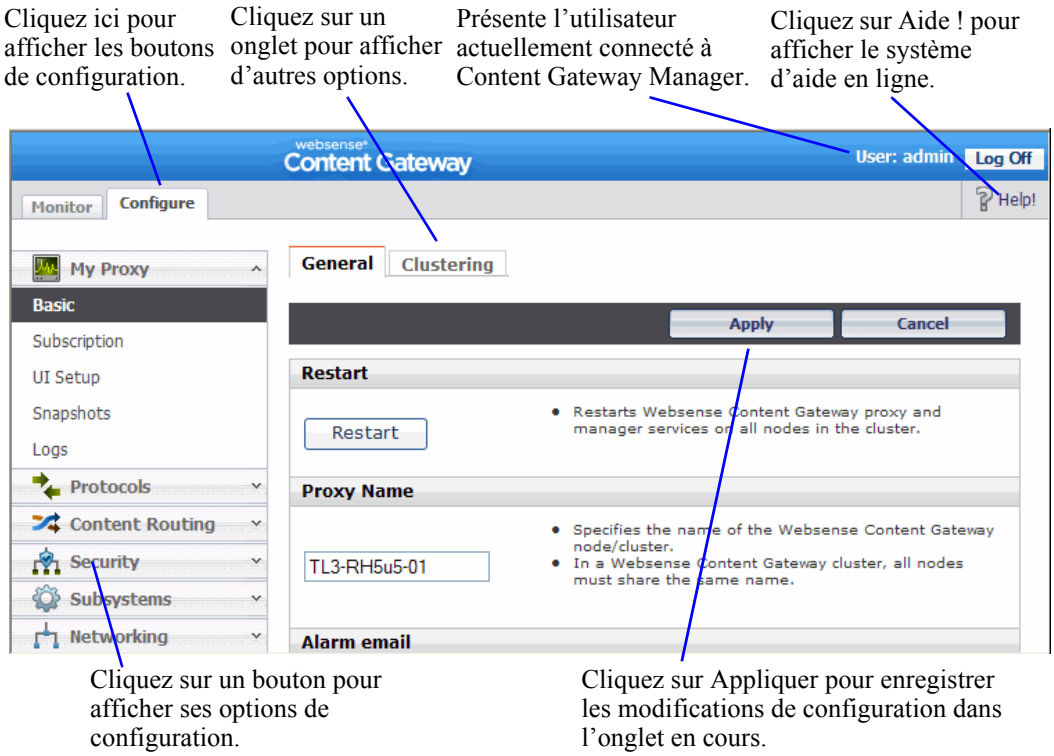
> **Remarque**
> Certaines options ne peuvent être modifiées qu'en éditant les variables de configuration dans le fichier **records.config** ou via l'interface de ligne de commande. Voir *Interface de ligne de commande*, page 103, et *Fichiers de configuration*, page 104.

Pour obtenir des instructions sur la connexion à Content Gateway Manager, consultez la section *Accès à Content Gateway Manager*, page 11.

Utilisation du mode Configuration

Par défaut, Content Gateway Manager s'ouvre en mode Monitor (Surveillance).

Pour afficher les boutons du mode Configuration, ouvrez l'onglet **Configurer**.



En mode Configuration, Content Gateway Manager affiche une suite de boutons. Chaque bouton correspond à un groupe d'options de configuration.

L'ensemble des options de configuration disponibles en mode Configuration sont détaillées à la section *Options de configuration*.

Mon proxy

- Cliquez sur **De base** pour redémarrer le proxy et les services Manager (vous devez redémarrer lorsque vous modifiez certaines options de configuration), identifiez le nom du nœud Content Gateway, définissez une alarme par e-mail, et activez ou désactivez des fonctionnalités (par exemple le traitement FTP, l'authentification des utilisateurs du proxy, WCCP, les options de cluster, etc.).
- Cliquez sur **Abonnement** pour afficher votre clé d'abonnement. Pour plus d'informations sur les clés d'abonnement et les options d'analyse, consultez le système d'aide de Web Security Manager. Si Content Gateway est intégré à Data Security Suite uniquement, saisissez votre clé d'abonnement Data Security dans le champ fourni.
- Cliquez sur **UI Setup (Configuration de l'interface utilisateur)** pour identifier et modifier le port par lequel les navigateurs se connectent à Content Gateway Manager, activer les connexions SSL à Content Gateway Manager, définir la fréquence d'actualisation des statistiques par Content Gateway Manager dans l'onglet Monitor (Surveiller), et configurer les listes de contrôle d'accès et les comptes d'administrateur et d'utilisateur pour sécuriser l'accès à Content Gateway Manager.
- Cliquez sur **Snapshots (Instantanés)** pour créer et restaurer des instantanés de la configuration.
- Cliquez sur **Journaux** pour afficher, supprimer ou copier un fichier journal sélectionné dans le système de fichiers local.

Protocoles

- Cliquez sur **HTTP** pour configurer la mise en cache HTTP et régler les délais d'expiration HTTP.
- Cliquez sur **HTTP Responses (Réponses HTTP)** pour définir les réponses HTTP envoyées aux clients lorsque le proxy détecte un problème HTTP dans une transaction (par exemple des serveurs d'origine indisponibles, une authentification requise et des erreurs de protocole).
- Cliquez sur **HTTP Scheduled Update (HTTP - Mise à jour planifiée)** pour configurer le proxy de sorte qu'il charge des objets spécifiques dans le cache aux moments programmés.
- Cliquez sur **FTP** pour configurer les options FTP et régler les délais d'expiration FTP.
- Les options FTP affectent uniquement les requêtes provenant des clients FTP. Vous pouvez configurer les options qui affectent les requêtes FTP provenant de clients HTTP dans le groupe HTTP. Le bouton FTP ne s'affiche que si vous avez activé le traitement FTP dans le tableau **Features (Fonctions)** sous **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **HTTPS** pour définir les informations sur les ports du trafic HTTPS entrant et sortant.

Routage du contenu

- Cliquez sur **Hiérarchies** pour configurer la mise en cache transparente HTTP.
- Cliquez sur **Mapping and Redirection (Mappage et redirection)** pour définir les règles de correspondances URL et les règles de correspondances FTP.
- Cliquez sur **Browser Auto-Config (Configuration automatique du navigateur)** pour identifier le port utilisé pour télécharger les fichiers de configuration automatique des navigateurs et définir les options PAC et WPAD.

Sécurité

- Cliquez sur **Connection Control (Contrôle des connexions)** pour définir les clients autorisés à accéder au proxy.
- Cliquez sur **FIPS Security (Sécurité FIPS)** pour activer la sécurité FIP 140-2 sur les connexions HTTPS.
- Cliquez sur **Access Control (Contrôle d'accès)** pour définir les règles de filtrage et les options d'authentification du proxy (Authentification Windows intégrée, Authentification dans plusieurs domaines, NTLM hérité, LDAP, RADIUS).
- Cliquez sur **Data Security (Sécurité des données)** pour vous enregistrer auprès du serveur Data Security Management Server et activer le moteur de stratégie Data Security local.
- Cliquez sur **SOCKS** pour configurer Content Gateway afin qu'il utilise un pare-feu SOCKS. Le bouton SOCKS ne s'affiche que si vous avez activé SOCKS dans le tableau Features (Fonctions) sous **Configurer > Mon proxy > De base > Général**.

Remarque

Un serveur SOCKS est intégré à Content Gateway lorsque ce dernier est installé dans un dispositif Websense V-Series.

Lorsque Content Gateway est installé sous forme de logiciel dans un serveur distinct, **aucun** serveur SOCKS intégré n'est fourni. Pour utiliser SOCKS, un serveur SOCKS distinct doit être présent.

Sous-systèmes

- Cliquez sur **Cache** pour activer ou désactiver l'épinglage du cache, configurer la taille du cache de mémoire RAM, définir la taille maximale des objets autorisés dans le cache et partitionner votre cache en fonction du protocole et des serveurs d'origine.
- Cliquez sur **Journalisation** pour activer ou désactiver la journalisation des événements et définir les options de configuration de la journalisation.

Mise en réseau

- Cliquez sur **Connection Management (Gestion des connexions)** pour spécifier :
  - Le nombre maximal de connexions que peut accepter le proxy.
  - Pour la mise en cache du proxy transparent, définissez le nombre maximal de connexions de clients autorisées avant que le proxy ne commence à transmettre les requêtes entrantes directement au serveur d'origine.
  - Le nombre maximal de connexions simultanées et les clients autorisés à ne pas respecter ces limites.
- Cliquez sur **ARM** pour définir les règles de redirection régissant le réadressage des paquets entrants en mode transparent. Vous pouvez également définir des règles de contournement dynamique et statique.
- Cliquez sur **WCCP** pour définir les paramètres de configuration WCCP. Le bouton WCCP ne s'affiche que si vous avez activé WCCP dans le tableau Features (Fonctions) dans l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **Proxy DNS** pour définir le port du proxy DNS. Le bouton Proxy DNS ne s'affiche que si vous avez activé l'option Proxy DNS dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **DNS Resolver (Résolveur DNS)** pour activer ou désactiver l'extension du domaine local, régler les délais d'expiration de la base de données des hôtes et configurer les options Split DNS (Diviser DNS).
- Cliquez sur **Virtual IP (Adresse IP virtuelle)** pour activer ou désactiver le basculement IP virtuel et spécifier les adresses IP virtuelles gérées par le nœud Content Gateway. Le bouton Virtual IP (Adresse IP virtuelle) ne s'affiche que si vous avez activé l'option Virtual IP dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.

SSL

- Cliquez sur **Certificats** pour afficher l'arborescence des autorités de certification. Cliquez sur une entrée pour afficher les détails de ce certificat.
- Cliquez sur **Decryption/Encryption (Décryptage/Cryptage)** pour configurer le mode de gestion du trafic entrant et sortant par SSL Manager. Le trafic entrant circule du navigateur vers SSL Manager, trajet au cours duquel le contenu est décrypté et inspecté. Le trafic sortant circule de SSL Manager vers le serveur Web de destination SSL Manager vérifie l'état de révocation du certificat du site avant de transmettre les données à nouveau cryptées au site.
- Cliquez sur **Validation** pour configurer la validation du certificat, définir les mesures à prendre lorsque le certificat n'est pas valide, configurer le contournement de la vérification et configurer la gestion des listes de révocation de certificat.

- Cliquez sur **Incidents** pour afficher un rapport présentant les occurrences de réception d'un message d'accès refusé par les clients et identifier les URL que vous souhaitez autoriser, placer dans une liste noire ou détourner.
- Cliquez sur **Client Certificates (Certificats clients)** pour configurer le mode de gestion des requêtes de certificat client par SSL Manager.
- Cliquez sur **Journalisation** pour sélectionner le niveau de journalisation SSL, les détails de la journalisation, et les noms et la gestion des fichiers journaux.
- Cliquez sur **Personnalisation** pour personnaliser le message d'échec de validation de certificat.
- Cliquez sur **Internal Root CA (Autorité de certification racine interne)** pour importer, créer ou sauvegarder l'Autorité de certification racine interne.

Interface de ligne de commande

En alternative à Content Gateway Manager, vous pouvez utiliser l'interface de ligne de commande pour afficher et modifier votre configuration de Content Gateway.

1. Connectez-vous à un nœud Content Gateway en tant qu'utilisateur racine, puis accédez au répertoire ('cd') **bin** de Content Gateway (/opt/WCG/bin).
2. Pour afficher un paramètre de configuration, saisissez la commande suivante :

   ```
   content_line -r var
   ```

   où *var* correspond à la variable associée à l'option de configuration (pour obtenir la liste des variables, consultez la section *Variables de configuration*, page 378).
3. Pour modifier la valeur d'un paramètre de configuration, saisissez la commande suivante :

   ```
   content_line -s var -v valeur
   ```

   où *var* correspond à la variable associée à l'option de configuration et *valeur* à la valeur que vous souhaitez utiliser.

   Par exemple, pour définir l'option d'expiration d'inactivité FTP sur 200 secondes, saisissez la commande suivante, puis appuyez sur la touche Entrée :

   ```
   content_line -s
   proxy.config.ftp.control_connection_timeout -v 200
   ```

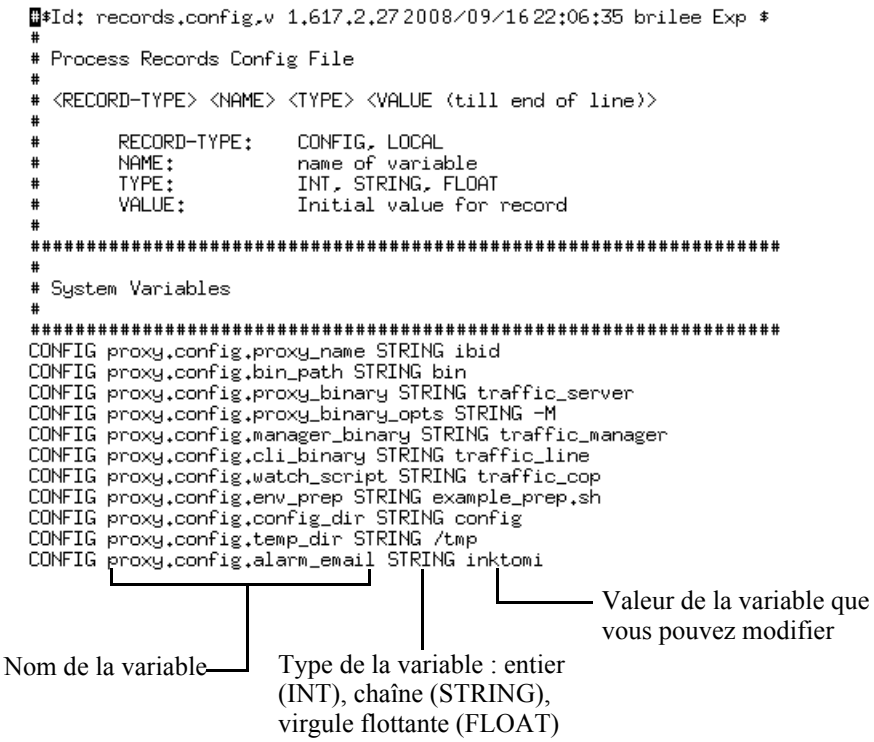
> **Remarque**
> Si le répertoire **bin** de Content Gateway ne fait pas partie de votre chemin, précédez la commande de : ./
>
> Par exemple :
>
> ```
> ./content_line -r variable
> ```

Fichiers de configuration

Vous pouvez modifier les options de configuration de Content Gateway en modifiant des variables spécifiques dans le fichier **records.config**, situé dans **/opt/WCG/config**. Ouvrez le fichier dans un éditeur de texte, (tel que **vi** ou **emacs**) et modifiez la valeur de la variable.

> **Remarque**
>
> Lorsque vous modifiez le fichier **records.config**, Content Gateway doit relire les fichiers de configuration. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**), saisissez la commande suivante :
>
> ```
> content_line -x
> ```
>
> Dans certains cas, le redémarrage du proxy est nécessaire pour que les modifications entrent en vigueur.

La figure ci-dessous présente un exemple d'extrait du fichier **records.config** :



Content Gateway fournit d'autres fichiers de configuration utilisés pour configurer des fonctions spécifiques. Tous les fichiers de configuration sont décris à la section *Fichiers de configuration*, page 345.

Enregistrement et restauration des configurations

La fonctionnalité d'instantané de configuration vous permet d'enregistrer tous les paramètres de configuration existants et de les restaurer si nécessaire. Content Gateway peut stocker les instantanés de configuration dans le nœud sur lequel ils ont été créés, dans un serveur FTP ou un support amovible. Content Gateway peut restaurer un instantané de configuration dans tous les nœuds du cluster.

> **Remarque**
> Nous vous recommandons de créer un instantané de votre configuration avant d'effectuer la maintenance du système ou de tenter de régler les performances du système. La création d'un instantané de configuration ne prend que quelques secondes.

Cette section présente les procédures à suivre pour les tâches suivantes :

- Création d'un instantané de la configuration existante. Voir *Création d'instantanés de configuration*, page 105.
- Restauration d'instantanés de configuration créés précédemment. Voir *Restauration des instantanés de configuration*, page 106.
- Suppression des instantanés de configuration stockés dans le nœud Content Gateway. Voir *Suppression des instantanés de configuration*, page 107.

Création d'instantanés de configuration

Vous pouvez enregistrer tous les paramètres de configuration présents dans votre système Content Gateway via Content Gateway Manager.

Pour créer un instantané de configuration et l'enregistrer dans le système local :

1. Sélectionnez **Configurer > Snapshots (Instantanés) > File System (Système de fichiers)**.
2. Le champ **Change Snapshot Directory (Modifier le répertoire des instantanés)** présente le nom du répertoire dans lequel Content Gateway enregistre les instantanés de la configuration. L'emplacement par défaut est le répertoire **config/snapshots** de Content Gateway. Pour changer de répertoire, entrez le chemin complet dans le champ **Change Snapshot Directory (Modifier le répertoire des instantanés)**. Si vous saisissez un chemin relatif, Content Gateway suppose que ce répertoire est situé dans son répertoire **config**.
3. Dans le champ **Save Snapshot (Enregistrer l'instantané)**, saisissez le nom à utiliser pour la configuration actuelle.
4. Cliquez sur **Appliquer**.

Pour créer un instantané de votre configuration et l'enregistrer sur un serveur FTP :

1. Sélectionnez **Configurer > Snapshots (Instantanés) > FTP Server (Serveur FTP)**.
2. Dans les champs fournis, saisissez le nom du serveur FTP, l'identifiant de connexion et le mot de passe, et le répertoire distant dans lequel le serveur FTP stocke les instantanés de la configuration.
3. Cliquez sur **Appliquer**.

   Une fois que vous êtes connecté au serveur FTP, la page **FTP Server (Serveur FTP)** présente des champs supplémentaires.
4. Dans le champ **Save Snapshot to FTP Server (Enregistrer l'instantané sur le serveur FTP)**, saisissez le nom de l'instantané de configuration que vous souhaitez créer.
5. Cliquez sur **Appliquer**.

Restauration des instantanés de configuration

Si vous exécutez un cluster de serveurs Content Gateway, la configuration est restaurée dans tous les nœuds du cluster.

Pour restaurer un instantané de configuration stocké dans le nœud local :

1. Ouvrez l'onglet **Configurer > Snapshots (Instantanés) > File System (Système de fichiers)**.
2. Dans la liste déroulante **Restaurer > Delete Snapshot (Supprimer un instantané)**, sélectionnez l'instantané de configuration que vous souhaitez restaurer.
3. Cliquez sur **Restore Snapshot from** *nom_répertoire* **Directory** (Restaurer l'instantané à partir du répertoire nom_répertoire).
4. Cliquez sur **Appliquer**.

   Le système Content Gateway ou le cluster utilise la configuration restaurée.

Pour restaurer un instantané de configuration à partir d'un serveur FTP :

1. Sélectionnez **Configurer > Snapshots (Instantanés) > FTP Server (Serveur FTP)**.
2. Dans les champs fournis, saisissez le nom du serveur FTP, l'identifiant de connexion et le mot de passe, et le répertoire distant dans lequel le serveur FTP stocke les instantanés de la configuration.
3. Cliquez sur **Appliquer**.

   Une fois que vous êtes connecté au serveur FTP, l'onglet **FTP Server (Serveur FTP)** présente des champs supplémentaires.
4. Dans la liste déroulante **Restore Snapshot (Restaurer un instantané)**, sélectionnez l'instantané de la configuration que vous souhaitez restaurer.
5. Cliquez sur **Appliquer**.

   Le système Content Gateway ou le cluster utilise la configuration restaurée.

Suppression des instantanés de configuration

1. Sélectionnez **Configurer > Snapshots (Instantanés) > File System (Système de fichiers)**.
2. Dans la liste déroulante **Restaurer > Delete a Snapshot (Supprimer un instantané)**, sélectionnez l'instantané de configuration à supprimer.
3. Cliquez sur **Delete Snapshot from "***nom_répertoire***" Directory** (Supprimer l'instantané à partir du répertoire nom_répertoire).
4. Cliquez sur **Appliquer**.

   L'instantané de configuration est supprimé.

11 Surveillance du trafic

Pour surveiller les performances du système et analyser le trafic réseau, Websense Content Gateway fournit les outils suivants :

- Statistiques présentant les performances de Content Gateway et des informations sur le trafic réseau. Voir *Affichage des statistiques*, page 109. L'interface de ligne de commande est autre moyen d'afficher ces informations. Voir *Affichage des statistiques depuis la ligne de commande*, page 112.
- Alarmes signalant les conditions de défaillance détectées. Voir *Utilisation des alarmes*, page 113.
- Graphiques de performances présentant l'historique des performances de Content Gateway et des informations sur le trafic réseau. Voir *Utilisation des graphiques de performances*, page 115.
- Rapports générés via SSL Manager pour voir l'état des autorités de certification et des incidents. Voir *Création de rapports via SSL Manager*, page 116.

Affichage des statistiques

Servez-vous de Content Gateway Manager pour collecter et interpréter les statistiques relatives aux performances de Content Gateway et au trafic Web. Affichez les statistiques en mode Surveillance.

Pour obtenir des instructions sur la connexion à Content Gateway Manager, consultez la section *Accès à Content Gateway Manager*, page 11.

Utilisation du mode Surveillance

En mode Surveillance, Content Gateway Manager affiche une série de boutons à gauche de l'écran. Cliquez sur un bouton pour afficher les statistiques correspondantes.

Toutes les statistiques affichées en mode Surveillance sont détaillées à la section *Statistiques*, page 235.

Mon proxy

Cliquez sur **Mon proxy** pour afficher les statistiques de Content Gateway.

- Cliquez sur **Summary (Résumé)** pour afficher un récapitulatif de votre système Content Gateway. La partie supérieure de la page présente des informations sur les fonctionnalités de votre abonnement Websense Web Security Gateway, notamment

sur sa date d'expiration. La partie centrale présente des informations sur les moteurs d'analyse utilisés et leurs fichiers de données associés. La partie inférieure de la page contient des statistiques sur les nœuds du proxy, présente tous les nœuds du cluster par nom et surveille les principales statistiques de chaque nœud. Pour afficher des informations détaillées sur un nœud spécifique d'un cluster, cliquez sur le nom de ce nœud dans le tableau Summary (Résumé), puis sur l'un des autres boutons de l'onglet **Monitor (Surveiller)**.

- Cliquez sur **Node (Nœud)** pour afficher des informations sur le nœud sélectionné. Vous pouvez alors voir si le nœud est actif ou inactif, la date et l'heure de démarrage du processus **content_gateway**, des informations sur les performances du cache (taux d'accès aux documents, économie de bande passante et pourcentage d'espace actuellement disponible dans le cache), le nombre de connexions de clients et de serveurs actuellement ouvertes et le nombre de transferts en cours. Vous pouvez également consulter des informations sur la résolution des noms, par exemple le taux d'accès à la base de données des hôtes et le nombre de recherches DNS par seconde.

  Remarque

  Lorsque le nœud fait partie d'un cluster, deux jeux de statistiques s'affichent : Des informations sur le nœud lui-même et des données présentant la valeur moyenne de tous les nœuds du cluster. Cliquez sur le nom d'une statistique pour afficher ses informations au format graphique.

- Cliquez sur **Graphs (Graphiques)** pour afficher les statistiques présentées dans la page **Node (Nœud)** (performances du cache, connexions et transfert en cours, réseau et résolution de noms) au format graphique. Vous pouvez afficher plusieurs statistiques dans un même graphique.

  Pour afficher une statistique particulière au format graphique, cliquez sur la case accolée au nom du graphique en question, puis sur **Graph (Graphique)**. Pour afficher plusieurs statistiques dans un même graphique, cliquez sur la case accolée au nom de chaque graphique à afficher, puis sur **Graph (Graphique)**.

- Cliquez sur **Alarmes** pour afficher les alarmes signalées par Content Gateway. Voir *Utilisation des alarmes*, page 113.

Protocoles

Le bouton Protocoles donne des informations sur les transactions HTTP et FTP.

- Cliquez sur **HTTP** pour afficher des informations sur les vitesses et les transactions HTTP (par exemple les éléments absents du cache, les éléments présents dans le cache, les erreurs de connexion, les transactions annulées) et des informations sur les connexions des clients et des serveurs. Vous pouvez également voir des informations sur les requêtes FTP provenant de clients HTTP, par exemple le nombre de connexions de serveurs FTP ouvertes, le nombre de connexions PASV et PORT réussies et en échec, et le nombre de recherches, d'accès et d'absences dans le cache.
- Cliquez sur **FTP** pour voir les informations relatives aux requêtes FTP provenant de clients FTP.

  Remarque

  Le bouton **FTP** ne s'affiche que si vous avez activé le traitement FTP dans le tableau **Features (Fonctions)** de l'onglet **Configurer > Mon proxy > De base**.

Sécurité

Le bouton Sécurité donne des informations sur l'authentification du proxy et les connexions du serveur SOCKS :

- Cliquez sur **LDAP** pour voir le nombre d'éléments présents et absents dans le cache LDAP, ainsi que le nombre d'erreurs de serveur d'authentification LDAP et d'échecs de tentative d'authentification. Le bouton LDAP ne s'affiche que si vous avez activé l'option LDAP dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **NTLM** pour voir le nombre d'éléments présents et absents dans le cache NTLM, ainsi que le nombre d'erreurs du serveur d'authentification NTLM et d'échecs de tentative d'authentification. Le bouton NTLM ne s'affiche que si vous avez activé l'option NTLM dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **Authentification Windows intégrée** (IWA) pour afficher les compteurs de requêtes négociées, les compteurs de requêtes NTLM et les compteurs de requêtes d'authentification de base. L'onglet IWA ne s'affiche que si vous avez activé l'option IWA dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **SOCKS** pour voir le nombre de connexions au serveur SOCKS réussies et en échec et le nombre de connexions en cours. Le bouton SOCKS ne s'affiche que si vous avez activé l'option SOCKS dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.

Sous-systèmes

Le bouton Sous-systèmes donne des informations sur le cache du proxy, les clusters et la journalisation des événements :

- Cliquez sur **Cache** pour afficher des informations sur le cache du proxy. Déterminez l'espace actuellement utilisé dans le cache, la taille totale du cache en giga-octets, la taille totale du cache de mémoire RAM en octets, le nombre de présences et d'absences dans le cache de mémoire RAM et le nombre de recherches, de lecture d'objets, d'écriture, de mises à jour et de suppression effectuées dans le cache.
- Cliquez sur **Clustering (Mise en cluster)** pour voir le nombre de nœuds présents dans le cluster, le nombre total d'opérations du cluster, le nombre d'octets lus et écrits dans la totalité des nœuds du cluster et le nombre de connexions actuellement ouvertes dans le cluster.
- Cliquez sur **Journalisation** pour voir le nombre de fichiers journaux actuellement ouverts, le volume d'espace actuellement utilisé par les fichiers journaux, le nombre d'événements d'accès et d'événements d'erreur enregistrés dans le journal et le nombre d'événements d'accès ignorés.

Mise en réseau

Le bouton Networking (Mise en réseau) donne des informations sur la configuration réseau du système, le module ARM, les routeurs WCCP, le proxy DNS, la résolution des noms de domaine et l'adressage IP virtuel.

- Cliquez sur **Système** pour voir la configuration réseau du système, notamment le nom d'hôte affecté à l'ordinateur proxy et la passerelle par défaut, le domaine de recherche et les serveurs DNS utilisés par l'ordinateur proxy.

- Cliquez sur **ARM** pour voir des informations sur la Traduction d'adresses réseau et le contournement dynamique.
- Cliquez sur **WCCP** pour voir les statistiques de fragmentation WCCP v2 et la configuration de chaque groupe de services WCCP activé dans le nœud Content Gateway. L'onglet WCCP ne s'affiche que si vous avez activé WCCP dans le tableau Features (Fonctions) dans l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **Proxy DNS** pour voir le nombre total de requête DNS desservies par Content Gateway et le nombre d'absences et de présences dans le cache. Le bouton Proxy DNS ne s'affiche que si vous avez activé l'option Proxy DNS dans le tableau Features (Fonctions) de l'onglet **Configurer > Mon proxy > De base > Général**.
- Cliquez sur **DNS Resolver (Résolveur DNS)** pour voir le nombre total de recherches et d'accès à la base de données des hôtes et le temps moyen des recherches, le nombre total de recherches et le nombre total de recherches réussies dans le serveur DNS.
- Cliquez sur **Virtual IP Address (Adresse IP virtuelle)** pour voir les mappages d'adresses IP virtuelles existants. Le bouton Virtual IP Address (Adresse IP virtuelle) s'affiche uniquement si vous avez activé l'option Virtual IP (IP virtuelle) dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Performances

Le bouton Performances présente des graphiques sur l'historique des performances. Voir *Utilisation des graphiques de performances*, page 115.

Affichage des statistiques depuis la ligne de commande

Vous pouvez utiliser l'interface de ligne de commande pour afficher des statistiques sur les performances de Content Gateway et le trafic Web.

L'interface de ligne de commande vous permet également de configurer, d'arrêter et de redémarrer Content Gateway. Voir *Interface de ligne de commande*, page 103, et *Variables de Websense Content Gateway*, page 260.

Pour afficher des informations spécifiques sur un cluster ou un nœud Content Gateway, spécifiez la variable correspondant à la statistique désirée.

1. Devenez utilisateur racine :

   ```
   su
   ```

2. Connectez-vous à un nœud Content Gateway.
3. Dans le répertoire **bin** de Content Gateway (/opt/WCG/bin), saisissez la commande suivante :

   ```
   content_line -r variable
   ```

   où *variable* correspond à la variable représentant les informations désirées. Vous trouverez la liste des variables disponibles à la section *Variables de Websense Content Gateway*, page 260.

   La commande suivante affiche par exemple le taux d'accès aux documents pour ce nœud :

```
content_line -r proxy.node.http.cache_hit_ratio
```

Remarque

Si le répertoire **bin** de Content Gateway ne fait pas partie de votre chemin, précédez la commande de : ./

Par exemple :

```
./content_line -r variable
```

Utilisation des alarmes

Content Gateway signale une alarme lorsqu'il détecte un problème, par exemple lorsque l'espace affecté aux journaux d'événements devient insuffisant ou lorsqu'il ne parvient pas à écrire dans un fichier de configuration.

Toutes les alarmes ne sont pas critiques. Certaines d'entre elles signalent des conditions temporaires. Par exemple, une alarme **license download failed:4** (échec de téléchargement de licence) peut être due à l'interruption temporaire de la connectivité Internet.

Sélectionnez **Monitor (Surveiller) > Mon proxy > Alarmes** pour voir la liste des alarmes en cours, telles qu'illustrées ci-dessous.

Remarque

Content Gateway envoie également les alarmes sélectionnées à TRITON - Web Security, où elles sont appelées **alertes**. Un résumé des messages d'alerte s'affiche dans la page TRITON - Web Security **Status (État) > Today (Aujourd'hui)**. Les administrateurs de Web Security peuvent configurer quelles conditions de Content Gateway doivent entraîner l'envoi de messages d'alerte et quelles méthodes (e-mail ou SNMP) doivent être utilisées pour envoyer l'alerte dans les pages **Paramètres > Alertes**.

Effacement des alarmes

Lorsque vous avez lu le message d'une alarme, vous pouvez cliquer sur **Effacer** dans la fenêtre du message pour la faire disparaître. La section *Messages d'alarme*, page 455, décrit certains des messages d'alarme générés par Content Gateway.

Important

L'option **Effacer** fait uniquement disparaître les messages d'alarme et n'en résout pas les causes.

Lorsque la même condition d'alarme se produit une seconde fois, elle n'est pas enregistrée lorsque la première alarme n'a pas encore été effacée.

Configuration de Content Gateway pour l'envoi des alarmes par e-mail

1. Ouvrez l'onglet **Configurer> Mon proxy> De base > Général**.
2. Dans le champ **Alarm eMail (Envoyer l'alarme par e-mail)**, saisissez l'adresse électronique à laquelle vous souhaitez envoyer les alarmes. Assurez-vous d'utiliser l'adresse électronique complète, y compris la notation @, par exemple :

   `nomdestinataire@exemple.com`
3. Cliquez sur **Appliquer**.

Utilisation d'un fichier script pour les alarmes

Les messages d'alarme sont intégrés à Content Gateway et ne sont pas modifiables. Vous pouvez toutefois rédiger un script exécutant certaines actions lorsqu'une alarme est signalée.

Vous trouverez un exemple de script nommé **example_alarm_bin.sh** dans le répertoire **/opt/WCG/bin**. Vous pouvez modifier ce fichier.

Utilisation des graphiques de performances

L'outil des graphiques de performances (Multi Router Traffic Grapher) vous permet de surveiller les performances de Content Gateway et d'analyser le trafic réseau. les graphiques de performances donnent des informations sur l'utilisation de la mémoire virtuelle, les connexions des clients, les taux de présences et d'absences dans le cache, etc. Les informations fournies sont enregistrées à partir du démarrage de Content Gateway. Les statistiques sont collectées par intervalles de 5 minutes.

Pour accéder aux graphiques des performances, sélectionnez **Monitor (Surveiller) > Performances**.

Important

Pour exécuter l'outil des graphiques de performances (Multi Router Traffic Grapher), le logiciel Perl version 5.005 ou ultérieure doit être installé dans votre système Content Gateway.

1. Si votre nœud Content Gateway est dans un cluster, sélectionnez le nœud pour lequel vous souhaitez afficher les statistiques dans l'onglet **Monitor (Surveiller) > Mon proxy > Summary (Résumé)**.
2. Dans l'onglet **Monitor (Surveiller)**, cliquez sur **Performances**.
3. Cliquez sur **Overview (Vue d'ensemble)** pour voir un sous-ensemble des graphiques disponibles.

   Cliquez sur **Daily (Quotidien)** pour voir les statistiques du jour.

   Cliquez sur **Weekly (Hebdomadaire)** pour voir les statistiques de la semaine en cours.

   Cliquez sur **Monthly (Mensuel)** pour voir les statistiques du mois en cours.

   Cliquez sur **Yearly (Annuel)** pour voir les statistiques de l'année en cours.
4. Attendez au moins 15 minutes après le démarrage de Content Gateway avant d'afficher les graphiques. L'initialisation des statistiques par l'outil demande plusieurs intervalles de 5 minutes.

Lorsque l'outil MRTG (Multi Router Traffic Grapher) n'a pas été configuré, le système présente un message indiquant qu'il n'est pas disponible. Pour configurer cet outil, procédez comme suit :

1. Vérifiez que Perl 5.005 est bien installé dans votre système.
2. À l'invite de commande, tapez :

   ```
   perl ./pathfix.pl 'which perl'
   ```

   pour être certain que le code binaire de Perl est présent dans votre chemin d'accès (PATH).
3. Accédez au répertoire **bin** de Content Gateway (/opt/WCG/bin).
4. Modifiez l'intervalle de mise à jour de l'outil MRTG en saisissant la commande suivante à l'invite de commande :

   ```
   ./update_mrtg;sleep 5;./update_mrtg;sleep 5;
   ```

   Par défaut, l'intervalle de mise à jour de l'outil MRTG est défini sur 15 minutes. Cette commande le définit sur 5 minutes.

5. Démarrez les mises à jour du code cron de l'outil MRTG :

   ```
   ./mrtgcron start
   ```

6. Attendez 15 minutes environ avant d'accéder aux graphiques des performances dans Content Gateway Manager.

> **Remarque**
> Pour arrêter les mises à jour du code cron de l'outil MRTG, utilisez la commande `./mrtgcron stop`.

Création de rapports via SSL Manager

Vous pouvez demander un rapport détaillant l'état des autorités de certification (voir *Autorités de certification*, page 116) ou la liste des incidents (voir *Incidents*, page 117). Les rapports peuvent être générés au format HTML ou au format séparé par des virgules. Les rapports séparés par des virgules s'affichent sous forme de feuilles de calcul Excel dans SSL Manager.

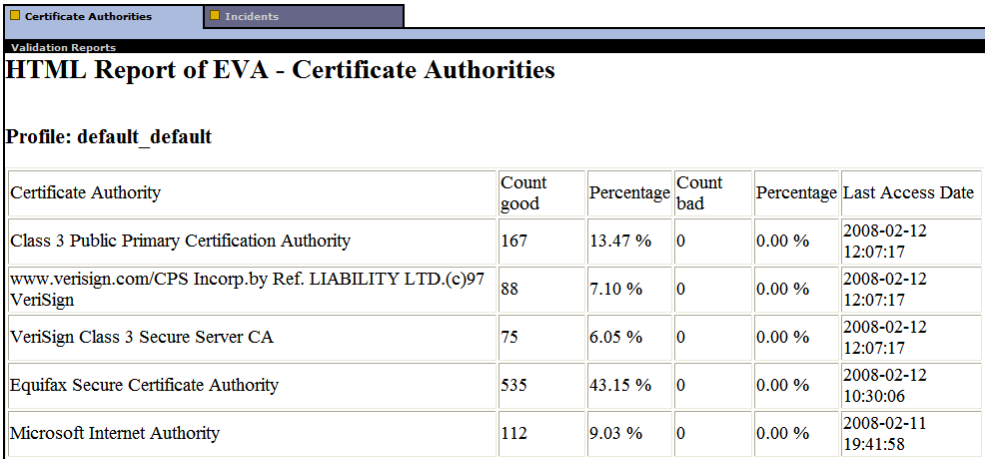
Autorités de certification

1. Ouvrez l'onglet **Monitor (Surveiller) > SSL > Rapports > Autorités de certification**.
2. Sélectionnez le format du rapport.
   a. HTML
   b. CSV (valeurs séparées par une virgule)

      Si vous sélectionnez le format CSV, le rapport prend la forme d'une feuille de calcul Excel.
3. Définissez la période couverte par le rapport.
   a. Un nombre de jours
   b. Une date de début jusqu'au moment présent
   c. Tous les enregistrements du journal
4. Définissez l'ordre de classement du rapport.
   a. Liste des autorités par date
   b. Liste des bonnes réponses OCSP d'abord
   c. Liste des mauvaises réponses OCSP d'abord

   Voir *Actualisation des informations de révocation*, page 151.
5. Cliquez sur **Generate Report (Générer le rapport)** pour obtenir votre rapport.

Le résultat HTML prend l'aspect suivant :



Certificate Authorities | Incidents

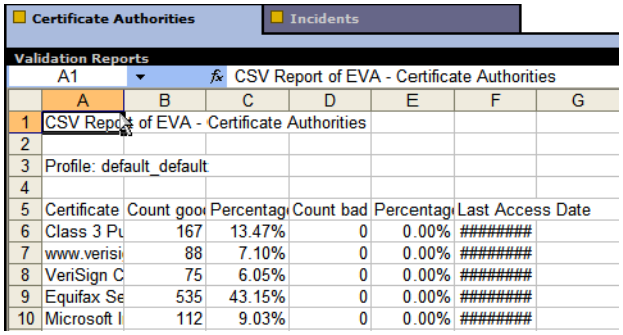
Validation Reports

HTML Report of EVA - Certificate Authorities

Profile: default_default

Certificate Authority	Count good	Percentage	Count bad	Percentage	Last Access Date
Class 3 Public Primary Certification Authority	167	13.47 %	0	0.00 %	2008-02-12 12:07:17
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign	88	7.10 %	0	0.00 %	2008-02-12 12:07:17
VeriSign Class 3 Secure Server CA	75	6.05 %	0	0.00 %	2008-02-12 12:07:17
Equifax Secure Certificate Authority	535	43.15 %	0	0.00 %	2008-02-12 10:30:06
Microsoft Internet Authority	112	9.03 %	0	0.00 %	2008-02-11 19:41:58

Le même rapport au format CSV prend l'aspect suivant :



Certificate Authorities | Incidents

Validation Reports

A1 — CSV Report of EVA - Certificate Authorities

	A	B	C	D	E	F	G
1	CSV Report of EVA - Certificate Authorities						
2							
3	Profile: default_default						
4							
5	Certificate	Count goo	Percentag	Count bad	Percentag	Last Access Date	
6	Class 3 Pu	167	13.47%	0	0.00%	########	
7	www.verisi	88	7.10%	0	0.00%	########	
8	VeriSign C	75	6.05%	0	0.00%	########	
9	Equifax Se	535	43.15%	0	0.00%	########	
10	Microsoft I	112	9.03%	0	0.00%	########	

Remarque

Pour supprimer les données collectées dans les journaux SSL, cliquez sur **Reset all collected data (Réinitialiser toutes les données collectées)**.

Incidents

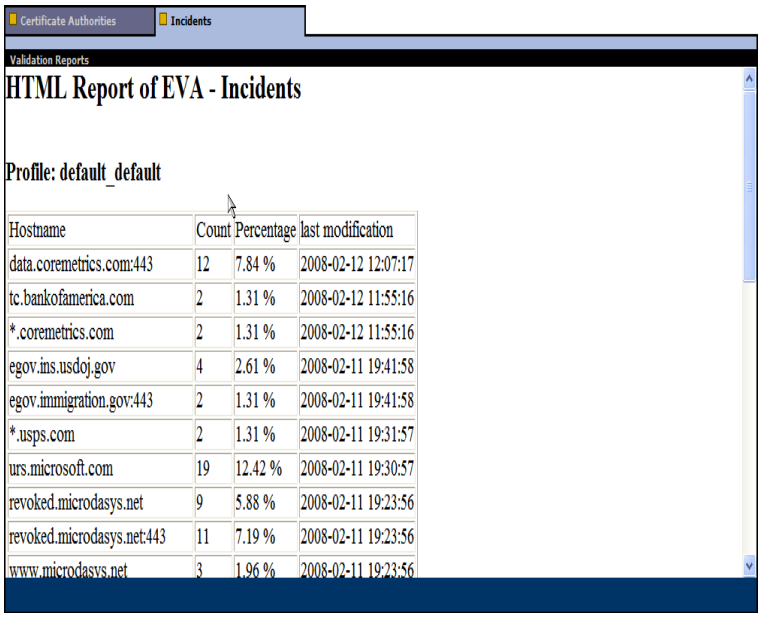
1. Ouvrez l'onglet **Monitor (Surveiller) > SSL > Rapports > Incidents**.
2. Sélectionnez le format HTML ou CSV. Si vous sélectionnez le format CSV, le rapport prend la forme d'une feuille de calcul Excel.
3. Définissez la période que doit couvrir le rapport. Vous pouvez spécifier
   a. Un nombre de jours
   b. Une plage de dates
   c. La période écoulée depuis le déploiement de SSL Manager
4. Définissez l'ordre de classement du rapport.
   a. Liste des incidents par date
   b. Liste des incidents par URL

c. Liste du nombre d'occurrences de chaque incident

Voir *Gestion des accès aux sites Web HTTPS*, page 152.

5. Cliquez sur **Generate Report (Générer le rapport)** pour obtenir votre rapport.

Le résultat HTML prend l'aspect suivant :


Certificate Authorities | Incidents

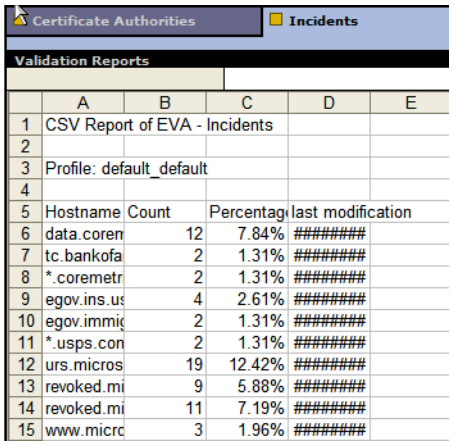
Validation Reports

HTML Report of EVA - Incidents

Profile: default_default

Hostname	Count	Percentage	last modification
data.coremetrics.com:443	12	7.84 %	2008-02-12 12:07:17
tc.bankofamerica.com	2	1.31 %	2008-02-12 11:55:16
*.coremetrics.com	2	1.31 %	2008-02-12 11:55:16
egov.ins.usdoj.gov	4	2.61 %	2008-02-11 19:41:58
egov.immigration.gov:443	2	1.31 %	2008-02-11 19:41:58
*.usps.com	2	1.31 %	2008-02-11 19:31:57
urs.microsoft.com	19	12.42 %	2008-02-11 19:30:57
revoked.microdasys.net	9	5.88 %	2008-02-11 19:23:56
revoked.microdasys.net:443	11	7.19 %	2008-02-11 19:23:56
www.microdasys.net	3	1.96 %	2008-02-11 19:23:56

Le même rapport au format CSV prend l'aspect suivant :


Certificate Authorities | Incidents

Validation Reports

	A	B	C	D	E
1	CSV Report of EVA - Incidents				
2					
3	Profile: default_default				
4					
5	Hostname	Count	Percentag	last modification	
6	data.coren	12	7.84%	########	
7	tc.bankofa	2	1.31%	########	
8	*.coremetr	2	1.31%	########	
9	egov.ins.us	4	2.61%	########	
10	egov.immi	2	1.31%	########	
11	*.usps.con	2	1.31%	########	
12	urs.micros	19	12.42%	########	
13	revoked.mi	9	5.88%	########	
14	revoked.mi	11	7.19%	########	
15	www.micro	3	1.96%	########	

Remarque

Pour supprimer les données collectées dans les journaux SSL, cliquez sur **Reset all collected data (Réinitialiser toutes les données collectées)**.

12 Utilisation de Websense Data Security

Rubriques connexes :

- *Enregistrement et configuration de Data Security*, page 121
- *Configuration du client ICAP*, page 125

Websense Content Gateway fonctionne avec les composants Websense Data Security pour prendre en charge :

- Le tableau de bord Threats (Menaces) de Web Security Gateway
- La prévention contre les pertes de données Web (DLP) et le tableau de bord Threats (Menaces) (Web Security Gateway Anywhere ou Web Security Gateway et un abonnement Data Security complet)

Tableau de bord Threats (Menaces) avec Web Security Gateway

Lorsque Content Gateway est déployé avec Web Security Gateway, plusieurs composants Data Security sont installés dans Content Gateway et les serveurs de gestion TRITON afin de prendre en charge le tableau de bord Web Security Threats (voir l'aide de TRITON – Web Security). Ces composants incluent Data Security Policy Engine (sur l'ordinateur Content Gateway) et Data Security Forensics Repository sur le serveur de gestion TRITON.

Content Gateway s'enregistre auprès de ces composants lorsqu'il est configuré pour la première fois, puis vérifie l'état de l'enregistrement au redémarrage, en se réenregistrant automatiquement si nécessaire.

WebDLP et tableau de bord Threats (Menaces) avec Websense Web Security Gateway Anywhere

Lorsque Content Gateway est déployé avec Web Security Gateway Anywhere (ou avec Web Security Gateway et un abonnement Data Security complet), les capacités incluent les données d'analyse du tableau de bord Threats (Menaces) et la prévention contre les pertes de données (DLP) sur les canaux Web tels que HTTP, HTTPS, FTP et FTP sur HTTP. (Un déploiement complet de Data Security peut étendre Web DLP pour inclure des canaux tels

que les périphériques mobiles, les supports amovibles et les imprimantes. Pour obtenir la description complète de Websense Data Security, consultez la page produit Data Security disponible sur notre site www.websense.com.)

WebDLP, de même que les configurations Data Security étendues, requièrent une installation distincte de TRITON – Data Security et des autres composants Data Security. Avant de configurer Content Gateway pour un fonctionnement avec Data Security, consultez les informations de déploiement et d'installation disponibles dans la Bibliothèque technique de Websense.

Deux méthodes permettent à Content Gateway de fonctionner avec Data Security :

- L'utilisation des composants Data Security prêts à l'emploi installés avec Content Gateway
- Sur ICAP à l'aide des composants Data Security situés dans un hôte distinct (destiné à une utilisation avec Data Security Suite, versions 7.1 et antérieures)

Une seule méthode peut être utilisée à la fois.

Fonctionnement de WebDLP

1. Le proxy intercepte le contenu sortant et le transmet à Data Security.
2. Data Security analyse ce contenu afin de déterminer si la publication Web ou le chargement FTP doit être autorisé ou bloqué.
   - Pour identifier la mesure à prendre, il se base sur la stratégie Data Security.
   - Le résultat est communiqué au proxy.
   - Data Security enregistre la transaction dans un journal.
3. Le proxy agit selon ce qui a été déterminé par Data Security.
   a. Si le contenu est bloqué, il n'est pas transmis à l'hôte distant et Data Security renvoie une page de blocage à l'expéditeur.
   b. Si le contenu est autorisé, il est transmis vers sa destination.

> **Remarque**
>
> Lorsqu'une requête est bloquée et que le serveur DLP envoie une page de blocage en réponse :
>
> - Content Gateway transmet la page de blocage à l'expéditeur dans un message 403 Refusé.
> - La taille de la page de blocage doit dépasser 512 octets, sinon certains agents d'utilisateur (ex. : Internet Explorer) le remplacent par un message d'erreur générique.

Les transactions effectuées sur HTTP, HTTPS, FTP et FTP sur HTTP peuvent être examinées.

Le détail des transactions est enregistré par Data Security, conformément à sa configuration.

Composants Data Security prêts à l'emploi avec Content Gateway

Lors de l'installation de Content Gateway, un petit nombre de composants Data Security sont installés simultanément. Content Gateway s'enregistre auprès de ces composants lorsqu'il est configuré pour la première fois, puis vérifie l'état de l'enregistrement chaque fois qu'il redémarre, en se réenregistrant automatiquement si nécessaire. Pour plus d'informations sur l'enregistrement de Data Security, consultez la section *Enregistrement et configuration de Data Security*, page 121.

Dès que des stratégies Data Security ont été créées et déployées, Content Gateway envoie le contenu (par exemple les publications et les chargements) à Data Security pour analyse et application des stratégies.

Content Gateway collecte et affiche les statistiques des transactions Data Security, par exemple :

- Le nombre total de publications
- Le nombre total de publications analysées
- Le nombre de chargements FTP analysés
- Le nombre de requêtes bloquées
- D'autres données

Pour afficher ces statistiques dans Content Gateway Manager, sélectionnez **Monitor (Surveiller) > Sécurité > Data Security**. La liste complète des statistiques est disponible à la section *Sécurité des données*, page 246.

Data Security sur ICAP

Lorsque le moteur de stratégie Data Security est installé dans un hôte distinct, Content Gateway peut communiquer avec Data Security sur ICAP v1.0. La configuration détaillée est disponible à la section *Configuration du client ICAP*, page 125.

Enregistrement et configuration de Data Security

Rubriques connexes :

- *Configuration du client ICAP*, page 125

La présentation de Websense Data Security est disponible à la section *Utilisation de Websense Data Security*, page 119.

Résumé de l'enregistrement et de la configuration :

- L'enregistrement auprès des composants Data Security prêts à l'emploi est automatique. Aucune configuration n'est nécessaire.

  Websense Web Security collecte automatiquement les données d'analyse du tableau de bord Threats (Menaces).

  En cas d'échec de l'enregistrement, une alarme s'affiche.

- L'enregistrement auprès du serveur de gestion de Data Security est automatique une fois que l'option **Configurer > Mon proxy > De base** > **Data Security > Integrated on-box (Intégration de Data Security prête à l'emploi)** est activée et que Content Gateway a redémarré.

  Content Gateway interroge la console TRITON pour savoir si le serveur de gestion de Data Security est présent.

  La synchronisation de Content Gateway avec le système Data Security Management Server ne prend que quelques minutes.

  L'enregistrement est testé, puis à nouveau tenté si nécessaire, à chaque démarrage de Content Gateway.

  En cas d'échec de l'enregistrement automatique, une alarme s'affiche.

  Important

  Data Security et Content Gateway communiquent par plusieurs ports. Si les Tables IP sont configurées dans le système hôte Content Gateway, ces ports doivent être ouverts dans les Tables IP. Consultez le Guide d'installation de Content Gateway ou l'article de la Bibliothèque technique intitulé « Configuring IPTables for Websense Content Gateway » (Configuration des tables IP pour Websense Content Gateway).

- Les stratégies Web DLP sont configurées dans TRITON – Data Security, à la section **System Modules (Modules système)**. Vous devez **déployer** les stratégies Data Security pour qu'elles entrent en vigueur. Pour plus d'informations, reportez-vous à l'aide de TRITON - Data Security.
- Pour afficher l'état de l'enregistrement dans la page **Monitor (Surveiller) > Summary (Résumé)** de Content Gateway Manager, cliquez sur **More Detail (Détails)** et examinez la liste située au bas de la section **Subscription Details (Détails de l'abonnement)**.
- Les conditions de réussite ou d'échec de l'enregistrement sont consignées dans le journal suivant : /opt/WCG/logs/dss_registration.log

Détails de l'enregistrement et de la configuration

Lorsque vous déployez Web Security Gateway ou Web Security Gateway Anywhere, l'enregistrement auprès du référentiel d'analyses (Forensics Repository) est automatique. Aucune autre configuration n'est nécessaire.

Si vous déployez Web Security Gateway Anywhere pour utiliser Web DLP, vous devez activer l'intégration de Data Security dans Content Gateway Manager :

- Sélectionnez **Configurer > Mon proxy > De base** et activez l'option **Data Security > Integrated on-box (Intégration de Data Security prête à l'emploi)**. Si cette option n'est **pas** activée, l'enregistrement est effectué auprès de Forensics Repository seulement.

  Remarque

  Avant d'activer l'option **Data Security >Integrated on-box (Intégration de Data Security prête à l'emploi)**, vérifiez que les ordinateurs Content Gateway et Data Security Management Server fonctionnent et sont accessibles et que leurs horloges système se synchronisent en quelques minutes.

Une fois l'option **Data Security > Integrated on-box** (Intégration de Data Security prête à l'emploi) activée, l'enregistrement auprès du serveur **Data Security Management Server** est automatique et effectuée au besoin à chaque démarrage de Content Gateway. Pour effectuer cet enregistrement, Content Gateway demande à Websense Web Security Policy Broker les informations nécessaires, y compris l'adresse IP et l'ID du cluster.

Pour afficher l'état de l'enregistrement dans la page **Monitor (Surveiller) > Summary (Résumé)** de Content Gateway Manager, cliquez sur **More Detail (Détails)** et examinez la liste située au bas de la section **Subscription Details (Détails de l'abonnement)**.

Une fois enregistré, Content Gateway utilise le moteur de stratégies Web DLP pour détecter les programmes malveillants. Accédez à TRITON – Data Security pour configurer et déployer des stratégies Web DLP. Vous devez déployer Web DLP dans TRITON – Data Security.

En cas d'échec de l'enregistrement automatique, une alarme s'affiche.

Enregistrement manuel

Lorsque l'option **Data Security > Integrated on-box** (Intégration de Data Security prête à l'emploi) est activée et que Content Gateway a redémarré, vous pouvez tenter un enregistrement manuel en sélectionnant **Configurer > Sécurité > Data Security** (voir ci-dessous).

Le redémarrage de Content Gateway entraîne systématiquement la vérification de l'état de l'enregistrement et, au besoin, une tentative d'enregistrement automatique.

Les conditions de réussite ou d'échec de l'enregistrement sont consignées dans le journal suivant : /opt/WCG/logs/dss_registration.log

Important

Si Content Gateway n'est **pas** dans un dispositif V-Series, l'enregistrement **implique** qu'une adresse IPv4 ait été attribuée au système hôte Content Gateway pour l'interface réseau eth0. Après l'enregistrement, l'adresse IP peut être déplacée vers une autre interface réseau du système. Cependant, cette adresse est utilisée pour le déploiement de la configuration Data Security et doit être disponible tant que les deux modules sont enregistrés.

Enregistrement manuel auprès du serveur Data Security Management Server :

1. Vérifiez que les systèmes Content Gateway et Data Security Management Server fonctionnent et sont accessibles, et que leurs horloges système se synchronisent en quelques minutes.
2. Vérifiez que l'option **Data Security > Integrated on-box** (Intégration de Data Security prête à l'emploi) est activée. Dans Content Gateway Manager, sélectionnez **Configurer > De base > Général**. Dans la liste des **Fonctions**, sous **Networking (Mise en réseau)** localisez **Data Security** et sélectionnez **On (Activé)**, puis **Integrated on-box** (Intégration prête à l'emploi).
3. Cliquez sur le lien **Not registered (Non enregistré)**. L'écran d'enregistrement **Configurer > Sécurité > Data Security** s'affiche.
4. Saisissez l'adresse IP du serveur **Data Security Management Server**.

5. Saisissez un nom d'utilisateur et un mot de passe permettant de se connecter à Data Security Manager. Il s'agit là de l'interface de gestion dans laquelle est configurée la stratégie Data Security. L'utilisateur doit être administrateur de Data Security et disposer de privilèges l'autorisant à déployer des paramètres.
6. Cliquez sur **Register (Enregistrer)**. Si l'enregistrement réussit, un message confirme ce résultat et vous invite à redémarrer Content Gateway.

   Si l'enregistrement échoue, un message d'erreur en donne la raison. Corrigez le problème et recommencez le processus d'enregistrement.

Options de configuration

Lorsque l'enregistrement a réussi, définissez les éléments suivants dans la page **Configurer > Sécurité > Data Security** :

1. **Analyze FTP Uploads (Analyser les chargements FTP)** : activez cette option pour envoyer les chargements FTP à Data Security pour analyse et application des stratégies.
2. **Analyze HTTPS Content (Analyser le contenu HTTPS)** : activez cette option pour envoyer les publications HTTPS décryptées à Data Security pour analyse et application des stratégies. SSL Manager doit être activé dans Content Gateway. Voir *Utilisation des données cryptées*, page 129.

Remarque

Pour que ces options entrent en vigueur, Content Gateway doit être configuré pour envoyer le trafic FTP et HTTPS par proxy.

3. Cliquez sur **Appliquer** pour enregistrer vos paramètres, puis redémarrez Content Gateway.
4. Accédez à TRITON – Data Security pour configurer le module Data Security Content Gateway. Reportez-vous à la section intitulée « Déploiement du module Content Gateway » du *Guide de mise en route de Websense Web Security Gateway Anywhere*.

Data Security et Content Gateway communiquent par plusieurs ports. Si les Tables IP sont configurées dans le système hôte Content Gateway, ces ports doivent être ouverts dans les Tables IP. Consultez le *Guide d'installation de Content Gateway* ou l'article de la Bibliothèque technique intitulé « Configuring IPTables for Websense Content Gateway » (Configuration des tables IP pour Websense Content Gateway).

Remarque

Une alarme Content Gateway Manager est générée dans les cas suivants :

- On-box Data Security est activé, mais pas enregistré.
- On-box Data Security est activé et enregistré, mais pas configuré dans Data Security Manager.

Configuration du client ICAP

Le protocole ICAP peut être utilisé avec toute version de Websense Data Security, mais l'utilisation de l'interface directe est recommandée lorsque le moteur de stratégies est intégré à Content Gateway. Voir *Enregistrement et configuration de Data Security*, page 121.

ICAP **doit** être utilisé pour assurer l'interopérabilité avec Data Security Suite versions 7.1 et antérieures.

> **Remarque**
>
> Un serveur ICAP secondaire peut être spécifié en tant que serveur de basculement en cas de défaillance du serveur principal.
>
> Les serveurs principal et secondaire peuvent également être configurés pour effectuer l'équilibrage de la charge.
>
> Voir la section *Basculement ICAP et équilibrage de la charge* ci-dessous.

Pour configurer l'intégration à ICAP, connectez-vous à Content Gateway Manager et ouvrez la page **Configurer > Mon proxy > De base > Général**.

1. Dans la section **Networking (Mise en réseau)** du tableau des fonctions, sélectionnez Data Security **On (Activé)**.
2. Cliquez sur **Appliquer**, puis sur **Redémarrer**.
3. Naviguez jusqu'à **Configurer > Networking (Mise en réseau) > ICAP > Général**.
4. Dans le champ **ICAP Service URI (URI du service ICAP)**, saisissez l'URI (Uniform Resource Identifier) du service ICAP principal, suivi d'une virgule (sans espace) et de l'URI du service ICAP secondaire. Le service ICAP secondaire est facultatif.

   Un URI est similaire à une URL mais se termine par un répertoire et non pas par une page. Demandez cet identifiant à votre administrateur Websense Data Security Suite. Entrez l'URI au format suivant :

   `icap://`*`nomhôte`*`:`*`port`*`/`*`chemin`*

   Pour *nomhôte*, saisissez l'adresse IP ou le nom d'hôte du dispositif Websense Data Security Suite Protector.

   Le port ICAP par défaut est le 1344.

   Chemin correspond au chemin d'accès du service ICAP dans l'ordinateur hôte.

   Par exemple :

   ```
   icap://ICAP_machine:1344/REQMOD
   ```

   Il n'est pas été nécessaire de spécifier le port lorsque vous utilisez le port ICAP par défaut 1344. Par exemple, l'URI précédent peut également être saisi sans le port par défaut :

   ```
   icap://ICAP_machine/REQMOD
   ```

5. Sous **Analyze HTTPS Content (Analyser le contenu HTTPS)**, indiquez si le trafic décrypté doit être envoyé à Websense Data Security Suite pour analyse ou envoyé directement à destination. Pour envoyer le trafic à Websense Data Security Suite, SSL Manager doit être en exécution. Voir *Utilisation des données cryptées*, page 129.
6. Sous **Analyze FTP Uploads (Analyser les chargements FTP)**, indiquez si les requêtes de chargement FTP doivent être ou non envoyées à Websense Data Security Suite pour analyse. Pour envoyer le trafic FTP à Websense Data Security Suite, la fonction de proxy FTP doit être activée. Voir *FTP*, page 288.
7. Sous **Action for Communication Errors (Action pour erreurs de communication)**, choisissez d'autoriser le trafic ou d'envoyer une page de blocage lorsque Content Gateway rencontre une erreur de communication avec Websense Data Security Suite.
8. Sous **Action for Large Files (Action pour les fichiers volumineux)**, choisissez d'autoriser le trafic ou d'envoyer une page de blocage lorsque la taille du fichier envoyé dépasse la limite définie dans Websense Data Security Suite. Par défaut, la taille maximale des fichiers est de 12 Mo pour Data Security Suite versions 7.0 et ultérieures.
9. Cliquez sur **Appliquer**.

Remarque

Si vous modifiez l'URI, vous devez redémarrer Content Gateway. Les autres modifications ne nécessitent pas de redémarrage.

Basculement ICAP et équilibrage de la charge

Content Gateway peut être configuré pour basculer vers un serveur ICAP de sauvegarde en cas de défaillance du serveur ICAP actif. Le proxy détecte dans ce cas la condition d'échec et envoie le trafic au serveur secondaire. Si le serveur secondaire ne répond pas, le proxy utilise le serveur principal. Lorsqu'aucun serveur ICAP n'est disponible, l'ouverture du proxy échoue.

L'équilibrage de la charge entre deux serveurs ICAP est également une possibilité.

Délai de basculement

Content Gateway peut expérimenter un certain retard de traitement des requêtes entre la défaillance réelle et le moment où le proxy désigne le serveur comme défaillant. Une fois que le serveur est désigné comme défaillant, toutes les nouvelles requêtes sont envoyées au serveur ICAP secondaire. Le délai de basculement est surtout limité par la configuration du délai d'expiration de la connexion.

Conditions d'échec entraînant un basculement

- Échec de la requête ICAP dû à une défaillance de niveau 3 (à deux reprises pour la même requête)
- Échec de connexion à un port dans le délai d'expiration donné
- Échec de l'envoi d'une requête (réinitialisation de la connexion par le serveur et autres)

Conditions d'échec exclues

Content Gateway ne considère pas les absences de réponse, les réponses non valides et les réponses lentes comme des défaillances.

Toutefois, Content Gateway ne s'assure pas que le serveur ICAP est valide au démarrage en vérifiant la réponse à la requête ICAP OPTIONS.

Conditions de récupération

Dès que le serveur est désigné comme défaillant, les nouvelles requêtes sont envoyées au serveur secondaire. Aucune nouvelle requête ICAP n'est envoyée au serveur défaillant tant qu'il n'est pas à nouveau détecté comme étant actif, conformément aux conditions de récupération ci-dessous.

Content Gateway teste les conditions de récupération de chaque serveur ICAP défaillant à intervalle défini. Lorsque l'équilibrage de la charge est désactivé, les requêtes continuent d'être envoyées à un serveur ICAP secondaire jusqu'à ce que le serveur principal soit de nouveau en ligne. Lorsque l'équilibrage de la charge est activé, Content Gateway commence à envoyer les requêtes à un serveur (round-robin) dès qu'il en détecte un désigné comme actif.

- Connexion TCP réussie
- Envoi d'une requête OPTIONS réussie
- Réception réussie d'une réponse valide à une requête OPTIONS

Actions de récupération

Dès la récupération d'un serveur (il revient en ligne et est désigné comme actif) :

- Équilibrage de la charge activé : les requêtes commencent à être envoyées au nouveau serveur actif (round-robin).
- Équilibrage de la charge désactivé : si le serveur principal reprend son rôle, toutes les requêtes commencent à lui être envoyées. Si le serveur secondaire reprend son rôle, le trafic continue à être envoyé au serveur principal jusqu'à ce que ce dernier soit défaillant.

Échec d'ouverture

Lorsque tous les serveurs ICAP sont défaillants, une option de configuration autorise un comportement d'échec à l'ouverture ou d'échec à la fermeture. Lorsque tous les serveurs ICAP sont défaillants, la thread d'arrière-plan tente en permanence d'établir une nouvelle connexion avec chaque serveur.

Paramètres de configuration

Ces paramètres de basculement ICAP sont définis dans le *Fichier de configuration records.config* (les valeurs par défaut sont indiquées ci-après) :

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.icap.ICAPUri`	CHAÎNE	(vide)	Listes des URI ICAP séparés par des virgules. Par exemple : icap://1.2.3.4:1344/reqmod, icap://4.3.2.1:1344/reqmod
`proxy.config.icap.ActiveTimeout`	ENTIER	5	Délai d'expiration de la lecture/réponse, en secondes. L'activité est considérée comme défaillante lorsque le délai d'expiration est dépassé.
`proxy.config.icap.RetryTime`	ENTIER	5	Intervalle de récupération, en secondes, permettant de tester la remise en activité d'un serveur défaillant
`proxy.config.icap.FailOpen`	ENTIER	1	Définissez cette valeur sur : • 1 pour autoriser le trafic lorsque les serveurs ICAP sont inactifs • 0 pour envoyer une page de blocage lorsque les serveurs ICAP sont inactifs
`proxy.config.icap.LoadBalance`	ENTIER	1	Définissez cette valeur sur : • 1 pour envoyer les requêtes à tous les serveurs disponibles • 0 pour envoyer les requêtes au serveur principal uniquement

13 Utilisation des données cryptées

Rubriques connexes :

- *Exécution en mode proxy explicite*, page 131
- *Tâches*, page 133
- *Activation de SSL Manager*, page 132
- *Certificats*, page 134
- *Autorité de certification racine interne*, page 134
- *Gestion des certificats*, page 141
- *Configuration de SSL Manager pour le trafic entrant*, page 144
- *Configuration de SSL Manager pour le trafic entrant*, page 145
- *Validation des certificats*, page 146
- *Gestion des accès aux sites Web HTTPS*, page 152
- *Certificats des clients*, page 156
- *Configuration de la journalisation de SSL Manager*, page 158
- *Personnalisation des messages d'échec des connexions SSL*, page 161

SSL (Secure Sockets Layer) constitue la norme de l'industrie en matière de transmission sécurisée des données sur Internet. Cette norme repose sur le cryptage des données et sur un système de certificats approuvés, publiés par des autorités de certification et reconnus par les serveurs et les clients.

Pour établir une connexion SSL, le client envoie une requête de connexion SSL au serveur. Si le serveur accepte la connexion, le client et le serveur utilisent un protocole standard (handshake) pour négocier une connexion SSL.

Lorsque SSL Manager est activé, le trafic SSL est décrypté, analysé, puis à nouveau crypté avant d'être envoyé à destination.

Important

Même si SSL Manager n'est **pas** activé et que les données HTTPS ne sont pas décryptées, Content Gateway exécute un filtrage des URL HTTPS. Par conséquent, une recherche d'URL est effectuée pour chaque requête HTTPS et la stratégie est ensuite appliquée.

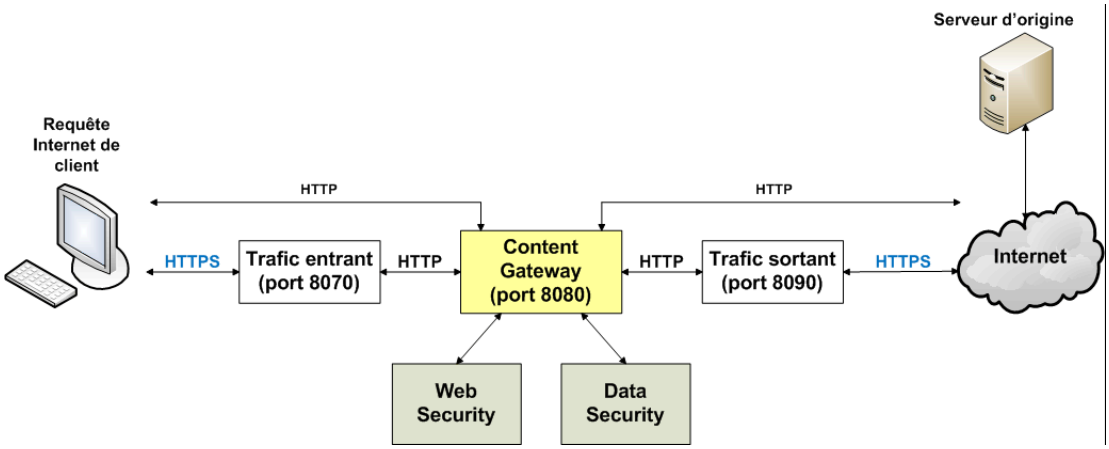
En mode proxy explicite, lorsque SSL est désactivé, Content Gateway filtre les URL sur la base du nom d'Hôte indiqué dans la requête. Si le site est bloqué, Content Gateway présente une page de blocage. Notez que certains navigateurs ne prennent pas en charge l'affichage de la page de blocage. Pour désactiver cette fonction, configurez vos clients de sorte qu'il n'envoient pas de requêtes HTTPS au proxy.

En mode proxy transparent, lorsque SSL est désactivé, Content Gateway filtre les URL sur la base du nom commun indiqué dans le certificat présenté par le serveur de destination. Si le site est bloqué, la connexion au client est abandonnée. Aucune page de blocage ne s'affiche. Pour désactiver cette fonction lorsqu'elle est utilisée avec WCCP, ne créez pas de groupe de services pour HTTPS.

Chaque requête de type SSL se compose de deux sessions distinctes :

- L'une à partir du navigateur client vers SSL Manager. Cette session est destinée au trafic SSL *entrant*.
- Une autre à partir de SSL Manager vers le serveur Web auquel sont destinées les données sécurisées. Cette session est destinée au trafic SSL *sortant*.

Ces sessions nécessitent des certificats différents.



Remarque

Content Gateway ne met pas le contenu HTTPS en cache.

Pour plus d'informations sur SSL et les certificats SSL, lancez une recherche sur Internet ou consultez l'un des ouvrages disponibles dans le commerce.

Pour plus d'informations sur la préparation de votre système, reportez-vous a la documentation relative au déploiement et à l'installation, présente dans la Bibliothèque technique de Websense.

Exécution en mode proxy explicite

Si vous avez déjà un fichier PAC, remplacez le fichier **proxy.pac** situé dans le répertoire **config** de Content Gateway (l'emplacement par défaut est **/opt/WCG/config**) par le fichier existant. Si vous n'avez pas encore de fichier PAC, reportez-vous à l'étape 4 ci-dessous pour copier le script fourni.

1. Vérifiez que HTTPS est bien activé dans l'onglet **Configurer > Mon proxy > De base > Général**. Si ce n'est pas le cas, définissez-le sur **On (Activé)**, cliquez sur **Appliquer**, puis sur **Redémarrer** Content Gateway.
2. Naviguez jusqu'à l'onglet **Configurer > Content Routing (Acheminement du contenu) >Browser Auto-Config (Auto-configuration du navigateur) > PAC**.
3. Dans le champ **Auto-Configuration Port (Port d'auto-configuration)**, indiquez le numéro du port utilisé par le proxy pour fournir le fichier PAC. Le port par défaut est le 8083.
4. Le volet Paramètres PAC affiche le fichier **proxy.pac** :
   - Si vous avez copié un fichier PAC existant dans le répertoire **config** de Content Gateway, le fichier **proxy.pac** contient les paramètres de configuration de votre proxy. Vérifiez ces paramètres et procédez à toute modification nécessaire.
   - Si vous n'avez pas copié de fichier PAC existant dans le répertoire **config** de Content Gateway, le fichier **proxy.pac** est vide. Copiez, puis collez le script suivant pour vos paramètres PAC. Vous devez fournir le nom de domaine ou l'adresse IP du proxy. Ce modèle ne correspond qu'à un test de base. Modifiez davantage ce fichier en fonction des besoins de votre organisation.

```
function FindProxyForURL(url, host)
{
  url = url.toLowerCase();
  host = host.toLowerCase();
  if(url.substring(0, 5) == "http:"){
    return "NOM_DOMAINE_ou_Adresse_IP_PROXY WCG:8080";
  }
  else if(url.substring(0, 4) == "ftp:"){
    return "NOM_DOMAINE_ou_Adresse_IP_PROXY WCG:2121";
  }
  else if(url.substring(0, 6) == "https:"){
    return "NOM_DOMAINE_ou_Adresse_IP_PROXY WCG:8080";
  }
  else{
    return "DIRECT";
  }
}
```

5. Cliquez sur **Appliquer**.
6. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Une fois les nouvelles données PAC en place, vous devez demander à vos utilisateurs de définir leur navigateur de sorte qu'il pointe vers ce fichier PAC. Par exemple, si le fichier PAC est stocké dans le serveur proxy avec le nom d'hôte **proxy1** et que Content Gateway utilise le port par défaut 8083 pour fournir ce fichier, les utilisateurs doivent spécifier l'URL suivante dans les paramètres de configuration du proxy :

```
http://proxy1.entreprise.com:8083/proxy.pac
```

Les procédures qui permettent de spécifier l'emplacement du fichier PAC varient d'un navigateur à l'autre.

Pour Microsoft Internet Explorer 7.0 et versions ultérieures :

1. Sélectionnez **Outils > Options Internet > Connexions > Paramètres réseau**.
2. Sélectionnez le champ **Utiliser un script de configuration automatique** et entrez `http://Nom_Domaine_ou_Adresse_IP_WCG:8083/proxy.pac` dans le champ **Adresse**.
3. Cliquez sur **OK**.

Pour Mozilla Firefox 2.0 et versions ultérieures :

1. Sélectionnez **Outils > Options > Avancé > Réseau > Connexion > Paramètres**.
2. Sélectionnez le champ **Adresse de configuration automatique du proxy** et entrez `http://Nom_Domaine_ou_Adresse_IP_WCG:8083/proxy.pac`
3. Cliquez sur **Actualiser**, puis sur **OK**.

Pour plus d'informations, consultez la documentation de votre navigateur.

Activation de SSL Manager

1. Dans l'onglet **Configurer > Mon proxy > De base > Général**, cliquez sur HTTPS **On (Activé)**.

   Remarque
   Si vous utilisez d'autres produits Websense pour analyser le trafic HTTPS, par exemple Websense Data Security Suite, vous devez activer HTTPS ici.

2. Cliquez sur **Appliquer**, puis sur **Redémarrer**.
3. Dans l'onglet **Configurer > Mon proxy > UI Setup (Configuration de l'interface utilisateur) > Général**, définissez le port de l'interface SSL Manager. Le port par défaut est le 8071. Ce port ne doit pas correspondre au port de l'interface Content Gateway Manager (par défaut 8081).
4. Entrez le nom de fichier du certificat SSL. Voir *Création d'une autorité de certification subordonnée*, page 136.

Utilisez la page **Configurer > Protocoles > HTTPS** pour définir les informations de port et activer le tunnel Skype.

1. Dans le champ **HTTPS Proxy Server Port (Port du serveur proxy HTTPS)**, entrez le port destiné au trafic HTTPS sortant (client vers SSL Manager). La valeur par défaut est 8070.

2. Dans le champ **SSL Outbound Port (Port sortant SSL)**, entrez le port que SSL Manager devra utiliser pour le trafic HTTPS sortant (SSL Manager vers le serveur de destination). La valeur par défaut est 8090.
3. Si Content Gateway est un **proxy explicite** et que vous souhaitez autoriser le trafic Skype, activez l'option **Tunnel Skype (Créer un tunnel Skype)**. Cette option est nécessaire car, bien que Skype présente un protocole de négociation SSL, les flux de données Skype ne respectent pas la norme SSL. La connexion est abandonnée lorsque le trafic ne passe pas par un tunnel.

   Pour terminer la configuration, assurez-vous que les stratégies de filtrage appliquées aux utilisateurs de Skype autorisent la « téléphonie Internet » dans **TRITON – Web Security**. Cette option est obligatoire pour les utilisateurs de Skype, que SSL Manager soit activé ou non.

   Par ailleurs, s'il n'en est pas empêché, Skype acheminera le trafic vers un port non HTTP après le protocole de négociation initial. Pour obliger le trafic Skype à passer par Content Gateway, un Objet de stratégie de groupe (GPO) doit être utilisé conformément à la description donnée dans le Guide de l'administrateur Skype.

Important

Il n'est pas nécessaire de définir cette option lorsque SSL Manager n'est pas activé.

Cette option n'est pas valide et n'a aucun effet lorsque Content Gateway est un proxy transparent.

Tâches

Pour le trafic entrant (client vers SSL Manager), procédez comme suit pour préparer le déploiement de SSL Manager :

1. Créez une autorité de certification (CA) racine interne. Pour signer le trafic SSL, SSL Manager requiert une autorité de certification SSL interne habilitée à signer des certificats SSL. Cette autorité de certification est destinée au trafic circulant entre le navigateur et SSL Manager. Voir *Autorité de certification racine interne*, page 134.
2. Ajoutez cette autorité de certification dans l'arborescence des certificats. Les serveurs (par exemple ceux de destination) consultent cette arborescence afin de vérifier qu'ils peuvent approuver les utilisateurs, ces derniers disposant d'un certificat publié par l'une des autorités répertoriées ici. Les certificats répertoriés dans cette arborescence sont les autorités de certification auxquelles vous faites confiance et chargées de vérifier la validité des différents sites Web individuels. Tout site Web signé par une autorité de certification présente dans l'arborescence des certificats et présentant l'état « autoriser » est autorisé à transiter par SSL Manager. Voir *Gestion des certificats*, page 141.
3. Personnalisez les pages devant s'afficher dans les navigateurs des utilisateurs. Voir *Personnalisation des messages d'échec des connexions SSL*, page 161. Les pages d'échec de connexion et d'échec de vérification du certificat font partie des pages à personnaliser.

Certificats

La sécurité est fondée sur les certificats. L'un des rôles de SSL Manager consiste à vérifier la validité de ces certificats. Un certificat doit respecter 3 critères :

- Il doit être à jour (ne pas avoir expiré ni avoir été révoqué). Voir *Validation des certificats*, page 146.
- Il doit avoir été publié par une autorité de certification approuvée. Voir *Gestion des certificats*, page 141.
- L'URL et le propriétaire du certificat doivent correspondre. Voir *Configuration des paramètres de validation*, page 147.

Le trafic qui va du navigateur client à SSL Manager requiert un certificat publié par une autorité de certification racine interne. Voir *Autorité de certification racine interne*, page 134.

Le trafic circulant de SSL Manager vers le serveur de destination requiert un certificat publié par l'une des autorités répertoriées dans l'arborescence des autorités de certification de l'onglet **Configurer > SSL > Certificats > Autorités de certification**. Voir *Gestion des certificats*, page 141.

Autorité de certification racine interne

L'autorité de certification racine interne génère tous les certificats utilisés entre le navigateur client et SSL Manager de manière dynamique.

- Pour transmettre le trafic entrant à SSL Manager, vous devez disposer d'une autorité de certification racine interne.
- Vous pouvez importer ou créer l'autorité de certification.
- L'autorité de certification racine interne est stockée dans **/opt/WCG/sxsuite/conf/CA_default/PCA**.
- Le nom de l'autorité de certification est **PCAcert.pem**.

Important

Sauvegardez l'autorité de certification racine interne existante avant d'en importer une ou d'en créer une nouvelle. Le cas échéant, vous pourrez ainsi récupérer la version antérieure du certificat. Pour plus d'informations, consultez la section *Sauvegarde de l'autorité de certification racine interne*, page 141.

À tout moment, une seule autorité de certification racine interne doit être active.

Important

L'autorité de certification racine interne incluse par défaut dans SSL Manager n'est pas unique et ne doit pas être utilisée dans un environnement de production.

Remplacez l'autorité de certification racine interne par défaut par celle de votre organisation ou créez-en une nouvelle. Reportez-vous aux sections suivantes.

Trois options permettent de créer une autorité de certification racine interne :

- Utilisez une autorité de certification d'entreprise existante et importez-la dans SSL Manager. Voir *Importation de l'autorité de certification racine*, page 135.
- Créez une nouvelle autorité de certification pour les proxy et mettez-la à la disposition des navigateurs. Voir *Création d'une nouvelle autorité de certification racine*, page 135.
- Créez une autorité de certification subordonnée. Cette option permet d'utiliser l'autorité de certification de l'entreprise, mais celle-ci peut également révoquer cette sous-autorité de certification. Voir *Création d'une autorité de certification subordonnée*, page 136.

Importation de l'autorité de certification racine

Si votre organisation a déjà une autorité de certification racine, vous pouvez l'importer. Ce certificat doit être approuvé par tous les navigateurs de votre organisation. Assurez-vous de sauvegarder toutes les nouvelles autorités de certification racines internes que vous importez. Pour plus d'informations, consultez la section *Sauvegarde de l'autorité de certification racine interne*, page 141.

1. Sélectionnez **Configurer > SSL > Internal Root CA (Autorité de certification racine interne)** > **Import Root CA (Importer une autorité de certification racine)**.
2. Sélectionnez le certificat à importer. Ce certificat doit être au format X.509 et codé en Base 64.
3. Sélectionnez la clé privée. Cette clé doit correspondre au certificat sélectionné à l'étape 2.
4. Saisissez, puis confirmez la phrase secrète.
5. Cliquez sur **Import Root CA (Importer une autorité de certification racine)**. L'autorité de certification importée est stockée dans **/opt/WCG/sxsuite/conf/CA_default/PCA**.

Création d'une nouvelle autorité de certification racine

Rubrique connexe :

- *Création d'une autorité de certification subordonnée*, page 136

Si vous n'avez pas encore d'autorité de certification racine, renseignez les champs de cet onglet pour en créer une. Assurez-vous de sauvegarder toute nouvelle autorité de certification racine interne créée. Pour plus d'informations, consultez la section *Sauvegarde de l'autorité de certification racine interne*, page 141.

Dans cette page, les champs qui doivent être obligatoirement renseignés sont désignés par un astérisque (*).

1. Sélectionnez **Configurer > SSL > Internal Root CA (Autorité de certification racine interne)**, puis **Create Root CA (Créer une autorité de certification racine)**.

2. Saisissez les informations demandées dans les champs, en faisant particulièrement attention aux éléments suivants :
   - Les champs **Organisation**, **Organizational Unit (Unité d'organisation)** (facultatif) et **Common Name (Nom commun)** doivent comprendre un *nom distinctif*.
     - Dans **Organisation**, saisissez le nom de votre société.
     - Dans **Common Name (Nom commun)**, saisissez le nom de l'autorité de certification de votre entreprise.
   - Le commentaire fait alors partie du certificat. La première ligne que vous saisissez est visible par les utilisateurs.
   - Saisissez, puis confirmez la phrase secrète. (Une phrase secrète est similaire à un mot de passe. Elle est toutefois généralement plus longue pour plus de sécurité. Il est recommandé d'utiliser une solide phrase secrète, qui combine des chiffres, des caractères et des lettres minuscules et majuscules.
3. Cliquez sur **Generate and Deploy Certificate (Générer et déployer le certificat)** pour déployer le certificat dans le serveur Content Gateway.

Création d'une autorité de certification subordonnée

La création d'une autorité de certification subordonnée (sous-autorité de certification) vous permet d'exploiter l'ensemble des informations déjà existantes pour votre autorité de certification racine. Toutefois, l'autorité de certification racine peut à tout moment révoquer la sous-autorité de certification.

Pour générer une sous-autorité de certification à l'aide d'OpenSSL et des services de certificat de Microsoft Windows, procédez comme suit.

Préparation

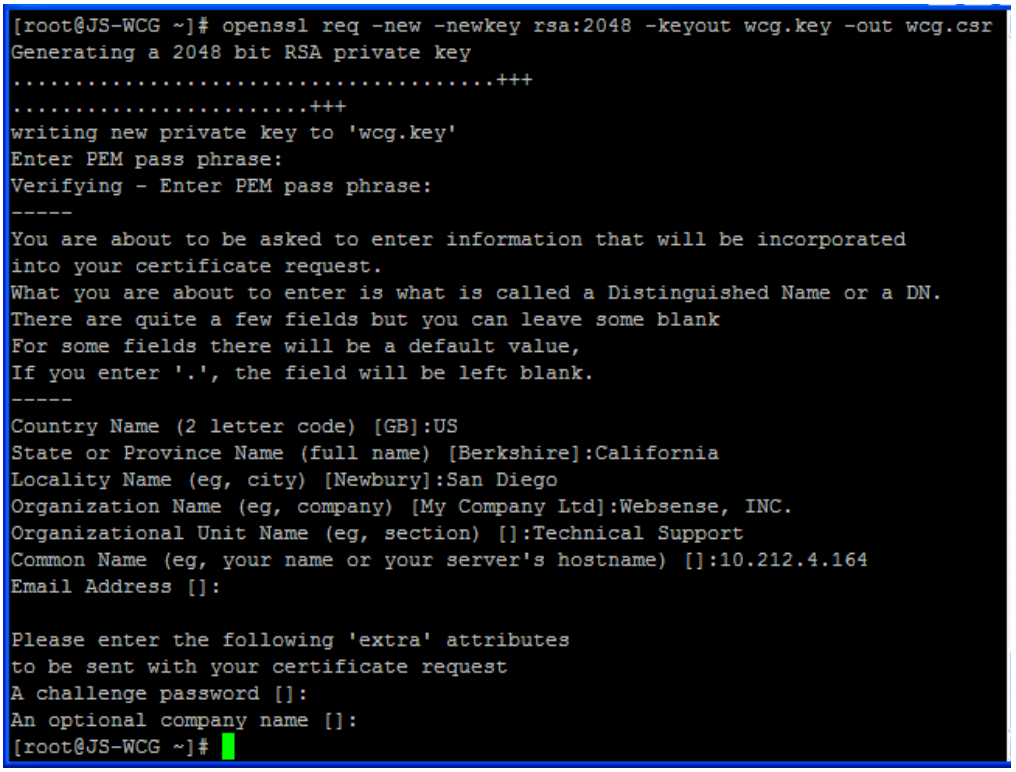
- **Si vous n'êtes pas l'administrateur du domaine de l'entreprise, il vous faudra faire appel à ce dernier pour disposer des autorisations de domaine nécessaires pour générer une sous-autorité de certification**.
- Installez le kit d'outils **OpenSSL 0.9.8(x)** (www.openssl.org) dans un ordinateur Windows ou Linux.

Création d'une requête de signature de certificat (CSR)

1. Créez une requête de signature de certificat (CSR) avec OpenSSL.

   À l'invite Windows ou Linux, créez une requête CSR à l'aide de la commande **openssl** suivante :

   ```
   openssl req -new -newkey rsa:2048 -keyout wcg.key -out wcg.csr
   ```



2. Une série de questions s'affiche. Répondez à chaque question et prenez note du mot de passe de vérification, car vous en aurez besoin pour la suite du processus.

   Cette commande openssl génère 2 fichiers :

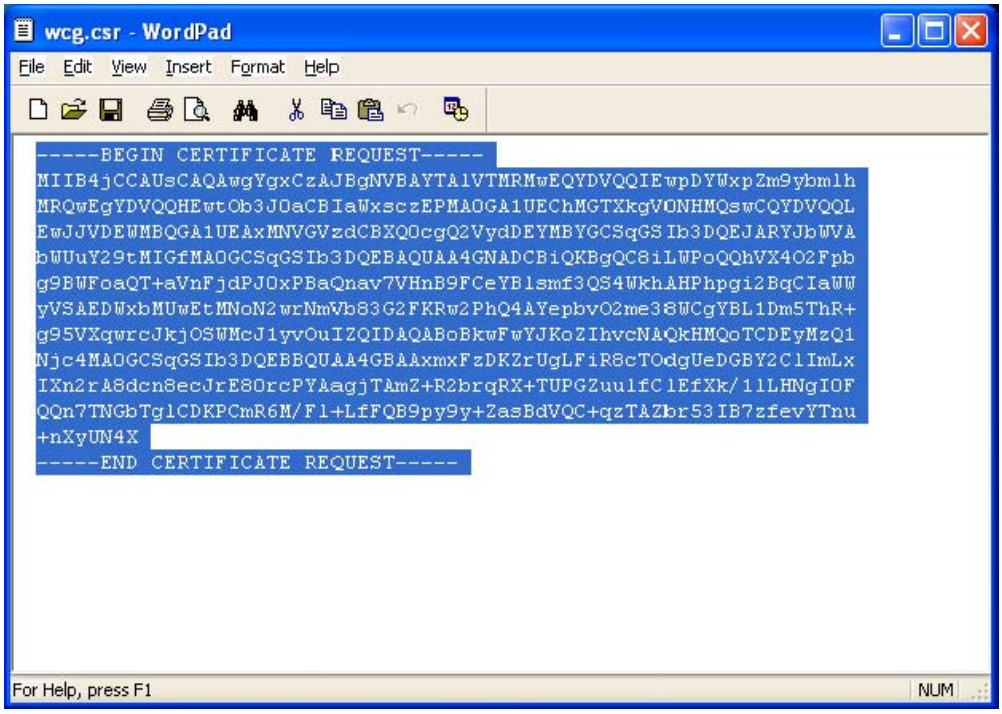
   - **wcg.csr** : requête CSR que sera signée par l'autorité de certification pour créer le certificat final
   - **wcg.key** : clé privée

3. Si vous avez créé cette requête CSR dans un système Linux, copiez-la dans votre hôte Windows via WinSCP ou un autre utilitaire de transfert de fichiers.

Signature de la requête

Vous devez signer la requête à l'aide des Services de certificats Microsoft.

1. Ouvrez le fichier **wcg.csr** dans **Wordpad** (pour préserver la mise en forme) et copiez son contenu dans le presse-papiers (Modifier > Sélectionner tout ; Modifier > Copier).

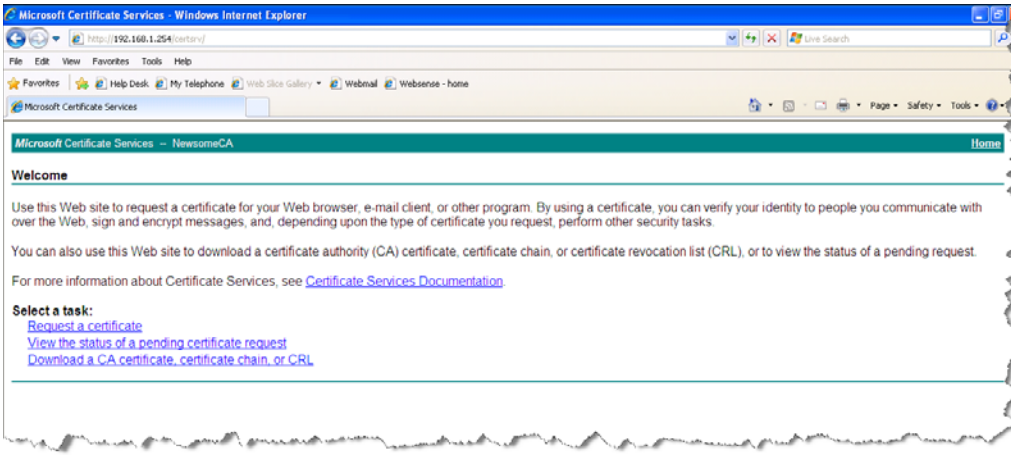


2. Dans **Internet Explorer**, accédez au **Serveur d'autorité de certification Microsoft**.

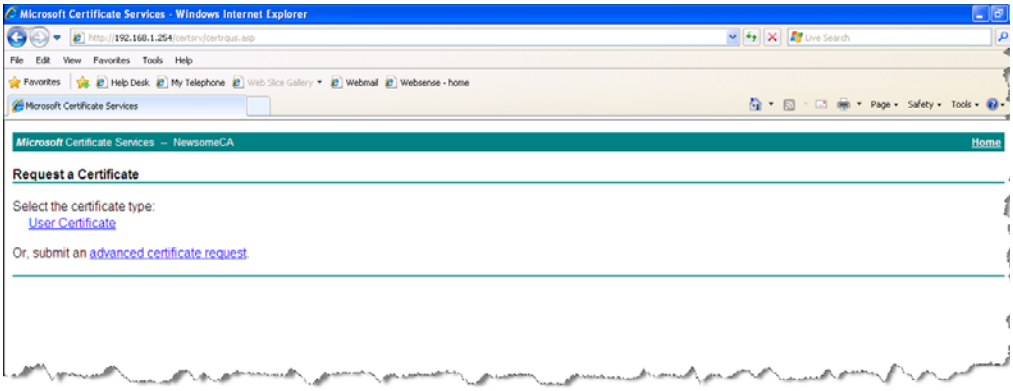
   Entrez l'URL suivante :

   http://<Adresse_IP_Serveur_CA>/certsrv

   L'applet **Services de certificats** démarre.

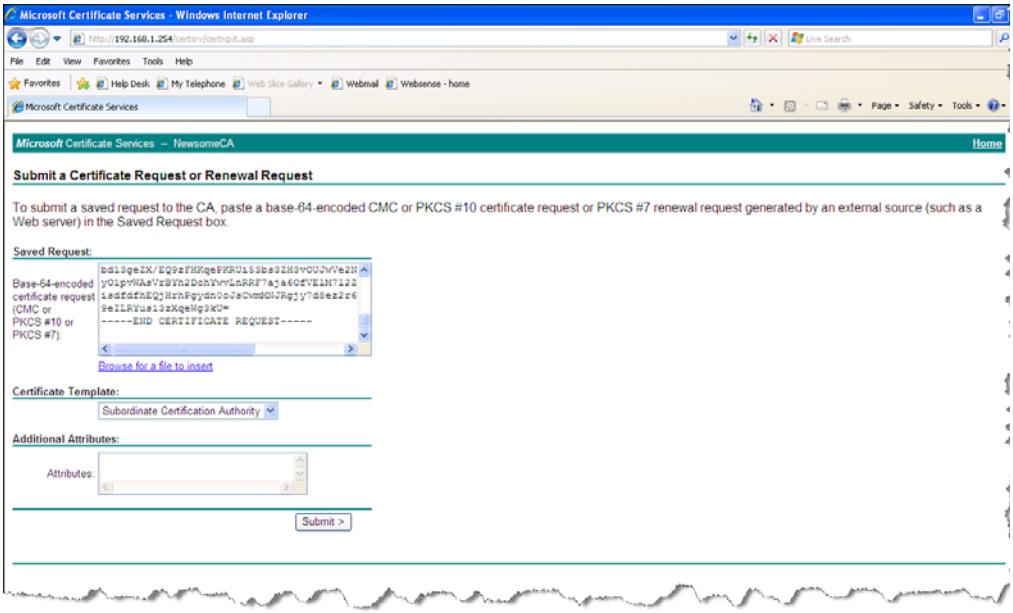


3. Dans l'écran **Bienvenue**, au-dessous de l'en-tête **Sélectionner une tâche**, sélectionnez **Demander un certificat**. La page **Demander un certificat** s'affiche.



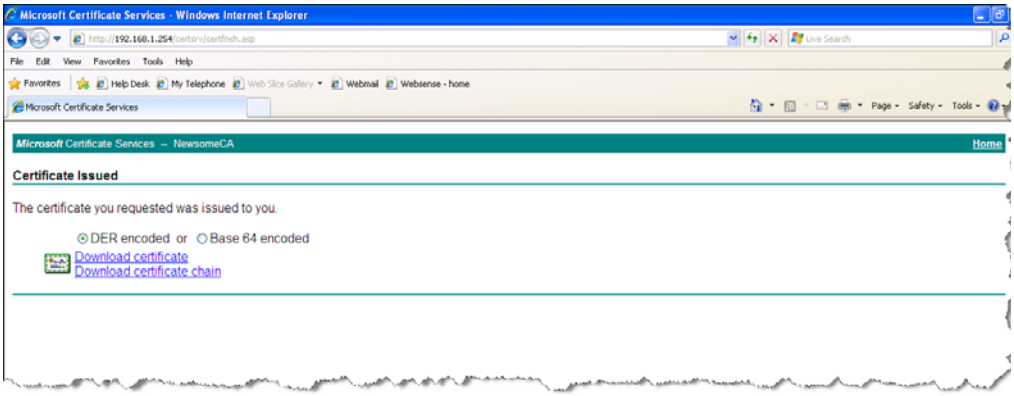
4. Choisissez d'envoyer une **demande de certificat avancée**.

5. Dans l'écran **Demande de certificat avancée**, sélectionnez **Soumettre une demande de certificat en utilisant un fichier CMC codé en base 64**. L'écran **Soumettre une demande de certificat ou de renouvellement** s'affiche.



6. Dans l'écran **Soumettre une demande de certificat ou de renouvellement**, collez le contenu du fichier **wcg.csr** (placé auparavant dans le presse-papiers) dans la fenêtre déroulante **Modèle de certificat**, puis cliquez sur **Envoyer**.

   Le certificat est publié et l'écran **Certificat délivré** s'affiche. Si, à la place de cet écran, l'écran **Certificat en attente** s'affiche, vous ne disposez pas de privilèges suffisants pour créer une sous-autorité de certification. Contactez l'administrateur du domaine de votre entreprise pour terminer le processus de création du certificat, puis passez à l'étape 7.

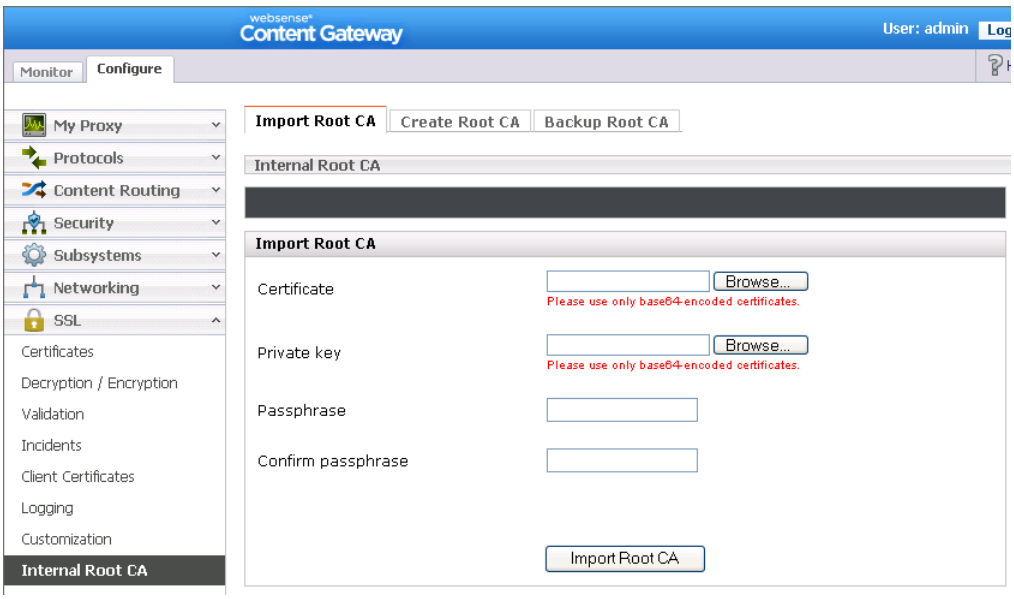


7. Activez le bouton radio **Codé en base 64**, puis sélectionnez **Télécharger le certificat**. Enregistrez le certificat dans votre poste de travail. Vous pourrez ensuite l'importer dans Content Gateway.

Lorsque le certificat codé en base 64 est dans votre poste de travail, de même que la clé privée créée pendant le processus de génération de la requête CSR, vous pouvez importer ces deux éléments dans Content Gateway SSL Manager.

Importation de la sous-autorité de certification dans SSL Manager

1. Ouvrez Content Gateway Manager et sélectionnez **Configurer > SSL > Internal Root CA (Autorité de certification racine interne) > Import Root CA (Importer une autorité de certification racine)**.



2. Cliquez sur **Parcourir** pour sélectionner le certificat. Ce certificat doit être au format X.509 et codé en base 64.
3. Cliquez sur **Parcourir** pour sélectionner la clé privée. Cette clé doit correspondre au certificat sélectionné à l'étape 2.
4. Saisissez, puis confirmez la phrase secrète.
5. Cliquez sur **Import Root CA (Importer une autorité de certification racine)**.
6. Redémarrez Content Gateway.

Sauvegarde de l'autorité de certification racine interne

Sauvegardez systématiquement les clés publique et privée de vos autorités de certification racines internes avant d'en importer d'autres ou d'en créer de nouvelles. Le cas échéant, vous pourrez ainsi récupérer la version antérieure du certificat. Sauvegardez également toute nouvelle autorité de certification racine que vous importez ou créez.

1. Sélectionnez **Configurer > SSL > Internal Root CA (Autorité de certification racine interne)** > **Backup Root CA (Sauvegarder une autorité de certification racine)**.
2. Cliquez sur **Save Public CA Key (Enregistrer la clé publique de l'autorité de certification)** pour afficher ou enregistrer la clé publique de l'autorité de certification. Cette clé publique doit être approuvée par les navigateurs Web des utilisateurs. Si vous n'avez pas cette clé, contactez votre administrateur réseau.
3. Cliquez sur **Save Private CA Key (Enregistrer la clé privée de l'autorité de certification)** pour afficher ou enregistrer la clé privée de l'autorité de certification. Si vous n'avez pas cette clé, contactez votre administrateur réseau.

Gestion des certificats

Rubriques connexes :

- *Ajout de nouvelles autorités de certification*, page 142
- *Sauvegarde des certificats*, page 143
- *Restauration des certificats*, page 143

Toutes les autorités de certification approuvées par Internet Explorer 7 sont répertoriées dans l'onglet **Configurer > SSL > Certificats > Autorités de certification**. Les serveurs de destination (trafic sortant à partir de SSL Manager) peuvent approuver les serveurs Web à l'aide de ces certificats. Notez qu'un petit « i » s'affiche devant le nom de certains certificats validés via les listes de révocation de certificats (CRL) ou le protocole OCSP (Online Certification Status Protocol). Ces certificats fournissent les URL qui vous permettent de vérifier leur état de révocation. Pour plus d'informations sur la vérification de l'état de révocation d'un certificat, consultez la section *Actualisation des informations de révocation*, page 151. SSL Manager vérifie l'état de révocation d'un certificat pour le trafic entrant et sortant.

Cliquez sur le nom d'une autorité de certification pour effectuer les opérations suivantes :

- *Affichage d'un certificat*, page 142
- *Suppression d'un certificat*, page 142
- *Modification de l'état autoriser/refuser d'un certificat*, page 142

Affichage d'un certificat

1. Sélectionnez **Configurer > SSL > Certificats** > **Autorités de certification**.
2. Sélectionnez le nom de l'autorité dont vous souhaitez afficher l'état.
3. Dans la fenêtre contextuelle, sélectionnez **Click to view certificate (Cliquez pour afficher le certificat)**.
4. Suivez les instructions de la fenêtre pour ouvrir ou enregistrer le fichier.

Suppression d'un certificat

1. Sélectionnez **Configurer > SSL > Certificats** > **Autorités de certification**.
2. Sélectionnez le nom de l'autorité de certification à supprimer.
3. Dans la fenêtre contextuelle, sélectionnez **Click to delete certificate (Cliquez pour supprimer le certificat)**.
4. Confirmez ou annulez la suppression du certificat.
5. Si vous confirmez la suppression du certificat, assurez-vous que celui-ci n'est plus répertorié dans l'onglet **Configurer > SSL > Certificats** > **Autorités de certification**.

Modification de l'état autoriser/refuser d'un certificat

1. Sélectionnez **Configurer > SSL > Certificats** > **Autorités de certification**.
2. Sélectionnez le nom de l'autorité dont vous souhaitez modifier l'état.
3. Dans la fenêtre contextuelle, sélectionnez **Click to change status to (Cliquez pour modifier l'état)**. Selon l'état du certificat, le choix disponible est **allow (autoriser)** ou **deny (refuser)**. Si vous définissez l'état sur refuser, un X rouge s'affiche à côté du nom de l'autorité de certification dans l'arborescence des autorités de certification. Si vous définissez l'état sur autoriser, un cercle vert s'affiche à côté du nom de l'autorité de certification.

Ajout de nouvelles autorités de certification

Rubriques connexes :

- *Sauvegarde des certificats*, page 143
- *Restauration des certificats*, page 143

Servez-vous de la page **Configurer > SSL > Certificats** > **Add Root CA (Ajouter une autorité de certification racine)** pour importer manuellement d'autres autorités de certification. L'état des certificats que vous importez manuellement est défini sur **allow (autoriser)**.

> **Important**
> Il est recommandé de sauvegarder les certificats existants avant d'effectuer toute modification, par exemple avant d'ajouter ou de supprimer des certificats. Voir *Sauvegarde des certificats*, page 143. Pour sauvegarder l'intégralité de votre configuration Content Gateway, consultez la section *Enregistrement et restauration des configurations*, page 105.

1. Cliquez sur **Parcourir** pour parcourir la structure de répertoires et localiser des certificats. Recherchez les fichiers portant une extension « .cer ». Ce certificat doit être au format X.509 et codé en Base 64.
2. Cliquez sur **Add Certificate Authority (Ajouter une autorité de certification)**.
3. Si l'importation a bien été effectuée, assurez-vous que le nouveau certificat soit répertorié dans la page **Configurer > SSL > Certificats** > **Autorités de certification**.

De nouvelles autorités de certification s'ajoutent également lorsque les utilisateurs consultent des sites signés par cette autorité. Ces certificats peuvent être **autorisés** ou **refusés**. Pour plus d'informations, consultez la section *Modification de l'état autoriser/refuser d'un certificat*, page 142.

Sauvegarde des certificats

Par précaution, il est recommandé de sauvegarder la base de données contenant les certificats des autorités de certification à chaque modification, par exemple lorsque vous ajoutez ou supprimez un certificat. Ces certificats peuvent alors être restaurés par la suite.

La sauvegarde des certificats sauvegarde également vos paramètres SSL Manager.

Utilisez la page **Configurer > SSL > Certificats** > **Backup Certificates (Sauvegarder les certificats)** pour sauvegarder vos certificats et vos paramètres SSL Manager.

- Cliquez sur **Back Up Configuration to Database (Sauvegarder la configuration dans la base de données)**.

Pour sauvegarder les certificats et l'ensemble de votre configuration Content Gateway, consultez la section *Enregistrement et restauration des configurations*, page 105.

Restauration des certificats

La restauration des certificats entraîne également la restauration de la base de données de configuration. Toutefois, les listes de révocation étant régulièrement mises à jour, elles ne sont pas restaurées dans le cadre de ce processus. Pour plus d'informations sur la mise à jour des listes de révocation de certificat, consultez la section *Actualisation des informations de révocation*, page 151.

Utilisez la page **Configurer > SSL > Certificats** > **Restore Certificates (Restaurer les certificats)** pour restaurer la base de données de configuration, certificats et paramètres SSL Manager compris.

1. Cliquez sur **Parcourir** pour localiser l'emplacement de la base de données des certificats de sauvegarde.
2. Cliquez sur **Restaurer**. Un message vous indique que la restauration a bien été effectuée et que la précédente base de données des certificats a été sauvegardée.

Si vous exécutez plusieurs proxy, servez-vous de cette fonction de restauration pour être certain que tous les proxy présentent la même configuration.

Décryptage et cryptage

Configuration de SSL Manager pour le trafic entrant, page 144

Configuration de SSL Manager pour le trafic entrant, page 145

Configuration de SSL Manager pour le trafic entrant

Rubriques connexes :

- *Configuration de SSL Manager pour le trafic entrant*, page 145

Servez-vous de la page **Configurer > SSL > Decryption / Encryption (Décryptage/ Cryptage)** > **Inbound (Entrant)** pour configurer la gestion du trafic entrant par SSL Manager. Le trafic entrant circule du navigateur vers SSL Manager, trajet au cours duquel le contenu est décrypté et inspecté.

1. Sélectionnez **Adresse IP** pour transmettre les informations d'authentification au prochain proxy.
2. Sélectionnez **Send VIA-Header (Envoyer l'en-tête VIA)** pour ajouter un en-tête spécial dans l'en-tête HTTP qui décrit la chaîne de proxy par laquelle passe le trafic. Cette option se révèle utile pour le dépannage. Si vous ne voulez pas inclure d'en-tête VIA-Header, n'activez pas cette case à cocher.
3. Sous **Protocol Settings (Paramètres des protocoles)**, définissez les protocoles devant être pris en charge par SSL Manager. Les protocoles pris en charge sont les protocoles SSLv2 et v3 et TLS v1. Sélectionnez le protocole pris en charge par le navigateur de votre entreprise. Vous devez sélectionner au moins un protocole. Le protocole par défaut est le protocole SSLv2. Ces paramètres remplacent les paramètres de ces protocoles dans les navigateurs des utilisateurs.

   Vous pouvez sélectionner des protocoles différents pour le trafic sortant.
4. La liste des cryptages décrit les algorithmes disponibles et le niveau de cryptage entre le client et SSL Manager. Les paramètres par défaut consistent à utiliser tout les cryptages disponibles à l'exception de eNULL et de ADH Suite. Le cryptage le plus fort (niveau de cryptage plus élevé) est appliqué en premier. Il peut être défini sur un autre niveau de cryptage que le trafic sortant. L'utilisation d'un niveau de cryptage élevé pour le trafic entrant peut renforcer l'intégrité et la sécurité de votre système.

Les autres paramètres de cryptage sont les suivants :

- **High** encryption cipher suites (Suites de cryptage élevé) : suites associées à des longueurs de clé supérieures à 128 bits et certaines suites de cryptage avec clés de 128 bits.
- **Medium** encryption cipher suites (Suites de cryptage moyen) : suites de cryptage avec clés de 128 bits.
- **Low** encryption cipher suites (Suites de cryptage faible) : suites de cryptage utilisant des algorithmes de cryptage 64 ou 56 bits, mais excluant les suites de cryptage d'exportation.

Pour les requêtes entrantes (requête d'un navigateur client de votre organisation vers SSL Manager), pensez à utiliser un cryptage faible afin d'améliorer les performances.

Pour plus d'informations sur les modes de cryptage, consultez le site www.openssl.org/docs.

5. Cliquez sur **Appliquer**.
6. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Configuration de SSL Manager pour le trafic entrant

Servez-vous de la page **Configurer > SSL > Decryption / Encryption (Décryptage/ Cryptage)** > **Outbound (Sortant)** pour configurer la gestion du trafic sortant par SSL Manager. Le trafic sortant circule de SSL Manager vers le serveur Web de destination SSL Manager vérifie l'état de révocation du certificat de ce site avant de lui transmettre les données à nouveau cryptées.

1. Lorsque plusieurs proxy sont présents entre SSL Manager et l'hôte de destination, sélectionnez **Adresse IP** pour transmettre les informations d'authentification d'un proxy ou suivant.
2. Sélectionnez **Send VIA-Header (Envoyer l'en-tête VIA)** pour ajouter un en-tête spécial dans l'en-tête HTTP qui décrit la chaîne de proxy par laquelle passe le trafic. Cette option se révèle utile pour le dépannage. Si vous ne voulez pas inclure d'en-tête VIA-Header, n'activez pas cette case à cocher.
3. Sous **Protocol Settings (Paramètres des protocoles)**, définissez les protocoles devant être pris en charge par SSL Manager. Les protocoles pris en charge sont les protocoles SSLv2 et v3 et TLS v1. Sélectionnez le protocole pris en charge par le navigateur de votre entreprise. Vous devez sélectionner au moins un protocole. Le protocole par défaut est le protocole SSLv2. Ces paramètres remplacent les paramètres de ces protocoles dans les navigateurs des utilisateurs.

   Vous pouvez sélectionner des protocoles différents pour le trafic entrant.
4. Sélectionnez **Session Cache (Cache de session)** pour mettre les clés en cache jusqu'à ce que le délai défini dans l'option Session Cache Timeout (Délai d'expiration du cache de session) soit écoulé. Cette option peut améliorer les performances. Lorsque les clés ne sont pas mises en cache, chaque requête est renégociée.
5. Indiquez, en secondes, la durée de conservation des clés dans le cache. La valeur par défaut est 300 secondes (5 minutes).
6. La liste des cryptages décrit les algorithmes disponibles et le niveau de cryptage entre le client et SSL Manager. Les paramètres par défaut consistent à utiliser tout les cryptages disponibles à l'exception de eNULL et de ADH Suite. Le cryptage le plus fort (niveau de cryptage plus élevé) est appliqué en premier. Il peut être défini sur un autre niveau de cryptage que le trafic entrant. L'utilisation d'un niveau de cryptage élevé pour le trafic sortant peut renforcer l'intégrité et la sécurité de votre système.

Les autres paramètres de cryptage sont les suivants :

- **High** encryption cipher suites (Suites de cryptage élevé) : suites associées à des longueurs de clé supérieures à 128 bits et certaines suites de cryptage avec clés de 128 bits.
- **Medium** encryption cipher suites (Suites de cryptage moyen) : suites de cryptage avec clés de 128 bits.
- **Low** encryption cipher suites (Suites de cryptage faible) : suites de cryptage utilisant des algorithmes de cryptage 64 ou 56 bits, mais excluant les suites de cryptage d'exportation.

Pour les requêtes sortantes (provenant de SSL Manager et envoyées au serveur de destination recevant les données cryptées), pensez à utiliser des niveaux de cryptage plus élevés pour renforcer la sécurité.

Pour plus d'informations sur les modes de cryptage, consultez le site www.openssl.org/docs.

7. Cliquez sur **Appliquer**.
8. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Validation des certificats

Rubriques connexes :

- *Contournement de la vérification*, page 150
- *Actualisation des informations de révocation*, page 151

La vérification des certificats SSL est un élément important de la sécurité SSL. C'est par le biais de l'échange de certificats et de la vérification que le client, dans ce cas Content Gateway SSL Manager, et le serveur d'origine vérifient leurs identités mutuelles.

Dans SSL Manager, cette tâche est effectuée par le moteur de vérification des certificats.

Savez-vous des onglets **Configurer > Mon proxy > SSL > Validation** pour activer et configurer le moteur de vérification des certificats (CVE, Certificate Verification Engine).

Pour plus d'informations sur les options disponibles en cas d'échec de la vérification ou lorsque vous préférez approuver le site, consultez la section *Contournement de la vérification*, page 150.

Pour obtenir une description complète de l'utilisation et des meilleures pratiques relatives aux moteurs CVE, consultez la page SSL Manager Certificate Verification Engine v7.7.

Configuration des paramètres de validation

1. Ouvrez la page **Configurer > SSL > Validation > Général**.
2. **Enable the certificate verification engine (Activer le moteur de vérification des certificats) :** cette option permet d'activer et de désactiver le moteur de vérification des certificats.

   Par défaut, la vérification des certificats est **désactivée**. Cela permet à l'administrateur de Content Gateway et aux utilisateurs du réseau de ne pas être surpris par les effets de la vérification des certificats lorsque HTTPS est activé à l'origine (dans la page **Configurer > Mon proxy > De base**).

   Si cette option n'est pas activée, la vérification des certificats n'est pas effectuée.

   Important

   Si vous désactivez le moteur de vérification des certificats, vous devez fournir des informations sur les pages suivantes seulement :

   - Configurer > SSL > Decryption / Encryption (Décryptage/Cryptage) > Inbound (Entrant)
   - Configurer > SSL > Decryption / Encryption (Décryptage/Cryptage) > Outbound (Sortant)
   - Configurer > SSL > pages Journalisation
   - Configurer > SSL > Customization (Personnalisation) > Connection Error (Erreur de connexion)

3. **Deny certificates where the common name does not match the URL (Refuser les certificats lorsque le nom commun ne correspond pas à l'URL)** : lorsque cette option est activée, deux vérifications sont effectuées :
   - D'abord, le système vérifie que le nom commun indiqué dans le certificat correspond exactement à l'URL de destination.
   - Lorsque la première vérification échoue, le système vérifie que la liste Autre nom de l'objet (SAN) du certificat correspond exactement à l'URL de destination.

   Les vérifications **ne respectent pas la casse**.

   Une correspondance exacte étant nécessaire, la présence d'une variation légitime du nom commun ou l'absence d'une variation correspondante dans la liste peut entraîner un blocage.

   Par exemple, le fait d'utiliser « https://cia.gov » pour accéder au site « https://www.cia.gov » peut générer un blocage. Un blocage peut également se produire lors de l'accès à un site Web via son adresse IP.
4. **Allow wildcard certificates (Autoriser les certificats avec caractères génériques)** : il s'agit là d'une sous-option de l'option **When Deny Certificates where the common name does not match the URL (Quand refuser les certificats lorsque le nom commun et l'URL ne correspondent pas)**. Lorsqu'elle est activée, cette option autorise les correspondances de noms communs incluant le caractère « * » (caractère générique).

   Certains serveurs HTTPS utilisent un caractère générique dans le champ Nom commun pour qu'un même certificat puisse couvrir un domaine entier. Par exemple : « *.exemple.com » pour couvrir « email.exemple.com », « stream.exemple.com », etc.

L'utilisation du caractère générique implique que les différents serveurs situés dans le domaine ne sont pas vérifiés, mais inclus du fait de la présence de ce caractère générique.

Autoriser les certificats avec caractère générique réduit la charge de correspondances strictes lorsqu'une correspondance stricte du nom commun est requise. Cette option est également utile dans le cas des domaines contenant plusieurs sous-domaines, tels que google.com ou yahoo.com. Elle se traduit également par un risque plus élevé de non blocage des variations frauduleuses ou indésirables d'un domaine.

5. **No expired or not yet valid certificates (Certificats n'ayant pas encore expiré ou pas encore valides) :** lorsqu'elle est activée, cette option refuse l'accès aux sites présentant un certificat arrivé à expiration ou non encore validé. Il s'agit là d'une vérification de base importante, car de nombreux sites malveillants utilisent des certificats expirés. Lorsque cette option n'est pas activée, l'accès à ces sites est autorisé.

   Remarque
   Les certificats auto-signés (certificats sans autorité de certification officielle) sont considérés comme non valides et entrent dans cette catégorie.

6. **Verify entire certificate chain (Vérifier la totalité de la chaîne de certificats)** : lorsqu'elle est activée, cette option vérifie l'état d'expiration et de révocation de tous les certificats situés entre le certificat du site et l'autorité de certification racine, conformément au chemin de certification du certificat. Cette vérification est importante.
7. **Check certificate revocation by CRL (Vérifier la révocation des certificats par CRL)** : les listes de révocation des certificats (CRL) sont utilisées pour vérifier l'état de révocation d'un certificat. Les listes CRL répertorient les certificats publiés, puis révoqués par l'autorité de certification.

   La vérification de l'état de révocation est une vérification de base essentielle, car les certificats sont généralement révoqués après une publication inappropriée, lorsqu'ils ont été compromis, lorsqu'ils utilisent une fausse identité ou lorsqu'ils ne respectent pas les stratégies définies par l'autorité de certification.
8. **Check certificate revocation by OCSP (Vérifier la révocation des certificats par OCSP)** : le protocole OCSP permet également de vérifier l'état de révocation d'un certificat. Bien qu'avantageux, il n'est pas aussi largement utilisé que les listes CRL et n'est donc pas aussi fiable. Par ailleurs, il s'agit là d'une vérification effectuée en temps réel et hébergée sur Internet qui peut générer un certain retard dans le traitement des requêtes.

   Remarque
   Il est recommandé d'utiliser OCSP en plus des listes CRL et non pas à la place. Pour plus d'informations sur les listes CRL et sur le protocole OCSP, consultez la section *Actualisation des informations de révocation*, page 151.

9. **Block certificates with Unknown OCSP state (Bloquer les certificats dont l'état OCSP est inconnu)** : lorsque la vérification de la révocation OCSP est activée, activez également cette option pour bloquer les certificats qui renvoient un état « Inconnu ».
10. **Preferred method for revocation check (Méthode de vérification de révocation favorite) :** lorsque les vérifications de révocation CRL et OCSP sont toutes deux activées, servez-vous de cette option pour désigner la méthode à appliquer en priorité. La valeur par défaut est CRL.
11. **Block certificates with no CRL URI and with no OCSP URI (Bloquer les certificats sans URI CRL et sans URI OCSP** : lorsque la vérification CRL, la vérification OCSP ou les deux sont activées, servez-vous de cette option pour bloquer les certificats non associés aux URI prévus. Par exemple, lorsque l'option de vérification CRL est activée et que le certificat ne contient pas d'URI CRL, la connexion est bloquée si cette option est activée. Lorsque les vérifications CRL et OCSP sont toutes deux activées, le blocage survient uniquement en cas d'absence des deux URI CRL et OCSP.

    Vous pouvez afficher les informations sur l'URI du certificat lorsque vous affichez le certificat dans votre navigateur. Pour plus d'informations, consultez la section *Affichage d'un certificat*, page 142.

    Un grand nombre de certificats n'incluant pas d'informations CRL ou OCSP, cette option peut générer un grand nombre d'échecs de vérification. Ces échecs sont dans ce cas signalés en tant qu'erreurs d'état de révocation inconnu (Unknown revocation state).

    La stratégie de sécurité qui en résulte peut être fortement restrictive et entraîner de nombreux refus d'accès.

    Comme pour les échecs de vérification, la liste des incidents vous permet d'autoriser des exceptions. Voir *Gestion des accès aux sites Web HTTPS*, page 152.
12. **Run external program on incidents (Exécuter un programme externe en cas d'incident)** : en vue du dépannage, vous pouvez exécuter un programme externe lorsque des incidents se produisent. Un incident est enregistré dans le journal chaque fois qu'un client reçoit un message d'accès refusé. Pour plus d'informations sur les incidents, consultez la section *Gestion des accès aux sites Web HTTPS*, page 152. Entrez le chemin d'accès au script dans ce champ.

    Pour exécuter ce script, les autorisations minimales sont les suivantes :

    ```
    chmod 700 /opt/WCG/sxsuite/bin/script.sh
    chown root /opt/WCG/sxsuite/bin/script.sh
    chgrp root /opt/WCG/sxsuite/bin/script.sh
    ```

    Pour simplifier le dépannage, il est recommandé de copier, puis de coller le script suivant. Ce script capture les éléments suivants et les écrits dans un fichier :

    - Le compte à l'origine de l'incident
    - L'adresse IP du client ou celle du proxy précédent si l'adresse IP du client n'a pas été transmise
    - L'ID de l'incident tel qu'indiqué dans la liste des incidents
    - Un message détaillé présentant la cause de l'incident
    - Le profil qui, au sein du compte, est à l'origine de l'incident

- La section hôte de l'URL qui a provoqué l'incident

```
#!/bin/sh
OUTFILE=/root/WCG/incidents.log

date >> $OUTFILE
echo "Account: $SCIP_INCIDENT_ACCOUNT" >> $OUTFILE
echo "Client-IP: $SCIP_INCIDENT_CLIENTIP" >> $OUTFILE
echo "Incident-ID: $SCIP_INCIDENT_ID" >> $OUTFILE
echo "Detailed Message: $SCIP_INCIDENT_MESSAGE" >> $OUTFILE
echo "Profile: $SCIP_INCIDENT_PROFILE" >> $OUTFILE
echo "Destination Host URL: $SCIP_INCIDENT_REMOTEHOST" >>
$OUTFILE
echo "User: $SCIP_INCIDENT_USER" >> $OUTFILE
echo >> $OUTFILE
```

Important

Nous vous conseillons de ne saisir aucune autre commande du répertoire **/opt/WCG/sxsuite/bin/** dans ce champ et de faire très attention si vous saisissez un autre script que celui fourni ci-dessus.

Contournement de la vérification

Servez-vous de la page **Configurer > SSL > Validation** > **Verification Bypass (Contournement de la vérification)** pour autoriser les utilisateurs à consulter un site lorsque la vérification du certificat échoue.

1. Sélectionnez **Permit users to visit sites with certificate failure after confirmation (Autoriser les utilisateurs à consulter les sites présentant un échec de certificat après confirmation)** pour autoriser les utilisateurs à accéder à un site après avoir été informés que le certificat de ce site était non valide. Lorsque cette case à cocher n'est pas activée, les utilisateurs n'ont pas la possibilité d'accéder au site.
2. Sélectionnez **Enable the SSL session cache for bypassed certificates (Activer le cache de session SSL pour les certificats ignorés)** pour stocker dans le cache les informations relatives aux certificats ignorés et réutiliser les connexions.
   - L'activation de cette option améliore les performances, mais tous les utilisateurs ne savent pas qu'ils tentent d'accéder à un site dont la vérification a échoué.
   - Lorsque cette option n'est pas activée, tous les utilisateurs savent que le site en question n'est pas associé à un certificat valide, mais les performances ne sont pas aussi rapides.
3. Dans le champ **Timeout (Délai d'expiration)**, définissez la période d'inactivité devant s'écouler entre les notifications envoyées aux utilisateurs qui ignorent que le site n'est pas associé à un certificat valide. La valeur par défaut est 6 minutes (360 secondes).

Il est recommandé d'activer le contournement de la vérification lors du déploiement initial. Par la suite, à mesure que le taux d'incidents évolue, vous pouvez utiliser la liste des incidents pour imposer une stratégie. Voir *Gestion des accès aux sites Web HTTPS*, page 152.

Actualisation des informations de révocation

Avant que votre site n'accepte des certificats, il est préférable que l'état du certificat soit vérifié afin d'être certain qu'il n'ait pas été révoqué. Deux méthodes permettent d'effectuer cette opération : via les listes CRL (voir *Listes de révocation des certificats (CRL)*, page 151) et via le protocole OCSP (voir *Protocole OCSP (Online certification status protocol)*, page 151).

Listes de révocation des certificats (CRL)

Servez-vous de la page **Configurer > SSL > Validation > Revocation Settings (Paramètres de révocation)** pour configurer l'actualisation des informations de révocation par SSL Manager. Par défaut, SSL Manager télécharge les listes CRL une fois par jour.

1. Pour que les téléchargements des listes CRL soit effectués au quotidien, sélectionnez **Download the CRL at (Télécharger la liste CRL à)**, puis l'heure à laquelle le téléchargement doit se produire.
2. Cliquez sur **Appliquer**.

Servez-vous également de cette page pour mettre immédiatement à jour la liste CRL.

1. Cliquez sur **Update CRL Now (Actualiser la liste CRL maintenant)** pour télécharger les listes CRL à un autre moment que celui défini. Par exemple, si votre abonnement comprend SSL Manager, téléchargez les listes CRL après l'installation de ce logiciel.

> **Remarque**
> Les fichiers CRL contenant des milliers de certifications, le téléchargement des listes CRL peut demander un certain temps et consommer des ressources CPU. Il est donc recommandé de télécharger les listes CRL lorsque le trafic Internet est peu important dans votre système.

2. Cliquez sur **View CRL Update Progress (Afficher la progression de la mise à jour de la liste CRL)** pour voir l'état de la mise à jour.

Pour plus d'informations sur les listes de révocation de certificats, consultez le document RFC 3280.

Protocole OCSP (Online certification status protocol)

OCSP est un protocole qui fonctionne sur une base requête/réponse. Cela signifie que, lorsqu'un site souhaite vérifier l'état de révocation d'un certificat, il envoie une requête à l'autorité de certification. L'autorité de certification lui répond ensuite, en confirmant la validité (ou la révocation) du certificat.

Comme il utilise des requêtes et ne télécharge pas de listes CRL, OCSP peut améliorer les performances. Toutefois, toutes les autorités de certification n'envoyant pas de réponse, les listes CRL peuvent fournir des informations sur l'état d'un plus grand nombre de certificats.

SSL Manager vous permet de mettre en cache les réponses OCSP relatives à l'état de révocation d'un certificat. Cette mise en cache des réponses peut se révéler utile dans les environnements de fort trafic SSL lorsqu'il est important d'économiser la bande passante.

Servez-vous de la page **Configurer > SSL > Validation > Revocation Settings (Paramètres de révocation)** pour configurer l'actualisation des informations de révocation par SSL Manager.

1. Définissez, en jours, la durée de mise en cache des données OCSP. Si vous préférez ne pas mettre en cache les données OCSP, entrez **0**. La durée maximale est de 1 000 jours.
2. Cliquez sur **Appliquer**.

Pour plus d'informations sur le protocole OCSP, consultez le document RFC 2560.

Gestion des accès aux sites Web HTTPS

Rubriques connexes :

- *Affichage des incidents*, page 153
- *Modification de l'état d'un incident*, page 154
- *Suppression d'un incident*, page 154
- *Modification du texte d'un message*, page 154
- *Affichage des détails d'un incident*, page 155
- *Ajout de sites Web à la liste des incidents*, page 155

Ces onglets peuvent vous aider à gérer l'accès aux sites Web et aider le service d'assistance à résoudre les problèmes d'accès. Les entrées et les modifications apportées dans cette page sont enregistrées dans la base de données SSL Manager.

Lorsqu'un client reçoit un message d'accès refusé parce que le site Web ne respecte pas les stratégies de sécurité, SSL Manager génère un *incident*. Voir *Affichage des incidents*, page 153.

Si vous voulez indiquer à SSL Manager comment traiter un site particulier, vous pouvez également l'ajouter dans la liste des incidents. Voir *Ajout de sites Web à la liste des incidents*, page 155.

Des informations complémentaires sur le dépannage sont disponibles dans SSL Manager Certificate Verification Engine v7.7.

Affichage des incidents

Servez-vous de la page **Configurer > SSL > Incidents** > **Incident List (Liste des incidents)** pour afficher un rapport répertoriant les incidents associés à la réception de messages d'accès refusé par les clients. Vous pouvez utiliser les champs de ce rapport pour indiquer à SSL Manager comment traiter par la suite l'accès demandé à un site donné.

- Pour afficher un incident spécifique, saisissez le numéro ID et cliquez sur **Rechercher**.
- Pour afficher la liste complète, cliquez sur **Afficher tout**.

Rapport d'incidents

Pour classer les incidents sur la base de l'une des colonnes, vous pouvez cliquer sur le petit triangle accolée au titre de la colonne en question.

Le rapport d'incidents comprend les champs suivants :

Champ	Description
ID	Attribué par le système, il s'agit là du numéro ID de l'incident, également appelé ID de ticket. Le service d'assistance peut demander à l'utilisateur l'ID indiqué dans le message d'erreur et le retrouver rapidement dans la liste des incidents URL. L'utilisateur voit l'ID de l'incident et un message de refus.
Statut (État)	Détermine le traitement futur de ce site Web par SSL Manager. Quatre conditions sont possibles : • Allow (Autoriser) Les utilisateurs peuvent accéder à ce site, y compris lorsque le certificat n'est pas valide. Le trafic est décrypté et la vérification du certificat est désactivée. • Blacklisted (Mis en liste noire) L'accès au site est entièrement bloqué. Les utilisateurs ne peuvent pas accéder à ce site, y compris lorsque le contournement de la vérification est configuré. • Block (Bloquer) En cas d'échec de la vérification du certificat, l'accès au site Web est bloqué, sauf lorsque le contournement de la vérification est configuré, auquel cas la page de blocage comprend un bouton « Visit site anyway (Accéder quand même au site) ». Voir *Contournement de la vérification*, page 150. • Tunnel Le site est mis en tunnel. Le trafic n'est pas décrypté et SSL Manager ne vérifie pas le certificat. La mise en tunnel permet de contourner l'examen des sites approuvés et d'améliorer les performances. **Remarque :** le tunnel par URL est uniquement pris en charge pour le trafic des proxy explicites. Vous pouvez modifier l'état d'un site Web via la liste déroulante de la colonne Action.

Champ	Description
Type	Indique si le site a été ajouté en fonction de son URL ou de son certificat. Il est recommandé d'ajouter des sites dans la liste des incidents par certificat. Voir *Ajout de sites Web à la liste des incidents*, page 155.
URL	URL d'un site dont le certificat n'a pas pu être validé
Message	Permet de modifier le message d'erreur. Pour plus d'informations sur la personnalisation des messages d'erreur, consultez la section *Modification du texte d'un message*, page 154. Le crayon et la loupe représentent chacun des liens. Pour plus d'informations sur ces liens, consultez la section *Affichage des détails d'un incident*, page 155.
Action	Permet de modifier l'état d'un incident. Permet également de supprimer l'incident. Voir *Suppression d'un incident*, page 154.

Modification de l'état d'un incident

Lorsque vous modifiez l'état d'un incident, vous modifiez le traitement que SSL Manager doit réserver à l'URL répertoriée dans le futur.

1. Sélectionnez **Configurer > SSL > Incidents** > **Incident List (Liste des incidents)**.
2. Sélectionnez l'un des éléments suivants dans la liste déroulante de la colonne Actions. Pour plus d'informations sur ces options, consultez la section *Rapport d'incidents*, page 153.
   - Tunnel
   - Block (Bloquer)
   - Liste noire
   - Allow (Autoriser)
3. Cliquez sur **Ok**. L'icône de la colonne Status (État) change pour refléter ce nouvel état.

Suppression d'un incident

1. Sélectionnez **Configurer > SSL > Incidents** > **Incident List (Liste des incidents)**.
2. Sélectionnez l'incident à supprimer. Si l'incident n'est pas visible, vous pouvez le rechercher via son ID. Voir *Affichage des incidents*, page 153.
3. Dans la colonne Action, sélectionnez **Supprimer** dans la liste déroulante Action, puis cliquez sur **Go (Ok)**.

Modification du texte d'un message

1. Sélectionnez **Configurer > SSL > Incidents** > **Incident List (Liste des incidents)**.
2. Localisez l'incident que vous souhaitez examiner plus précisément. Voir *Affichage des incidents*, page 153.
3. Cliquez sur le crayon pour ouvrir une fenêtre qui vous permet de modifier le texte de ce message d'erreur. Le service d'assistance peut par exemple ajouter d'autres détails à un message d'erreur.
4. Cliquez sur **Submit (Envoyer)** lorsque le nouveau texte est prêt ou sur **Close Window (Fermer la fenêtre)** si vous ne voulez pas le modifier.

Affichage des détails d'un incident

1. Sélectionnez **Configurer > SSL > Incidents** > **Incident List (Liste des incidents)**.
2. Localisez l'incident que vous souhaitez examiner plus précisément. Voir *Affichage des incidents*, page 153.
3. Cliquez sur la loupe pour afficher d'autres détails sur l'incident, par exemple :
   - Description (message qui s'affiche dans la liste des incidents)
   - Heure de création de l'incident
   - Heure de modification de l'incident
   - Nombre d'incidents (nombre de fois où les utilisateurs ont tenté d'accéder à ce site)

Ajout de sites Web à la liste des incidents

Utilisez la page **Configurer > SSL > Incidents** > **Add Website (Ajouter un site Web)** pour définir les sites que vous souhaitez autoriser, placer en liste noire ou mettre en tunnel. Les ID d'incident sont attribués aux sites ajoutés manuellement par ordre chronologique. Ces ID s'affichent dans la liste des incidents. Voir *Affichage des incidents*, page 153.

1. Saisissez l'URL du site que vous souhaitez ajouter à la liste des incidents.

> **Remarque**
> Lorsque vous spécifiez une adresse IPv6, ne la mettez **pas** entre crochets ([]).

2. Sélectionnez **By Certificate (Par certificat)** ou **By URL (Par URL)**.
   - L'option **By Certificate (Par certificat)** renforce la sécurité. Lorsque vous ajoutez un site Web par certificat, les clients ne peuvent pas contourner la stratégie en utilisant l'adresse IP à la place de l'URL. Lorsque vous sélectionnez l'option By Certificate (Par certificat), SSL Manager récupère le certificat du serveur et ajoute le site à la liste des incidents. Voir *Affichage des incidents*, page 153.

     Lorsque les sites sont bloqués par certificat, les certificats avec caractères génériques ne sont pas acceptés, y compris lorsque le nom commun est reconnu.
   - Sélectionnez **By URL (Par URL)** pour mettre le site en tunnel, l'autoriser ou le mettre en liste noire.
3. Dans la liste déroulante Action, indiquez si le site doit être ajouté avec l'état **Tunnel**, **Allow (Autoriser)** ou **Blacklist (Liste noire)**. Pour plus d'informations, consultez la section *Rapport d'incidents*, page 153.
   - **Tunnel** : (valide pour l'option **By URL (Par URL)** uniquement) le site est mis en tunnel. Le trafic n'est pas décrypté et SSL Manager ne vérifie pas le certificat.

> **Remarque**
> Le tunnel par URL est valide uniquement pour le trafic des proxy explicites. Pour mettre en tunnel le trafic d'un proxy transparent, utilisez les *Règles de contournement statique* du module ARM.

- **Allow (Autoriser)** : Les utilisateurs peuvent accéder à ce site, y compris lorsque le certificat n'est pas valide. Le trafic est décrypté et la vérification du certificat est désactivée.
- **Blacklist (Liste noire)** : l'accès au site est entièrement bloqué. Les utilisateurs ne peuvent pas accéder à ce site, y compris lorsque le contournement de la vérification est configuré.

4. Cliquez sur **Appliquer**.

Nous vous conseillons d'ajouter manuellement des sites à la liste des incidents après avoir surveillé votre trafic réseau pendant une certaine période, avec le moteur de vérification de certificats désactivé. (Voir *Configuration des paramètres de validation*, page 147.) Vous pourrez ainsi améliorer les performances en mettant les sites approuvés en tunnel et en bloquant ceux qui doivent rester inaccessibles. Pour plus d'informations sur l'attribution d'un état, par exemple la mise en tunnel, à un site ou un incident, consultez la section *Rapport d'incidents*, page 153.

Certificats des clients

Par sécurité, le serveur de destination peut demander un certificat de client.

Rubriques connexes :

- *Importation des certificats de clients*, page 157
- *Lorsqu'un certificat de client est toujours requis : liste des hôtes*, page 157
- *Suppression de certificats de clients*, page 157

Lorsqu'un certificat de client est demandé :

1. Sélectionnez **Configurer > SSL > Client Certificates (Certificats de clients)** > **Général**.
2. Sélectionnez **Tunnel** ou **Create incident (Créer un incident)** pour indiquer à SSL Manager comment traiter ce certificat et ce site. Vous devez choisir **Create incident (Créer un incident)** lorsque vous voulez prendre d'autres mesures que le tunnel (mise en liste blanche). Les listes blanches fourniront toujours le certificat au serveur. Reportez-vous à la section *Rapport d'incidents*, page 153 pour obtenir la liste des mesures possibles.
3. Cliquez sur **Appliquer**.

Importation des certificats de clients

Servez-vous de la page **Configurer > SSL > Client Certificates (Certificats de clients)** > **Importer** pour importer les certificats de l'organisation représentée par le client.

> **Important**
> N'oubliez pas de n'utiliser que des certificats au format X.509 et codés en base 64.

1. Entrez le nom du certificat du client.
2. Entrez la clé publique du certificat. Au besoin, demandez cette clé à votre administrateur réseau.
3. Entrez la clé privée du certificat. Au besoin, demandez cette clé à votre administrateur réseau.
4. Saisissez, puis confirmez la phrase secrète. Il est recommandé d'utiliser une solide phrase secrète, qui combine des chiffres, des caractères et des lettres minuscules et majuscules. Au besoin, demandez cette phrase secrète à votre administrateur réseau.
5. Cliquez sur **Importer**.

Lorsqu'un certificat de client est toujours requis : liste des hôtes

Servez-vous de la page **Configurer > SSL > Client Certificates (Certificats de clients)** > **Hostlist (Liste des hôtes)** pour répertorier les serveurs de destination devant systématiquement exiger un certificat de client. Assurez-vous d'importer le certificat avant de l'ajouter à la liste des hôtes. Voir *Importation des certificats de clients*, page 157.

1. Saisissez l'URL du serveur de destination demandant le certificat de client.
2. Dans la liste déroulante **Client Certificate (Certificat du client)**, sélectionnez le nom du certificat du client. Seuls les certificats que vous avez déjà importés s'affichent dans cette liste.
3. Cliquez sur **Ajouter**.

Suppression de certificats de clients

Servez-vous de la page **Configurer > SSL > Client Certificates (Certificats des clients) > Manage Certificates (Gérer les certificats)** pour supprimer les certificats de clients importés.

1. Sélectionnez le certificat à supprimer.
2. Cliquez sur **Supprimer**.

Configuration de la journalisation de SSL Manager

Rubriques connexes :

- *Durée de conservation des fichiers journaux SSL*, page 159
- *Croissance maximale de la taille des fichiers journaux SSL*, page 159
- *Champs devant s'afficher dans les fichiers journaux des accès SSL*, page 160

SSL Manager crée deux types de fichiers journaux :

- Des journaux d'activité. Ces journaux surveillent l'activité de SSL Manager et incluent les messages au niveau défini dans l'interface utilisateur.
- Des journaux d'accès

Vous pouvez enregistrer dans un journal l'activité du trafic entrant (client vers SSL Manager) et sortant (SSL Manager vers serveur). Vous avez la possibilité d'enregistrer les données dans le journal système (syslog) ou dans un fichier.

Servez-vous de la page **Configurer > SSL > Logging (Journalisation) > Général** pour définir le nom et l'emplacement des fichiers journaux.

1. Pour le trafic *entrant*, sélectionnez le type des fichiers journaux à conserver. Dans le cas des journaux d'activité, vous définissez le niveau de détail du journal.
2. Entrez un nombre compris entre 1 et 7 pour définir le niveau de détails à journaliser. Notez que chaque niveau donne davantage d'informations. Le niveau 7 est le plus détaillé. Les niveaux de journalisation et de granularité sont les suivants :

1 (alerte)	Événements du journal devant être corrigés immédiatement, par exemple un fichier système endommagé
2 (critique)	Événements du journal correspondant à des défaillances de périphériques
3 (normal)	Erreurs de journal
4 (avertissement)	Avertissements du journal
5 (notification)	Événements ne correspondant pas à des conditions d'erreur, mais demandant tout de même une attention particulière
6 (informations)	Messages d'informations du journal
7 (débogage)	Informations de débogage. Le niveau 7 comprend la plupart des résultats des journaux.

3. Indiquez si les données des journaux doivent être envoyées dans le journal système (syslog) ou dans un fichier.
4. Répétez l'Etape 2 et l'Etape 3 pour le fichier du journal des accès.
5. Pour le trafic *sortant*, reprenez la procédure de l'Etape 2 à l'Etape 4.
6. Cliquez sur **Appliquer**.

Les journaux sont écrits dans **/opt/WCG/sxsuite/log**.

Durée de conservation des fichiers journaux SSL

Un nouveau jeu de fichiers journaux est créé toutes les 24 heures. Par défaut, cette opération est effectuée à minuit. Cette rotation intervient quelle que soit la taille du fichier journal. De plus, le fichier journal est remplacé lorsqu'il atteint sa taille maximale avant la rotation prévue. Dans ce cas, la rotation prévue intervient tout de même à minuit. Pour plus d'informations sur la définition de la taille maximale du fichier journal, consultez la section *Croissance maximale de la taille des fichiers journaux SSL*, page 159.

Servez-vous de la page **Configurer > SSL > Logging (Journalisation) > Options** pour définir la durée de conservation des fichiers journaux.

1. Définissez, en jours, la durée de conservation des fichiers journaux. La valeur par défaut est 3.
2. Définissez les autres options de cette page, puis cliquez sur **Appliquer**.

Croissance maximale de la taille des fichiers journaux SSL

Les fichiers journaux sont remplacés chaque soir, à minuit. Un nouveau fichier journal est toutefois créé lorsque sa taille maximale est atteinte, y compris avant la rotation quotidienne prévue. La taille des fichiers journaux étant vérifiée toutes les minutes, il est possible que l'un d'eux dépasse sa taille maximale pendant une brève période.

Lorsqu'un fichier journal atteint sa taille maximale, il est enregistré avec une extension « *x* » (où *x* correspond à 1, 2, 3, etc.) et un nouveau fichier est créé. Lorsque cette opération est nécessaire à plusieurs reprises au cours d'une période de 24 heures, vous devez définir le nombre de générations de fichiers à conserver. Pour plus d'informations sur la rotation des journaux, consultez la section *Durée de conservation des fichiers journaux SSL*, page 159.

Servez-vous de la page **Configurer > SSL > Logging (Journalisation) > Options** pour définir la taille maximale des fichiers journaux.

1. Indiquez, en Ko, la taille maximale des fichiers journaux. La valeur par défaut est 50 000 Ko.
2. Pour les générations, définissez le nombre de fichiers journaux à conserver lorsque le fichier atteint sa taille maximale à plusieurs reprises avant la rotation quotidienne. Lorsque ce nombre est atteint et que de nouveaux fichiers journaux sont créés, le plus ancien est supprimé. La valeur par défaut est 3 générations.
3. Définissez les autres options de cette page, puis cliquez sur **Appliquer**.

Champs devant s'afficher dans les fichiers journaux des accès SSL

Servez-vous de la page **Configurer > SSL > Logging (Journalisation) > Options** pour ajouter ou supprimer des champs dans le fichier journal.

1. Supprimez ou ajouter des champs dans le volet de personnalisation des fichiers journaux des accès. Les champs disponibles sont les suivants :

time_stamp	Horodatage au format [AAAA.MM.JJ HH:MM:SS]
time_of_day	Horodatage au format brut : Sec.mSec à partir du 1er janvier 1970 UTC
src_ip	Adresse IP du client
auth_user	Utilisateur qui a été authentifié
account	Compte auquel l'utilisateur appartient
profile	Profil de l'utilisateur
req_line	Requête au format suivant : « method path protocol/ version.subversion ». Par exemple : GET / HTTP/1.1
status_code	Code de réponse d'état HTTP envoyé par le serveur Web
user_agent	Nom du navigateur du client
referer	Section hôte de l'URL
content_type	Contenu, par exemple HTML, texte, image, etc.
content_length	Longueur du contenu, en octets
server_host	Adresse IP du serveur Web
bytes_from_client	Octets transférés du client vers SSL Manager
bytes_to_client	Octets transférés de SSL Manager vers le client
bytes_from_server	Octets transférés du serveur Web vers SSL Manager
bytes_to_server	Octets transférés de SSL Manager vers le serveur Web

2. Cliquez sur **Appliquer**.

Personnalisation des messages d'échec des connexions SSL

Vous pouvez personnaliser le message reçu par les utilisateurs dans les cas suivants :

- Ils tentent de se connecter à un site dont le certificat n'est pas valide. Voir *Échec de validation du certificat*, page 161.
- Un échec de connexion s'est produit. Voir *Échec des connexions SSL*, page 162.

Les variables suivantes sont disponibles dans les modèles de messages.

%P	Protocole (HTTP ou HTTPS)
%h	Adresse IP et port de l'hôte du proxy à l'origine du message
%o	Adresse IP de l'hôte du proxy à l'origine du message
%H	Nom d'hôte distant de la requête
%t	Heure
%s	Nom du serveur SSL Manager
%u	URL complète
$$DETAILS	Message d'erreur détaillé
$$TICKET_ID	Numéro ID de l'incident

Échec de validation du certificat

Servez-vous de la page **Configurer > SSL > Customization (Personnalisation) > Certificate Failure (Échec de certificat)** pour personnaliser le message reçu par les utilisateurs en cas d'échec de validation du certificat.

> **Remarque**
> Vous pouvez cliquez sur **Aperçu** pour voir l'apparence du message par défaut.

1. Modifiez le code HTML dans la fenêtre pour qu'il se reflète dans votre message. Pour obtenir la liste des variables utilisables dans le message, consultez la section *Personnalisation des messages d'échec des connexions SSL*, page 161.
2. Cliquez sur **Aperçu** pour voir vos modifications.
3. Répétez les étapes 1 et 2 jusqu'à ce que le message vous convienne.
4. Cliquez sur **Appliquer** pour confirmer vos modifications ou sur **Annuler** pour retrouver le message d'origine.

Échec des connexions SSL

Servez-vous de la page **Configurer > SSL > Customization (Personnalisation) > Connect Error (Erreur de connexion)** pour personnaliser le message reçu par les utilisateurs lorsque SSL Manager ne parvient pas à se connecter au serveur Web de destination.

> **Remarque**
> Vous pouvez cliquez sur **Aperçu** pour voir l'apparence du message par défaut.

1. Modifiez le texte dans la fenêtre pour qu'il se reflète dans votre message. Pour obtenir la liste des variables utilisables dans le message, consultez la section *Personnalisation des messages d'échec des connexions SSL*, page 161.
2. Cliquez sur **Aperçu** pour voir vos modifications.
3. Répétez les étapes 1 et 2 jusqu'à ce que le message vous convienne.
4. Cliquez sur **Appliquer** pour confirmer vos modifications ou sur **Annuler** pour retrouver le message d'origine.

14 Sécurité

Websense Content Gateway vous permet d'établir une communication sécurisée entre le proxy et les autres ordinateurs du réseau. Vous pouvez :

- Contrôler les clients autorisés à accéder au proxy. Voir *Contrôle de l'accès des clients au proxy*, page 163.
- Contrôler l'accès à Content Gateway Manager via :
  - Des comptes d'administrateur (voir *Définition de l'ID et du mot de passe de l'administrateur*, page 164, et *Création d'une liste de comptes d'utilisateur*, page 165)
  - La protection SSL (Secure Sockets Layer) pour un accès avec cryptage et authentification (voir *Utilisation de SSL pour l'administration sécurisée*, page 166)
- Créer des règles de filtrage afin de contrôler l'accès à Internet, en particulier les conditions d'authentification spéciales, et les autres trafics passant par le proxy. Voir *Règles de filtrage*, page 167.
- Configurer l'intégration de Content Gateway à votre pare-feu et contrôler le trafic via un ou plusieurs serveurs SOCKS. Voir *Configuration de l'intégration du pare-feu SOCKS*, page 171.
- Configurer Content Gateway pour qu'il utilise plusieurs serveurs DNS conformément à la configuration de la sécurité de votre site. Voir *Utilisation de l'option de division DNS*, page 175.
- Configurer Content Gateway pour qu'il authentifie les utilisateurs. Le proxy prend en charge l'Authentification Windows intégrée (avec Kerberos), NTLM hérité (NTLMSSP), LDAP et RADIUS. Plusieurs méthodes d'authentification sont également prises en charge avec authentification dans plusieurs domaines Kerberos. Voir *Authentification des utilisateurs du proxy*, page 175.

Contrôle de l'accès des clients au proxy

Vous pouvez configurer Content Gateway pour qu'il n'autorise que certains clients à utiliser le proxy.

Pour autoriser l'accès, définissez les adresses IP et les plages d'adresses IP des clients dans le fichier **ip_allow.config**.

Pour refuser l'accès à certains clients, n'incluez pas leurs adresses IP dans ce fichier.

1. Ouvrez la page **Configurer > Sécurité > Connection Control (Contrôle des connexions) > Proxy Access (Accès au proxy)**.

2. Cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **ip_allow.config** dans l'éditeur de fichiers de configuration.
3. Renseignez les champs fournis, puis cliquez sur **Ajouter**. Tous les champs sont décris à la section *Options de configuration*.
4. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis cliquez sur **Fermer**.

> **Remarque**
> Lorsqu'un client non autorisé tente d'accéder à Content Gateway, un message s'affiche dans son navigateur pour signaler que le contenu demandé ne peut pas être fourni.

Contrôle de l'accès à Content Gateway Manager

Vous pouvez limiter l'accès à Content Gateway Manager de manière à être certain que seuls les utilisateurs authentifiés peuvent modifier les options de configuration et afficher les performances et les statistiques du trafic réseau.

Vous pouvez :

- Définir l'ID et le mot de passe de l'administrateur principal. Un utilisateur qui se connecte à Content Gateway Manager avec l'ID d'administrateur a accès à la totalité des activités de Content Gateway Manager. Voir *Définition de l'ID et du mot de passe de l'administrateur*, page 164.
- Créer et gérer la liste des comptes d'utilisateur déterminant les personnes autorisées à se connecter à Content Gateway Manager et les activités qu'elles peuvent y effectuer. Voir *Création d'une liste de comptes d'utilisateur*, page 165.
- Créer une liste de contrôle d'accès des adresses IP définissant les ordinateurs autorisés à accéder à Content Gateway Manager. Voir *Contrôle de l'accès des hôtes à Content Gateway Manager*, page 166.
- Utiliser SSL pour l'administration sécurisée. Voir *Utilisation de SSL pour l'administration sécurisée*, page 166.
- Obliger les administrateurs à se connecter à TRITON Unified Security Center, avec ou sans authentification à deux facteurs, puis à utiliser la page d'accès à TRITON – Web Security Content Gateway pour se connecter à Content Gateway Manager. Voir *Accès à Content Gateway Manager*, page 11.

Définition de l'ID et du mot de passe de l'administrateur

Lors de l'installation, vous affectez un mot de passe qui contrôle l'accès administratif à Content Gateway Manager. Tout utilisateur qui se connecte à Content Gateway Manager à l'aide de l'ID et du mot de passe appropriés peut afficher toutes les statistiques dans l'onglet Monitor (Surveiller) et modifier les options de configuration dans l'onglet Configurer.

Vous pouvez à tout moment modifier l'ID et le mot de passe de l'administrateur.

1. Ouvrez l'onglet **Configurer > Mon proxy > UI Setup (Configuration de l'interface utilisateur) > Connexion**.

2. Assurez-vous que l'option **Authentification de base** soit activée.

   Lorsque l'authentification de base est désactivée, tous les utilisateurs peuvent accéder à Content Gateway Manager sauf si vous avez configuré une liste d'adresses IP pour lesquelles l'accès est refusé (voir *Contrôle de l'accès des hôtes à Content Gateway Manager*, page 166).

3. Pour modifier l'ID de l'administrateur actuel, saisissez un nouvel ID dans le champ **Connexion** de la section **Administrateur**.

4. Pour modifier le mot de passe actuel, saisissez ce dernier dans le champ Ancien mot de passe. Saisissez le nouveau mot de passe dans le champ Nouveau mot de passe, puis à nouveau dans le champ New Password (Retype) (Confirmer le nouveau mot de passe).

   Si vous avez oublié le mot de passe actuel de l'administrateur, consultez la section *Comment accéder à Content Gateway Manager si j'ai oublié le mot de passe de l'administrateur principal ?*, page 466.

5. Cliquez sur **Appliquer**.

Création d'une liste de comptes d'utilisateur

Lorsqu'un unique ID/mot de passe d'administrateur pour Content Gateway Manager ne répond pas à vos besoins en matière de sécurité, vous pouvez créer une liste de comptes d'utilisateur définissant les personnes autorisées à accéder à Content Gateway Manager et les actions que ces personnes peuvent effectuer.

1. Ouvrez l'onglet **Configurer > Mon proxy > UI Setup (Configuration de l'interface utilisateur) > Connexion**.
2. Entrez le nom de l'utilisateur autorisé à accéder à Content Gateway Manager.
3. Entrez son mot de passe et saisissez-le une deuxième fois dans le champ New Password (Retype) (Confirmer le nouveau mot de passe).
4. Cliquez sur **Appliquer**.
5. Dans la liste déroulante **Accès** du tableau des utilisateurs, sélectionnez les actions Content Gateway Manager que l'utilisateur peut effectuer :
   - Sélectionnez **No Access (Aucun accès)** pour désactiver l'accès à Content Gateway Manager pour cet utilisateur.
   - Sélectionnez **Monitor Only (Surveiller uniquement)** pour autoriser l'utilisateur à consulter les statistiques dans l'onglet Monitor (Surveiller) uniquement.
   - Sélectionnez **Monitor and View Configuration (Surveiller et afficher la configuration)** pour autoriser l'utilisateur à afficher les statistiques dans l'onglet Monitor (Surveiller) et à afficher les options de configuration dans l'onglet Configurer.
   - Sélectionnez **Monitor and Modify Configuration (Surveiller et modifier la configuration)** pour autoriser l'utilisateur à afficher les statistiques dans l'onglet **Monitor (Surveiller)** et à modifier les options de configuration dans l'onglet Configurer.
6. Cliquez sur **Appliquer**.
7. Répétez l'Etape 2 à Etape 6 pour chaque utilisateur autorisé à accéder à Content Gateway Manager.
8. Assurez-vous que l'option **Authentification de base** soit activée.

   Content Gateway ne vérifie les noms d'utilisateur et les mots de passe que si cette option est activée.

Contrôle de l'accès des hôtes à Content Gateway Manager

En plus d'utiliser un ID d'administrateur et des comptes d'utilisateur, vous pouvez contrôler les hôtes autorisés à accéder à Content Gateway Manager.

1. Sélectionnez **Configurer > Mon proxy > UI Setup Access (Accès à la configuration de l'interface utilisateur)**.
2. Dans la zone Access Control (Contrôle d'accès), cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **mgmt_allow.config** dans l'éditeur de fichiers de configuration.
3. Renseignez les champs fournis, puis cliquez sur **Ajouter**. L'ensemble des champs sont décris à la section *UI Setup (Configuration de l'interface utilisateur)*, page 270.
4. Cliquez sur **Appliquer**, puis sur **Fermer**.

Utilisation de SSL pour l'administration sécurisée

Pour protéger la surveillance administrative distante et la configuration via Content Gateway Manager, Websense prend en charge le protocole Secure Sockets Layer (SSL). La sécurité SSL assure une authentification aux deux extrémités d'une connexion réseau à l'aide de certificats et fournit la confidentialité à l'aide du cryptage.

Pour utiliser SSL, vous devez :

- Obtenir un certificat SSL
- Activer l'option SSL de Content Gateway Manager

Obtention d'un certificat SSL

Vous pouvez obtenir un certificat SSL auprès d'une autorité de certification reconnue (par exemple, VeriSign). Installez le certificat dans le répertoire **config** de Content Gateway (**/opt/WCG/bin**). Vous devez remplacer le nom du certificat par le nom de fichier par défaut **private_key.pem** ou spécifier le nom du certificat via Content Gateway Manager (suivez la procédure indiquée à la section *Activation de SSL*, page 166).

Activation de SSL

Après avoir obtenu un certificat SSL, vous pouvez activer SSL.

1. Ouvrez l'onglet **Configurer > Mon proxy > UI Setup (Configuration de l'interface utilisateur) > Général**.
2. Activez l'option **HTTPS**.
3. Dans le champ Certificate File (Fichier du certificat), spécifiez le nom de fichier du certificat SSL.

   Vous ne devez modifier ce nom de fichier que si le fichier du certificat n'utilise pas le nom par défaut **private_key.pem**.
4. Cliquez sur **Appliquer**.

Mode FIPS 140-2

La norme FIPS (Federal Information Processing Standard) 140-2 est une norme de sécurité définie par le gouvernement des États-Unis pour les modules cryptographiques matériels et logiciels. Les modules pour lesquels le respect de cette norme est certifié permettent au gouvernement et aux autres utilisateurs d'être certains que la cryptographie du système répond à la norme la plus exigeante.

La bibliothèque cryptographique utilisée dans Content Gateway version 7.7 a été soumise à la certification FIPS 140-2. Consultez la page de validation du programme CMVP (Cryptographic Module Validation Program) pour plus d'informations.

Par défaut, la norme FIPS 140-2 ne s'applique pas aux connexions SSL.

Vous pouvez configurer Content Gateway pour imposer la norme FIPS 140-2 aux connexions HTTPS afin d'être certain que les connexions HTTPS utilisent bien les algorithmes TLS v1 et FIPS 140-2 approuvés. Toutefois, une fois activée, l'option n'est pas réversible sans réinstallation complète de Content Gateway. Si Content Gateway est installé sur un dispositif, ce dernier doit être réimagé.

Pour activer FIPS 140-2 sur les connexions HTTPS :

1. Dans Content Gateway Manager, sélectionnez **Configurer > Sécurité > FIPS Security (Sécurité FIPS)**.
2. Examinez l'avertissement, sélectionnez **Enabled (Activé),** puis cliquez sur **Appliquer**.
3. Si vous êtes certain de vouloir activer FIPS, redémarrez Content Gateway.
4. Si vous ne souhaitez pas activer FIPS, sélectionnez Désactiver, puis cliquez sur Appliquer.

Règles de filtrage

Content Gateway permet de créer des règles chargées de rechercher certains paramètres dans les requêtes et, en cas de correspondance, d'imposer l'action spécifiée. Des règles peuvent être créées pour :

- Refuser ou autoriser des requêtes d'URL
- Insérer des en-têtes personnalisés
- Autoriser des applications spécifiées ou des requêtes de sites Web à contourner l'authentification
- Conserver ou supprimer les informations d'en-tête dans les requêtes des clients
- Empêcher les applications spécifiées de passer par le proxy

Remarque

Pour créer des règles pour l'authentification NTLM et LDAP, consultez la section *Authentification dans plusieurs domaines Kerberos*, page 194. Pour découvrir les options d'authentification de Content Gateway, consultez la section *Authentification des utilisateurs du proxy*, page 175.

Les règles de filtrage sont créées et modifiées dans l'onglet **Configurer** > **Sécurité** > **Access Control (Contrôle d'accès) > Filtering (Filtrage)**. Les règles sont stockées dans le fichier **filter.config**.

Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas. Seule la première correspondance s'applique. Lorsque aucune règle ne correspond, la requête poursuit sa route.

Les spécificateurs secondaires sont facultatifs. Il est possible d'utiliser plusieurs spécificateurs secondaires dans une même règle. Vous ne pouvez cependant pas répéter un même spécificateur secondaire.

Lorsque vous ajoutez, supprimez ou modifiez une règle, redémarrez Content Gateway.

Pour plus d'informations sur la structure des règles stockées, consultez la section *Fichier de configuration filter.config*.

Création de règles de filtrage

1. Ouvrez l'onglet **Configurer** > **Sécurité** > **Access Control (Contrôle d'accès) > Filtering (Filtrage)**, puis cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le *Fichier de configuration filter.config* dans l'éditeur de fichiers de configuration.
2. Sélectionnez **Rule Type (Type de règle)** dans la liste déroulante. Le type de règle définit l'action appliquée par la règle. Les options prises en charge sont :

   allow (autoriser) : permet aux requêtes URL spécifiées d'ignorer l'authentification. Le proxy met en cache, puis envoie le contenu demandé.

   deny (refuser) : refuse les requêtes d'objets associées à des destinations spécifiques. Lorsqu'une requête est refusée, le client reçoit un message d'accès refusé.

   keep_hdr : définit les informations d'en-tête à conserver dans les requêtes des clients.

   strip_hdr : définit les informations d'en-tête à supprimer dans les requêtes des clients.

   add_hdr : entraîne l'insertion d'une paire en-tête/valeur personnalisée. Dans ce cas, les options **Custom Header (En-tête personnalisé)** et **Header Value (Valeur de l'en-tête)** doivent obligatoirement être définies. Cette option permet de prendre en charge les hôtes de destination exigeant une paire en-tête/valeur spécifique. Pour obtenir un exemple, reportez-vous à la section *Création d'une règle add_hdr pour autoriser Google Enterprise Gmail* ci-dessous.

   Remarque

   Le type de règle « radius » n'est **pas** pris en charge.

3. Sélectionnez **Primary Destination Type (Type de destination principale)** et saisissez une valeur correspondante dans le champ **Primary Destination Value (Valeur de la destination principale)**. Les différents types de destinations principales comprennent :

   dest_domain : nom du domaine demandé. La valeur est un nom de domaine.

   dest_host : nom d'hôte demandé. La valeur est un nom d'hôte.

   dest_ip : adresse IP demandée. La valeur est une adresse IP.

   url_regex : expression régulière que l'on retrouve dans une URL. La valeur est l'expression régulière.

4. Si le type de destination principale est **keep_hdr** ou **strip_hdr**, sélectionnez le type d'informations à conserver ou à supprimer dans la liste déroulante **Header Type (Type d'en-tête)**. Options proposées :
   - **date**
   - **hôte**
   - **cookie**
   - **client_ip**
5. Si la règle ne s'applique qu'au trafic entrant passant par un port spécifique, saisissez une valeur pour **Proxy Port (Port du proxy)**.
6. Si le type de règle est **add_hdr**, définissez les options **Custom Header (En-tête personnalisé)** et **Header Value (Valeur de l'en-tête)**. Les valeurs de **Custom Header (En-tête personnalisé)** et **Header Value (Valeur de l'en-tête)** doivent correspondre aux valeurs attendues par l'hôte de destination. Reportez-vous à l'exemple donné ci-dessous pour Google Business Gmail.
7. Définissez les valeurs des **Spécificateurs secondaires** requis ou souhaités. Ces derniers comprennent :

   Time (Heure) : définit une plage horaire, par exemple 08:00 à 14:00.

   Prefix (Préfixe) : définit un préfixe situé dans le chemin d'une URL.

   Suffix (Suffixe) : définit un suffixe de fichier dans l'URL.

   Source IP address (Adresse IP source) : définit l'adresse IP d'un client unique ou une plage d'adresses IP de clients.

   Port : définit le port dans une URL demandée.

   Method (Méthode) : définit une méthode d'URL de requête :
   - get
   - post
   - put
   - trace

   Scheme (Schéma) : définit le protocole d'une URL demandée. Les options disponibles sont :
   - HTTP
   - HTTPS
   - FTP (pour FTP sur HTTP uniquement)

   User-Agent (Agent-utilisateur) : définit la valeur User-Agent de l'en-tête de la requête. Il s'agit d'une expression régulière (regex).

   Vous pouvez utiliser le champ User-Agent pour créer des règles de filtrage des applications permettant :
   - D'autoriser les applications qui ne gèrent pas correctement les demandes d'authentification à contourner l'authentification
   - De bloquer l'accès à Internet de certaines applications de type client

   Pour obtenir davantage d'informations et quelques exemples, consultez l'article intitulé « When authentication prevents devices, browsers, and custom applications from working with the proxy (À quel moment l'authentification empêche les périphériques, les navigateurs et les applications personnalisées de fonctionner avec le proxy) » de la base de connaissances Websense.
8. Lorsque la définition de la règle est terminée, cliquez sur **Ajouter** pour ajouter la règle, puis sur **Appliquer** pour l'enregistrer.

9. Lorsque l'ajout de règles est terminé, cliquez sur **Appliquer** pour enregistrer toutes les modifications, puis sur **Fermer** pour fermer la fenêtre d'édition.
10. Pour que les nouvelles règles entrent en vigueur, sélectionnez la fenêtre Content Gateway Manager et redémarrez Content Gateway.

Modification d'une règle

1. Ouvrez l'onglet **Configurer** > **Sécurité** > **Access Control (Contrôle d'accès) > Filtering (Filtrage)**, puis cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le *Fichier de configuration filter.config* dans l'éditeur de fichiers de configuration.
2. Dans la liste, sélectionnez la règle à modifier et changez ses valeurs en fonction de vos besoins.
3. Cliquez sur **Set (Définir)** pour actualiser la règle, puis sur **Appliquer** pour l'enregistrer.
4. Cliquez sur **Fermer** pour fermer la fenêtre de l'éditeur.
5. Pour que les modifications entrent en vigueur, sélectionnez la fenêtre Content Gateway Manager et redémarrez Content Gateway.

Création d'une règle add_hdr pour autoriser Google Enterprise Gmail

Le mécanisme sous forme d'en-tête personnalisé placé dans la requête qui est utilisé par Google lui permet de reconnaître et d'autoriser ou de bloquer l'accès à la messagerie de l'entreprise et aux autres applications Google de l'entreprise.

Pour qu'une solution Google fonctionne pour la messagerie Gmail de l'entreprise avec TRITON – Web Security et Content Gateway :

1. Dans TRITON – Web Security, autorisez la catégorie Web Security **Internet Communication (Communication Internet) > General Email (Courrier électronique général)**.
2. Dans Content Gateway Manager, activez **HTTPS** (décryptage SSL). Si votre site n'utilise pas encore SSL Manager pour gérer les connexions HTTPS, apprenez à connaître cette fonction avant de l'activer.
3. Dans la page **Configurer > Sécurité > Access Control (Contrôle d'accès)** de Content Gateway Manager, ouvrez le fichier **filter.config** et créez une règle **add_hdr**.

> **Remarque**
> Le type de règle **add_hdr** peut être utilisé avec n'importe quel site qui utilise une paire en-tête-valeur pour effectuer une action particulière.

   a. Sélectionnez **add_hdr**.
   b. Dans **Primary Destination Type (Type de destination principale)**, sélectionnez **dest_domain**.
   c. Dans **Primary Destination Value (Valeur de la destination principale)**, spécifiez « mail.google.com ».
   d. Dans le champ **Custom Header (En-tête personnalisé)**, spécifiez « X-GoogApps-Allowed-Domains ».

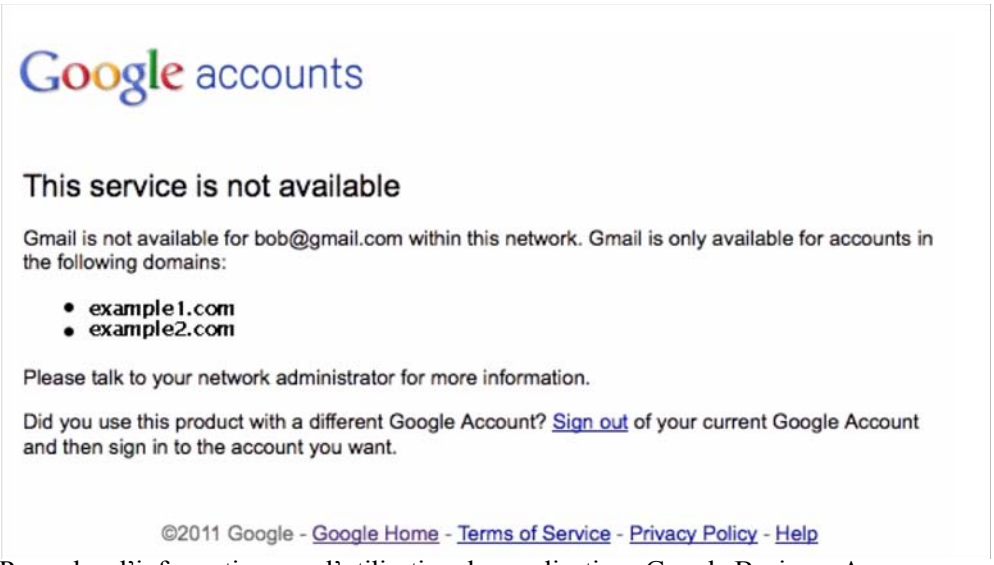
e. Dans le champ **Header Value (Valeur de l'en-tête)**, spécifiez votre domaine ou une liste de domaines séparés par des virgules. Par exemple : www.exemple1.com,www.exemple2.com

f. Cliquez sur **Ajouter** pour ajouter la règle.

g. Cliquez sur **Appliquer** pour enregistrer toutes les modifications, puis sur **Fermer** pour fermer la fenêtre de l'éditeur.

h. Pour que la nouvelle règle entre en vigueur, redémarrez Content Gateway.

Lorsqu'un utilisateur tente d'accéder à des services Google à l'aide d'un compte non autorisé, Google présente une page de blocage similaire à celle-ci :



Pour plus d'informations sur l'utilisation des applications Google Business Apps avec Websense Web Security Gateway et Web Security Gateway Anywhere, consultez [link to KBA]. Pour obtenir la description de la solution de filtrage Google, consultez l'article Block access to consumer accounts and services while allowing access to Google Apps for your organization (Bloquer l'accès aux comptes et aux services des clients tout en autorisant l'accès aux applications Google Apps dans votre entreprise).

Configuration de l'intégration du pare-feu SOCKS

Rubriques connexes :

- *Configuration des serveurs SOCKS*, page 172
- *Définition des options de proxy SOCKS*, page 174
- *Définition du contournement des serveurs SOCKS*, page 174

SOCKS est communément utilisé comme pare-feu réseau autorisant les hôtes situés derrière un serveur SOCKS à disposer d'un accès complet à Internet, tout en empêchant l'accès non autorisé depuis Internet aux hôtes protégés par le pare-feu.

À réception d'une demande de contenu non présent dans le cache, Content Gateway doit demander ce contenu au serveur d'origine. Dans une configuration SOCKS, au

lieu d'accéder directement au serveur d'origine, le proxy passe par un serveur SOCKS. Ce serveur SOCKS autorise la communication entre le proxy et le serveur d'origine et relaye les données vers ce dernier. Le serveur d'origine renvoie ensuite le contenu au proxy par l'intermédiaire du serveur SOCKS. Lorsque la mise en cache est activée, Content Gateway met le contenu en cache avant de l'envoyer au client.

- Content Gateway peut jouer le rôle de client SOCKS, auquel cas il reçoit et dessert les requêtes HTTP ou FTP de manière traditionnelle.
- Content Gateway peut jouer le rôle de proxy SOCKS, en relayant les requêtes destinées au et provenant du serveur SOCKS (en général sur le port 1080).
- Lorsque Content Gateway est installé dans un dispositif V-Series, il peut jouer le rôle de serveur SOCKS et assurer tous les services d'un serveur SOCKS. (Lorsque Content Gateway n'est **pas** installé dans un dispositif, il ne peut pas jouer le rôle de serveur SOCKS.)

Configuration des serveurs SOCKS

Content Gateway peut être configuré pour fonctionner avec un ou plusieurs serveurs SOCKS dans votre réseau. Lorsque Content Gateway est installé dans un dispositif V-Series, un serveur SOCKS est inclus avec le module.

> **Remarque**
>
> Lorsque Content Gateway n'est**pas** installé dans un dispositif V-Series, aucun serveur SOCKS n'est fourni avec Content Gateway.

Pour configurer des serveurs SOCKS :

1. Activez la fonction SOCKS.
   a. Ouvrez l'onglet **Configurer > Mon proxy > De base > Général**.
   b. Dans la section **Sécurité** du tableau **Features (Fonctions)**, cliquez sur **SOCKS On (SOCKS activé)**, puis sur **Appliquer**.
   c. Redémarrez Content Gateway.
2. Spécifiez la version SOCKS.
   a. Sélectionnez **Configurer > Sécurité > SOCKS > Général**.
   b. Sélectionnez la version SOCKS en exécution dans vos serveurs SOCKS, puis cliquez sur **Appliquer**.
3. Pour configurer le serveur SOCKS sur dispositif V-Series :
   a. Sélectionnez l'onglet **Serveur**.
   b. Dans le volet **On-Appliance SOCKS Server (Serveur SOCKS sur dispositif)**, sélectionnez **Enabled (Activé)**, puis cliquez sur **Appliquer**.

      Une entrée est créée pour ce serveur dans le fichier **socks_server.config**.
   c. Pour modifier l'entrée par défaut, cliquez sur **Edit File (Modifier le fichier)** dans le volet **SOCKS Server (Serveur SOCKS)**. Dans l'éditeur, sélectionnez la règle **On-Appliance-SOCKS-Server (Serveur SOCKS sur dispositif)**.

      Vous pouvez alors modifier le port et indiquer s'il s'agit du serveur SOCKS par défaut et si l'authentification du serveur doit s'appliquer.

      Vous ne pouvez pas modifier le nom du serveur ni son adresse IP, qui correspond toujours à l'adresse de bouclage.

      Lorsque les modifications nécessaires sont terminées, cliquez sur **Set (Définir)**.

4. Pour configurer l'utilisation d'autres serveurs SOCKS dans votre réseau :
   a. Ouvrez l'onglet **Serveur**, puis cliquez sur **Edit File (Modifier le fichier)** dans le volet **SOCKS Server (Serveur SOCKS)**.
   b. Entrez un nom de serveur SOCKS.
   c. Entrez l'adresse IP du serveur SOCKS ou un nom de domaine que le serveur DNS de votre réseau peut résoudre.
   d. Indiquez s'il doit s'agir du serveur SOCKS par défaut.
   e. Si l'authentification doit être utilisée, fournissez un nom d'utilisateur et un mot de passe SOCKS.
   f. Cliquez sur **Set (Définir)** pour ajouter ce serveur à la liste.

      Vous pouvez toujours revenir dans l'éditeur, sélectionner la règle, apporter des modifications, puis cliquer sur **Set (Définir)** pour les enregistrer.
5. Lorsqu'il existe plusieurs serveurs SOCKS, vous pouvez les classer par ordre de priorité, après ou pendant leur ajout, en sélectionnant une entrée et en la déplaçant vers le haut ou le bas dans la liste à l'aide des flèches haut et bas.
6. Cliquez sur **Appliquer** pour accepter vos modifications, puis sur **Fermer** pour fermer l'éditeur.
7. Le volet **SOCKS Server Rules (Règles des serveurs SOCKS)** vous permet de créer des règles spécifiques de routage et de contournement par adresse IP de destination. Voir *Définition du contournement des serveurs SOCKS*, page 174.
8. Pour vérifier les options de configuration s'appliquant à l'ensemble des serveurs SOCKS, ouvrez l'onglet **Options**.
   a. Vérifiez et ajustez la valeur **Server Connection Timeout (Expiration des connexions des serveurs)**. Cette option définit le nombre de secondes pendant lesquelles Content Gateway doit tenter de se connecter à un serveur SOCKS avant expiration.
   b. Vérifiez et ajustez la valeur **Connection Attempts Per Server (Tentatives de connexion par serveur)**. Cette option définit le nombre de fois où Content Gateway doit tenter de se connecter à un certain serveur SOCKS avant de le désigner comme indisponible.
   c. Vérifiez et ajustez la valeur **Server Pool Connection Attempts (Tentatives de connexion au pool de serveurs)**. Cette option définit le nombre de fois où Content Gateway doit tenter de se connecter à un certain serveur SOCKS du pool avant d'abandonner.
9. Lorsque la configuration des serveurs SOCKS est terminée, cliquez sur **Appliquer**, puis sélectionnez **Configurer > Mon proxy > Général** et redémarrez Content Gateway.

Pour retirer un serveur de la liste :

1. Dans le volet **SOCKS Server (Serveur SOCKS)**, cliquez sur **Edit File (Modifier le fichier)**.
2. Dans la liste, sélectionnez l'entrée à supprimer, puis cliquez sur le **X** situé à gauche de la liste.
3. Cliquez sur **Appliquer**, puis sur **Fermer** lorsque vous êtes prêt à quitter l'éditeur.
4. Lorsque la configuration est terminée, sélectionnez **Configurer > Mon proxy > Général** et redémarrez Content Gateway.

Définition des options de proxy SOCKS

Pour configurer Content Gateway en tant que proxy SOCKS, vous devez activer l'option de proxy SOCKS et spécifier le port sur lequel Content Gateway accepte le trafic SOCKS provenant des clients SOCKS.

En tant que proxy SOCKS, Content Gateway peut recevoir les paquets SOCKS (en général sur le port 1080) provenant des clients et transmettre les requêtes directement au serveur SOCKS.

> **Remarque**
> Vous devez définir les options de proxy SOCKS en plus d'activer l'option SOCKS et de définir les informations des serveurs SOCKS décrites dans la section *Configuration des serveurs SOCKS*, page 172.

1. Sélectionnez **Configurer** > **Sécurité** > **SOCKS > Proxy**.
2. Activez l'option **SOCKS Proxy (Proxy SOCKS)**.
3. Spécifiez le port sur lequel Content Gateway accepte le trafic SOCKS. Le port par défaut est le 1080.
4. Cliquez sur **Appliquer**.
5. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Définition du contournement des serveurs SOCKS

Vous pouvez configurer Content Gateway pour qu'il ignore les serveurs SOCKS et qu'il accède directement à certains serveurs d'origine.

1. Sélectionnez **Configurer > Sécurité > SOCKS > Serveur**. Dans le volet **SOCKS Server Rules (Règles des serveurs SOCKS)**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le fichier **socks.config**.
2. Pour modifier une règle existante, sélectionnez-la dans la liste, apportez les modifications nécessaires, puis cliquez sur **Set (Définir)**.
3. Pour créer une nouvelle règle, définissez les paramètres, puis cliquez sur **Ajouter**.
   a. Sélectionnez un type de règle dans le champ **Rule Type** :

      Route through SOCKS server (Acheminer via le serveur SOCKS)

      Do not route through SOCKS server (Ne pas acheminer via le serveur SOCKS)

   b. Définissez une adresse IP ou une plage d'adresses de destination. Ne spécifiez jamais l'adresse de diffusion de tous les réseaux : 255.255.255.255
   c. Sélectionnez les serveurs SOCKS à utiliser pour le trafic.
   d. Indiquez si le trafic doit être distribué ou non vers les serveurs SOCKS spécifiés en mode round-robin (recherche circulaire).
   e. Cliquez sur **Ajouter** pour ajouter la règle.
4. Cliquez sur **Appliquer**, puis sur **Fermer**.
5. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Utilisation de l'option de division DNS

Vous pouvez configurer Content Gateway pour qu'il utilise plusieurs serveurs DNS, selon vos propres conditions de sécurité. Par exemple, vous pouvez configurer Content Gateway pour qu'il utilise un lot de serveurs DNS pour résoudre les noms d'hôte de votre réseau interne, tout en autorisant les serveurs DNS situés à l'extérieur du pare-feu à résoudre les hôtes situés sur Internet. Vous assurez ainsi la sécurité de votre réseau intranet, tout en continuant à autoriser un accès direct aux sites situés à l'extérieur de votre organisation.

Pour considérer l'option Split DNS (Diviser DNS), vous devez effectuer les tâches suivantes :

- Définir les règles de sélection des serveurs DNS en fonction du domaine destination, de l'hôte de destination ou d'une expression régulière d'URL
- Activer l'option Split DNS (Diviser DNS)

Dans Content Gateway Manager :

1. Ouvrez l'onglet **Configurer** > **Networking (Mise en réseau)** > **DNS Resolver (Résolveur DNS)** > **Split DNS (Diviser DNS)**.
2. Activez l'option **Split DNS (Diviser DNS)**.
3. Dans le champ **Default Domain (Domaine par défaut)**, entrez le domaine par défaut de division des requêtes DNS. Content Gateway ajoute automatiquement cette valeur à un nom d'hôte qui n'inclut pas de domaine avant d'identifier le serveur DNS à utiliser.
4. Dans le volet **DNS Servers Specification (Spécification des serveurs DNS)**, cliquez sur **Edit File (Modifier le fichier)** pour ouvrir le *Fichier de configuration splitdns.config* dans l'éditeur de fichiers de configuration.
5. Renseignez les champs fournis, puis cliquez sur **Ajouter**. L'ensemble des champs sont décris à la section *Fichier de configuration splitdns.config*.
6. Cliquez sur **Appliquer**, puis sur **Fermer**.
7. Dans l'onglet **Split DNS (Diviser DNS)**, cliquez sur **Appliquer** pour enregistrer votre configuration.
8. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Authentification des utilisateurs du proxy

Rubriques connexes :

- *Restrictions des navigateurs*, page 177
- *Paramètres de l'authentification transparente du proxy*, page 178
- *Authentification Windows intégrée*, page 179
- *Authentification NTLM héritée*, page 185
- *Authentification LDAP*, page 188
- *Authentification RADIUS*, page 190
- *Authentification dans plusieurs domaines Kerberos*, page 194

Content Gateway prend en charge plusieurs méthodes d'authentification des utilisateurs avant de les autoriser à accéder au contenu. Ces méthodes peuvent être combinées aux agents d'identification des utilisateurs de Websense Web Security pour assurer le basculement en cas d'indisponibilité de l'authentification des utilisateurs du proxy.

En modes proxy explicite et transparent, Content Gateway prend en charge l'authentification des utilisateurs avec :

- *Authentification Windows intégrée*, page 179 (avec Kerberos)
- *Authentification NTLM héritée*, page 185 (NTLMSSP)
- *Authentification LDAP*, page 188
- *Authentification RADIUS*, page 190

Par ailleurs, Content Gateway prend également en charge l'*Authentification dans plusieurs domaines Kerberos*, page 194, pour authentifier :

- Des jeux distincts d'adresses IP en fonction de domaines spécifiques
- Le trafic passant par certains ports en fonction de domaines spécifiques (proxy explicite uniquement)
- Des combinaisons des deux options précédentes (proxy explicite uniquement)

Pour chaque domaine Kerberos (définition ci-dessous), une méthode d'authentification (Authentification Windows intégrée, NTLM ou LDAP) est définie. Cette fonction permet donc d'utiliser plusieurs méthodes pour authentifier les utilisateurs de plusieurs domaines Kerberos.

Termes utilisés dans le contexte de l'authentification dans plusieurs domaines Kerberos

- Un **domaine** est un domaine Windows Active Directory.
- Un **domaine Kerberos** est un domaine Windows Active Directory non associé à une relation sortante approuvée avec d'autres domaines. Dans ce cas, les membres de ce domaine doivent être authentifiés par un contrôleur de domaine situé au sein du domaine.

Sélection du mode d'authentification

Dans Content Gateway Manager, le mode d'authentification est sélectionné via la section **Authentification** de la page **Configurer > Mon proxy > De base**. La configuration de l'authentification pour les environnements à plusieurs domaines Kerberos commence par la sélection de l'option **Multiple Realm Authentication (Authentification dans plusieurs domaines Kerberos)**.

Contrôleurs de domaine et annuaires pris en charge

- Contrôleurs de domaine Windows NT
- Windows 2003 et 2008 Active Directory
- Novell eDirectory 8.7 et 8.8 (LDAP uniquement)
- Oracle DSEE 11g, Sun Java 7 et 6.2 (LDAP uniquement)

Meilleures pratiques pour l'utilisation de Windows Active Directory

Si vous utilisez un domaine Active Directory, ou lorsque l'ensemble de vos domaines Active Directory partagent des relations de confiance en entrée et en sortie, la meilleure option consiste à utiliser l'Authentification Windows intégrée.

Lorsque vous utilisez plusieurs domaines Kerberos et que l'authentification est une obligation, vous devez utiliser l'option de plusieurs domaines Kerberos. Pour plus d'informations, et notamment pour une présentation des limites d'application des stratégies, consultez la section *Authentification dans plusieurs domaines Kerberos*, page 194.

Si l'identification des utilisateurs suffit, vous pouvez utiliser l'une des options d'identification des utilisateurs de Web Security. Reportez-vous à la section intitulée *Identification des utilisateurs* de l'Aide de TRITON -- Web Security.

Authentification transparente des utilisateurs

Content Gateway prend à la fois en charge l'authentification transparente (authentification unique) et l'authentification interactive (invite d'authentification). L'authentification transparente est prise en charge avec l'Authentification Windows intégrée et l'authentification NTLM héritée. Certains navigateurs n'assurent qu'une prise en charge limitée. Voir *Restrictions des navigateurs*, page 177.

Dans les réseaux Windows, l'authentification unique permet aux utilisateurs de ne se connecter qu'une seule fois et d'accéder ensuite de manière transparente à toutes les ressources réseau autorisées. Par conséquent, lorsqu'un utilisateur a déjà réussi à se connecter au réseau Windows, les informations d'identification spécifiées lors de la connexion Windows sont utilisées pour l'authentification du proxy et l'utilisateur n'a plus à saisir son nom d'utilisateur et son mot de passe.

L'authentification interactive est prise en charge dans les réseaux et les navigateurs qui ne sont pas configurés pour l'authentification unique. Avec l'authentification interactive, les utilisateurs sont invités à saisir leurs informations d'identification pour pouvoir accéder au contenu via Content Gateway.

Contrôleurs de domaine de sauvegarde

Pour l'Authentification Windows intégrée et l'authentification NTLM héritée, Content Gateway prend en charge la spécification des contrôleurs de domaine de sauvegarde pour le basculement. Lorsque le contrôleur de domaine principal ne répond pas aux requêtes du proxy, Content Gateway contacte le contrôleur de domaine suivant dans la liste (contrôleur de domaine de sauvegarde). À la prochaine requête, le proxy tente de nouveau de contacter le contrôleur de domaine principal, puis le contrôleur de domaine de sauvegarde lorsque la connexion échoue.

Restrictions des navigateurs

Tous les navigateurs Web ne prennent pas en charge l'authentification transparente des utilisateurs.

> **Remarque**
>
> Pour obtenir des informations complètes et à jour, consultez les Notes de publication de Content Gateway version 7.7.

Le tableau suivant indique comment un navigateur doit répondre à une demande d'authentification lorsque l'Authentification Windows intégrée (IWA) est configurée.

Navigateur/ Système d'exploitation	Internet Explorer (v8 & 9 testées)	Firefox (v11 testée)	Chrome (v17 & 18 testées)	Opera (v10 testée sous Windows, v11 testée sous Red Hat)	Safari (v5 testée)
Windows	Effectue l'authentification transparente	Effectue l'authentification transparente	Effectue l'authentification transparente	Revient à NTLM et demande les informations d'identification	Revient à NTLM et demande les informations d'identification
Mac OS X	Sans objet	Effectue l'authentification transparente	Problème de navigateur empêchant le fonctionnement d'IWA	Non testé	Effectue l'authentification transparente
Red Hat Enterprise Linux, mise à jour 6	Sans objet	Effectue l'authentification transparente	Problème de navigateur empêchant le fonctionnement d'IWA	Ne prend en charge aucune forme d'authentification de proxy	Sans objet

Remarque

Lorsque l'utilisateur ne saisit pas de nom de domaine quand il est invité à saisir ses informations d'identification, il peut être à nouveau invité à saisir ces informations ou recevoir une erreur d'expiration de la session.

Paramètres de l'authentification transparente du proxy

Lorsque Content Gateway est un proxy transparent qui effectue également l'authentification des utilisateurs, il est nécessaire de définir plusieurs options de configuration spéciales liées à l'authentification. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Transparent Proxy Authentication (Authentification du proxy transparent)**.

- **Redirect Hostname (Rediriger le nom d'hôte)** (facultatif) : définit un autre nom d'hôte pour le proxy. L'option Redirect Hostname (Rediriger le nom d'hôte) n'est pas nécessaire et n'est pas utilisée par l'Authentification Windows intégrée (IWA).

  Par défaut, les clients en cours d'authentification sont redirigés vers le nom d'hôte de l'ordinateur Content Gateway. Lorsque ces clients ne peuvent pas résoudre ce nom d'hôte via DNS, ou lorsque un autre nom DNS est défini pour le proxy, ce

nom d'hôte peut être spécifié dans le champ **Redirect Hostname (Rediriger le nom d'hôte)**.

> **Remarque**
>
> Pour être sûr que l'authentification des utilisateurs du proxy transparent s'effectue en transparence (c.-à-d. sans demander d'informations d'identification à l'utilisateur), le navigateur doit être configuré de sorte que la redirection du nom d'hôte s'effectue au sein de sa **Zone intranet**. Pour ce faire, il suffit généralement de s'assurer que la redirection du nom d'hôte s'effectue dans le même domaine que l'ordinateur dans lequel s'exécute le navigateur. Par exemple, si le client est **postedetravail.exemple.com** et que la redirection du nom d'hôte est **nomdhôteduproxy.exemple.com**, le navigateur autorisera l'authentification transparente, sans inviter l'utilisateur à saisir ses informations d'identification. Consultez la documentation de votre navigateur.

- **Authentication Mode (Mode d'authentification)** : définit le mode d'authentification transparente. Content Gateway doit être défini sur l'un des modes suivants :
  - **Mode IP :** en mode IP (par défaut), l'adresse IP du client est associée à un nom d'utilisateur lors de l'authentification de la session. Les requêtes provenant de cette adresse IP ne sont plus authentifiées jusqu'à expiration du paramètre **Session TTL (Durée de vie maximale de la session)** (par défaut, 15 minutes). Les requêtes provenant de cette adresse IP au cours de cette durée de vie sont considérées comme effectuées par l'utilisateur associé à cette adresse.
  - **Mode Cookie :** le mode Cookie sert exclusivement à identifier les utilisateurs qui partagent une même adresse IP, par exemple dans les environnements Terminal Server ou lorsqu'une traduction d'adresses réseau (NAT) est effectuée.
- **Session TTL (Durée de vie maximale de la session)** : une fois authentifiée, la session de l'utilisateur reste valide pour la durée spécifiée dans **Session TTL** (par défaut, 15 minutes). La plage des valeurs prises en charge va de 5 à 65 535 minutes.

Lorsque vous modifiez l'un de ces champs, cliquez sur **Appliquer** pour enregistrer vos modifications, puis redémarrez le proxy afin que ces modifications entrent en vigueur.

> **Remarque**
>
> Content Gateway prend en charge l'authentification transparente dans les clusters de proxy a l'aide de l'équilibrage de la charge WCCP. Toutefois, l'attribut de distribution de la méthode d'affectation doit être l'adresse IP source. Pour plus d'informations, consultez la section *Distribution de la charge WCCP*, page 52.

Authentification Windows intégrée

L'Authentification Windows intégrée (IWA) assure une méthode solide et fortement sécurisée pour l'authentification des utilisateurs appartenant tous à un ou plusieurs domaines Windows de confiance partagée.

L'Authentification Windows intégrée :

- Utilise Kerberos
- Prend en charge Windows Active Directory 2003 et 2008
- Prend en charge NTLM en modes proxy explicite et transparent
- Prend en charge NTLM v2 avec Session Security et NTLM v1 avec Session Security
- Prend en charge Internet Explorer 7 et versions ultérieures, Firefox 4 et versions ultérieures, Google Chrome 6 et versions ultérieures, Windows Safari 4 et versions ultérieures, Safari 4 et versions ultérieures sur iPad iOS4 et Opera 10 et versions ultérieures
- Prend en charge les noms d'utilisateur UTF-8
- Prend en charge le retour à l'authentification interactive (invite d'authentification)
- Peut être utilisée avec l'option d'authentification dans plusieurs domaines Kerberos
- Exige que les clients appartiennent au domaine approuvé
- Exige que les navigateurs des clients spécifient le Nom de domaine complet (FQDN) de Content Gateway en tant que site intranet ou site approuvé
- Dans les déploiements de proxy, les navigateurs doivent spécifier le nom FQDN de Content Gateway.

Authentification Windows intégrée : Résumé de la configuration

Procédez comme suit pour configurer l'Authentification Windows intégrée (IWA) :

- Dans Content Gateway Manager, activez IWA dans la page **Configurer > Mon proxy > De base**. Cliquez sur **Appliquer**.
- Joignez Content Gateway au domaine Windows. Reportez-vous à la section *Configuration de l'Authentification Windows intégrée* pour obtenir la liste des conditions requises.
- Si Content Gateway est un proxy transparent, configurez les *Paramètres de l'authentification transparente du proxy*.
- Configurez les **Options d'authentification globales**. Ces options s'appliquent à l'authentification NTLM lorsque IWA négocie NTLM ou revient à NTLM.

Configuration de l'Authentification Windows intégrée

1. Sélectionnez **Configurer > Mon proxy > De base > Général**.
2. Dans la section **Authentification**, cliquez sur Authentification Windows intégrée **On (Activée)**, puis sur **Appliquer**.
3. Dans la section **Authentification**, cliquez sur le lien **Configurer** pour accéder à **Configurer > Sécurité > Access Control (Contrôle d'accès)**.
4. Joignez le domaine Windows.

   Pour joindre le domaine :

   - Content Gateway doit pouvoir résoudre ce nom de domaine.
   - L'heure système de Content Gateway doit être synchronisée avec celle du contrôleur de domaine, plus ou moins 1 minute.
   - Les nom et mot de passe appropriés de l'administrateur de domaine doivent être spécifiés.

- Il doit exister une connectivité TCP/UDP vers le(s) contrôleur(s) de domaine (ports 88, 389, 445).
- Lorsque des contrôleurs de domaine de sauvegarde sont configurés, Content Gateway doit pouvoir y accéder sur le réseau, de même qu'à leurs services KDC (Kerberos Distribution Center).

Important

Tous les clients doivent être joints au domaine.

Les navigateurs et les autres clients du proxy doivent être configurés pour spécifier le nom FQDN de Content Gateway en tant que site intranet ou site approuvé.

a. Dans le champ **Nom de domaine**, entrez le nom de domaine complet.

b. Dans le champ **Nom d'administrateur**, entrez le nom d'utilisateur de l'administrateur Windows.

c. Dans le champ **Mot de passe d'administrateur**, entrez le mot de passe de l'administrateur Windows.

Le nom et le mot de passe ne sont utilisés que pour la jonction et ne sont pas stockés.

d. Indiquez comment localiser le contrôleur de domaine :

- **Auto-detect using DNS (Auto-détection via DNS)**
- **DC name or IP address (Nom ou adresse IP du contrôleur de domaine)**

  Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules, sans espace.

e. Dans le champ **Content Gateway Hostname (Nom d'hôte Content Gateway)**, confirmez l'exactitude du nom d'hôte en vérifiant qu'il ne dépasse pas 15 caractères (11 caractères sur les dispositifs V-Series). Lorsque ce nom est plus long, il doit être raccourci lorsque IWA doit être utilisé. Cette limite de longueur est due à la limite de 15 caractères des noms d'hôte NetBIOS.

Avertissement

Le nom d'hôte ne doit plus être modifié après la jonction du domaine. Si ce nom est modifié, IWA cesse immédiatement de fonctionner et ne fonctionnera plus tant que la jonction au domaine n'aura pas été annulée, puis réeffectuée avec le nouveau nom d'hôte.

f. Cliquez sur **Join Domain (Joindre le domaine)**. En cas d'erreur, assurez-vous que les conditions décrites ci-dessus ont été respectées, puis reportez-vous à la section *Échec de la jonction du domaine*.

5. Si Content Gateway est déployé en tant que proxy transparent, configurez les *Paramètres de l'authentification transparente du proxy*, puis passez à l'étape suivante.

6. Configurez les paramètres NTLM globaux. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Global Authentication Options (Options d'authentification globales)**.

   Remarque
   Ces paramètres s'appliquent lorsque IWA négocie l'authentification NTLM ou revient à l'authentification NTLM.

   a. L'option **Fail Open (Échec ouvert)** est activée par défaut. Cette option autorise le traitement des requêtes lorsque l'authentification échoue dans les cas suivants :

      - Aucune réponse du contrôleur de domaine
      - Messages malformés provenant du client
      - Réponses SMB non valides

      Avec l'option Fail Open (Échec ouvert), lorsque le filtrage Web est utilisé avec le proxy et qu'un agent XID est configuré, le demandeur peut encore être identifié par l'agent XID et la stratégie appropriée être appliquée en cas d'échec de l'authentification IWA.

      Désactivez cette option si vous souhaitez que les requêtes ne soient pas envoyées vers Internet lorsque les conditions d'échec d'authentification répertoriées ci-dessus se produisent.

   b. L'option **Credential Caching (Mise en cache des informations d'identification)** est activée par défaut. La mise en cache des informations d'identification s'applique uniquement lorsque Content Gateway est déployé en tant que proxy explicite. Les informations d'identification ne sont mises en cache que si l'authentification réussit. Pour désactiver la mise en cache des informations d'authentification, sélectionnez **Désactiver**.

   c. L'option **Caching TTL (Durée de vie de la mise en cache)** définit la durée de vie des entrées stockées dans le cache des informations d'identification. La valeur par défaut est 900 secondes (15 minutes). Pour modifier cette durée, saisissez une nouvelle valeur dans le champ. La plage des valeurs prises en charge va de 300 à 86 400 secondes.

   d. Si certains utilisateurs se servent de serveurs Terminal Server pour accéder à Internet via le proxy (ex. : serveurs Citrix), vous devez dresser la liste de ces serveurs dans le champ **Multi-user IP Exclusions (Exclusion des adresses IP d'utilisateurs)**. Les informations d'identification de ces utilisateurs ne sont pas mises en cache. Entrez une liste d'adresses IP ou de plages d'adresses IP séparées par des virgules.

La configuration est à présent terminée. Redémarrez Content Gateway et testez le trafic via le proxy afin de vérifier que l'authentification fonctionne comme prévu. En cas de problème, reportez-vous à la section *Résolution des problèmes liés à l'Authentification Windows intégrée*.

Pour annuler la jonction au domaine actuel et joindre un nouveau domaine :

1. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentification Windows intégrée**, puis cliquez sur **Unjoin (Annuler la jonction)**.
2. Pour joindre un nouveau domaine, entrez le nom de domaine complet dans le champ **Nom de domaine**.
3. Dans le champ **Nom d'administrateur**, entrez le nom d'utilisateur de l'administrateur Windows.
4. Dans le champ **Mot de passe d'administrateur**, entrez le mot de passe de l'administrateur Windows. Le nom et le mot de passe ne sont utilisés que pour la jonction et ne sont pas stockés.
5. Indiquez comment localiser le contrôleur de domaine :
   - **Auto-detect using DNS (Auto-détection via DNS)**
   - **DC name or IP address (Nom ou adresse IP du contrôleur de domaine)**

     Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules, sans espace.
6. Cliquez sur **Join Domain (Joindre le domaine)**.

Pour modifier le mode de détection du contrôleur de domaine :

1. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentification Windows intégrée**.
2. Dans la section **Contrôleur de domaine**, indiquez comment localiser le contrôleur de domaine :
   - **Auto-detect using DNS (Auto-détection via DNS)**
   - **DC name or IP address (Nom ou adresse IP du contrôleur de domaine)**

     Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules, sans espace.
3. Cliquez sur **Appliquer**.

Résolution des problèmes liés à l'Authentification Windows intégrée

Cette section décrit deux problèmes courants :

- *Échec de la jonction du domaine*
- *Échec de l'authentification des clients*

Échec de la jonction du domaine

Les conditions suivantes sont requises pour la jonction de Content Gateway à un domaine :

- Content Gateway doit pouvoir résoudre ce nom de domaine.
- L'heure système de Content Gateway doit être synchronisée avec celle du contrôleur de domaine, plus ou moins 1 minute.
- Les nom et mot de passe appropriés de l'administrateur de domaine doivent être spécifiés.

- Il doit exister une connectivité TCP/UDP vers le(s) contrôleur(s) de domaine (ports 88, 389, 445).
- Lorsque des contrôleurs de domaine de sauvegarde sont configurés, Content Gateway doit pouvoir y accéder sur le réseau, de même qu'à leurs services KDC (Kerberos Distribution Center).

Dépannage :

- Les erreurs rencontrées lors de la jonction sont indiquées en haut de l'écran (onglet Authentification Windows intégrée).
- Le message d'erreur contient généralement un lien qui vous permet d'accéder au journal des échecs et d'obtenir davantage d'informations.
- Les échecs de jonction sont enregistrés dans le journal **/opt/WCG/logs/smbadmin.join.log**.
- Dans la plupart des cas, le message d'échec indiqué dans le journal est un message d'erreur standard Samba et Kerberos qu'une recherche Internet permet de localiser facilement.

Échec de l'authentification des clients

Les conditions suivantes sont nécessaires pour l'authentification des clients :

- Les clients Content Gateway doivent être membre du domaine auquel est joint Content Gateway.
- L'heure système du client doit être synchronisée avec celle du contrôleur de domaine et de Content Gateway, plus ou moins 1 minute.
- Les clients du proxy explicite ne doivent **pas** être configurés pour envoyer leurs requêtes à l'adresse IP de Content Gateway. Les clients doivent utiliser le nom de domaine complet (FQDN) de Content Gateway. Si l'adresse IP est utilisée, l'authentification NTLM l'est également systématiquement.
- Le nom de domaine complet de Content Gateway doit être indiqué dans le système DNS et tous les clients du proxy doivent pouvoir le résoudre.
- Les navigateurs et les clients du proxy doivent spécifier le nom FQDN de Content Gateway en tant que site intranet ou site approuvé.

Dépannage :

Dans Content Gateway Manager, servez-vous de la fonction **Diagnostic Test (Test de diagnostic)** de l'onglet **Monitor (Surveiller) > Sécurité > Authentification Windows intégrée**. Cet onglet Monitor (Surveiller) présente les statistiques des requêtes d'authentification et propose une fonction de diagnostic.

La fonction **Diagnostic Test (Test de diagnostic)** teste la connectivité et l'authentification en indiquant les erreurs éventuelles. Elle indique également la connectivité du port TCP au contrôleur de domaine et les retards.

Les erreurs et les messages sont enregistrés dans :

- /var/log/messages
- content_gateway.out
- /opt/WCG/logs/smbadmin.log
- /opt/WCG/logs/smbadmin.join.log

Problèmes de performances :

- **IWA (Kerberos) :** les performances de l'authentification sont données par processeur. Aucune communication n'est établie avec les contrôleurs de domaine pour l'authentification Kerberos.
- **NTLM et de base :** la réactivité des contrôleurs de domaine affecte les performances. La page **Monitor (Surveiller) > Sécurité > Authentification Windows intégrée** présente le temps moyen de réponse.

Authentification NTLM héritée

Content Gateway prend en charge le protocole d'authentification NTLM (NT LAN Manager) en tant que méthode garantissant l'authentification des utilisateurs d'un réseau Windows avant qu'ils n'accèdent à Internet.

Important

Cette implémentation de la prise en charge du protocole NTLM (authentification NTLM héritée) dépend exclusivement du protocole NTLMSSP. Si son fonctionnement est fiable (tel que documenté dans cette section), il est fortement recommandé d'utiliser le mode *Authentification Windows intégrée* à la place. Ce dernier garantit une prise en charge plus solide et plus sécurisée de NTLM.

Lorsque l'option d'authentification NTLM héritée est activée, le proxy invite les utilisateurs qui demandent du contenu à saisir leurs informations d'identification. Le proxy envoie ensuite directement ces informations d'identification au contrôleur de domaine Windows en vue de leur validation. Lorsque les informations d'identification sont valides, le proxy envoie le contenu demandé et stocke ces informations d'identification dans le cache NTLM pour les réutiliser ultérieurement. Lorsque les informations d'identification ne sont pas valides, le proxy envoie un message *d'échec d'authentification*.

Restrictions :

1. La **résolution WINS** n'est pas prise en charge. Les contrôleurs de domaine doivent disposer de noms d'hôte que le serveur DNS peut résoudre.
2. La **sécurité étendue** n'est pas prise en charge et ne peut pas être activée au niveau du contrôleur de domaine.
3. La **sécurité de la session NTLM2** n'est pas prise en charge et ne peut pas être activée au niveau des clients. Dans le volet Paramètres de sécurité du système d'exploitation Windows, examinez les paramètres **Sécurité réseau : sécurité de session minimale**.
4. **NTLMv2** n'est pas pris en charge avec Active Directory 2008. Le paramètre **Sécurité réseau : sécurité de session minimale** requis est décrit à l'étape 5 de la section *Configuration de l'authentification NTLM du proxy*, ci-dessous.
5. Tous les navigateurs ne prennent pas en charge l'authentification NTLM transparente. Voir *Restrictions des navigateurs*, page 177.
6. La mise en cache des informations d'identification NTLM est effectuée lorsque l'authentification en mode explicite est réussie. La mise en cache des authentifications de proxy transparent est gérée séparément et est configurée dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Transparent Proxy Authentication (Authentification du proxy transparent)**.

Configuration de l'authentification NTLM héritée

1. Sélectionnez **Configurer > Mon proxy > De base > Général**.
2. Dans la section Authentification, cliquez sur Legacy NTLM (Authentification NTLM héritée) **On (Activée)**, puis sur **Appliquer**.
3. Sélectionnez **Configurer > Sécurité > Access Control (Contrôle d'accès) > Legacy NTLM (Authentification NTLM héritée)**.
4. Dans le champ **Domain Controller Hostnames (Noms d'hôte des contrôleurs de domaine)**, saisissez le nom d'hôte du contrôleur de domaine principal, éventuellement suivi des contrôleurs de domaine de sauvegarde séparés par des virgules. Le format du nom d'hôte doit être le suivant :

   ```
   nom_hôte[:port][%nom_netbios]
   ```

   ou

   ```
   adresse_IP[:port][%nom_netbios]
   ```

   Remarque

   Si vous utilisez Active Directory 2008, vous devez inclure le nom_netbios ou utiliser le port SMB 445. Si vous n'utilisez **pas** le port 445, vous devez vous assurer que le service de partage des fichiers Windows s'exécute dans le serveur Active Directory. Reportez-vous à la documentation de Windows Server 2008 pour plus d'informations.

   Remarque

   Si vous utilisez Active Directory 2008, le paramètre **Sécurité réseau : niveau d'authentification Lan Manager** de Windows doit être défini sur **Envoyer uniquement les réponses NTLM**. Reportez-vous à la documentation de Windows Server 2008 pour plus d'informations.

5. Si vous voulez que le proxy équilibre la charge lorsqu'il envoie des demandes d'authentification à plusieurs contrôleurs de domaine, activez l'**équilibrage de la charge**.

   Remarque

   Lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé.

6. L'option **Fail Open (Échec ouvert)** est activée par défaut. Cette option autorise le traitement des requêtes lorsque l'authentification échoue dans les cas suivants :
   - Aucune réponse du contrôleur de domaine
   - Messages malformés provenant du client
   - Réponses SMB non valides

   Avec l'option Fail Open (Échec ouvert), lorsque le filtrage Web est utilisé avec le proxy et qu'un agent XID est configuré, le demandeur peut encore être identifié par l'agent XID et la stratégie appropriée être appliquée en cas d'échec de l'authentification NTLM.

   Désactivez cette option si vous souhaitez que les requêtes ne soient pas envoyées vers Internet lorsque les conditions d'échec d'authentification répertoriées ci-dessus se produisent.
7. L'option **Credential Caching (Mise en cache des informations d'identification)** est activée par défaut. La mise en cache des informations d'identification s'applique uniquement lorsque Content Gateway est déployé en tant que proxy explicite. Les informations d'identification ne sont mises en cache que si l'authentification réussit. Pour désactiver la mise en cache des informations d'authentification, sélectionnez **Désactiver**.
8. L'option **Caching TTL (Durée de vie de la mise en cache)** définit la durée de vie des entrées stockées dans le cache des informations d'identification. La valeur par défaut est 900 secondes (15 minutes). Pour modifier cette durée, saisissez une nouvelle valeur dans le champ. La plage des valeurs prises en charge va de 300 à 86 400 secondes.
9. Si certains utilisateurs se servent de serveurs Terminal Server pour accéder à Internet via le proxy (ex. : serveurs Citrix), vous devez dresser la liste de ces serveurs dans le champ **Multi-user IP Exclusions (Exclusion des adresses IP d'utilisateurs)**. Les informations d'identification de ces utilisateurs ne sont pas mises en cache. Entrez une liste d'adresses IP ou de plages d'adresses IP séparées par des virgules.
10. Cliquez sur **Appliquer**.
11. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Éventuellement, vous pouvez aussi :

- Configurer Content Gateway pour qu'il autorise certains clients à accéder à des sites Internet spécifiques sans être authentifiés par le serveur NTLM. (Voir *Contrôle d'accès*, page 298).
- Configurer un autre nom d'hôte Content Gateway pour l'authentification, définir le mode d'authentification (IP ou Cookie) et définir la durée de vie de la session. Voir *Paramètres de l'authentification transparente du proxy*, page 178.

Authentification LDAP

Pour s'assurer que les utilisateurs soient authentifiés auprès d'un serveur LDAP avant d'accéder au contenu via le proxy, Content Gateway prend en charge l'option LDAP.

> **Important**
>
> Dans les environnements à plusieurs domaines Kerberos (domaines qui ne partagent pas de relations de confiance), configurez l'authentification LDAP via l'option *Authentification dans plusieurs domaines Kerberos*.

Lorsque l'option LDAP est activée, le proxy joue le rôle de client LDAP et demande directement leur nom d'utilisateur et leur mot de passe aux utilisateurs qui demandent du contenu. À réception du nom d'utilisateur et du mot de passe, le proxy contacte le serveur LDAP pour vérifier l'exactitude de ces informations. Si le serveur LDAP accepte le nom d'utilisateur et mot de passe, le proxy envoie le contenu demandé au client et stocke ce nom d'utilisateur et ce mot de passe dans le cache LDAP de Content Gateway. Toutes les demandes d'authentification ultérieures de cet utilisateur sont ensuite desservies à partir du cache LDAP jusqu'à expiration des entrées du cache. Si le serveur LDAP refuse le nom d'utilisateur et le mot de passe, le navigateur de l'utilisateur présente un message signalant l'échec de l'autorisation et lui demande à nouveau de saisir un nom d'utilisateur et un mot de passe.

L'authentification LDAP prend en charge les liaisons simple et anonyme.

Configuration de Content Gateway en tant que client LDAP

1. Sélectionnez **Configurer > Mon proxy > De base > Général**.
2. Dans la section Authentification, cliquez sur LDAP **On (Activé)**, puis sur **Appliquer**.
3. Sélectionnez **Configurer > Sécurité > Access Control (Contrôle d'accès) > LDAP**.
4. Activez l'option **Purge Cache on Authentication Failure (Purger le cache en cas d'échec d'authentification)** pour configurer le proxy de sorte qu'il supprime l'entrée de l'autorisation du client dans le cache LDAP en cas d'échec de l'autorisation.
5. Entrez le nom d'hôte du serveur LDAP.
6. Entrez le port par lequel Content Gateway communique avec le serveur LDAP. Le port par défaut est le 389.

> **Remarque**
>
> Lorsque le service d'annuaire LDAP est Active Directory, les requêtes provenant des utilisateurs situés à l'extérieur du domaine de base du catalogue global ne peuvent pas être authentifiées. En effet, le port LDAP par défaut est le 389 et les requêtes envoyées à ce dernier recherchent uniquement les objets au sein du domaine de base du catalogue global. Pour authentifier les utilisateurs situés à l'extérieur du domaine de base, définissez le port LDAP sur le port 3268. Les requêtes envoyées au port 3268 recherchent des objets dans la totalité de la forêt.

7. Si vous voulez que le proxy communique de manière sécurisée avec le serveur LDAP, activez l'option Secure LDAP (LDAP sécurisé). La communication sécurisée est établie sur le port 636 ou 3269. Au besoin, remplacez la valeur du port dans le champ précédent.
8. Sélectionnez votre type de service d'annuaire afin de définir le filtre des recherches. Le type par défaut est **sAMAccountName** pour Active Directory. Sélectionnez **uid** pour eDirectory ou d'autres services d'annuaire.
9. Entrez le Nom distinctif complet (FDN) d'un utilisateur dans le service d'annuaire de type LDAP. Par exemple :

   `CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM`

   Entrez un maximum de 128 caractères dans ce champ.

   Lorsqu'aucune valeur n'est saisie dans ce champ, le proxy tente une liaison anonyme.
10. Entrez un mot de passe pour l'utilisateur spécifié à l'étape précédente.
11. Entrez le Nom unique de la base de recherche LDAP (DN). Demandez cette valeur à votre administrateur LDAP.
12. Cliquez sur **Appliquer**.
13. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Les étapes suivantes sont facultatives. Vous pouvez :

- Modifier les options du cache LDAP. Voir *Définition des options du cache LDAP*, page 189.
- Configurer Content Gateway pour qu'il autorise certains clients à accéder à des sites Internet spécifiques sans être authentifiés par le serveur LDAP. Voir *Contrôle d'accès*, page 298.
- Configurer un autre nom d'hôte Content Gateway pour l'authentification, définir le mode d'authentification (IP ou Cookie) et définir la durée de vie de la session. Voir *Paramètres de l'authentification transparente du proxy*, page 178.

Définition des options du cache LDAP

Par défaut, le cache LDAP est configuré pour stocker 5 000 entrées, chacune d'elles étant considérée comme récente pendant 3 000 minutes. Pour changer ces options, modifiez le fichier **records.config**.

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway (**/opt/WCG/config**).
2. Modifiez les variables suivantes :

Variable	Description
`proxy.config.ldap.cache.size`	Définit le nombre d'entrées autorisées dans le cache LDAP. La valeur par défaut est 5 000. La valeur minimale est 256.
`proxy.config.ldap.auth.ttl_value`	Définit la durée (en minutes) pendant laquelle Content Gateway peut stocker les entrées de nom d'utilisateur et de mot de passe dans le cache LDAP

Variable	Description
`proxy.config.ldap.cache.taille_stockage`	Définit le volume maximal d'espace (en octets) que peut occuper le cache LDAP sur le disque. Si vous modifiez cette valeur, vous devez actualiser la valeur **proxy.config.ldap.cache.size** en proportion. Par exemple, si vous doublez la taille du stockage, doublez également la taille du cache. Si vous modifiez cette variable sans modifier la valeur de **proxy.config.ldap.cache.size**, le sous-système LDAP cesse de fonctionner.

3. Enregistrez et fermez le fichier.
4. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**), exécutez la commande **content_line -L** pour redémarrer le proxy dans le nœud local ou **content_line -M** pour redémarrer le proxy dans tous les nœuds d'un cluster.

Configuration de la communication LDAP sécurisée

Par défaut, le trafic LDAP est transmis de façon non sécurisée. Vous pouvez assurer la confidentialité et la sécurité du trafic LDAP en utilisant la technologie SSL (Secure Sockets Layer) / TLS (Transport Layer Security). Vous pouvez activer LDAP sur SSL (LDAPS) en installant un certificat correctement mis en forme publié par une autorité de certification Microsoft ou non Microsoft.

Pour utiliser LDAPS avec Content Gateway :

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway (**/opt/WCG/config**).
2. Ajoutez l'entrée suivante dans le fichier **records.config** :

   ```
   CONFIG proxy.config.ldap.secure.bind.enabled INT 1
   ```

3. Sélectionnez **Configurer > Sécurité > Access Control (Contrôle d'accès) > LDAP** et définissez le port sur 3269.

> **Remarque**
> Le service d'annuaire doit être configuré pour prendre en charge l'authentification LDAPS. Pour plus de précisions, reportez-vous à la documentation fournie par le fabricant de votre annuaire.

Authentification RADIUS

Pour s'assurer que les utilisateurs soient authentifiés auprès d'un serveur RADIUS avant d'accéder au contenu via le proxy, Content Gateway prend en charge l'option RADIUS.

Lorsque l'option RADIUS est activée, Content Gateway joue le rôle de client RADIUS et demande directement leur nom d'utilisateur et leur mot de passe aux utilisateurs qui réclament du contenu. À réception du nom d'utilisateur et du mot de passe, Content Gateway contacte le serveur RADIUS pour vérifier l'exactitude de ces informations. Si le serveur RADIUS accepte le nom d'utilisateur et le mot de passe, le proxy envoie le

contenu demandé au client et stocke le nom d'utilisateur et mot de passe dans le cache RADIUS. Toutes les demandes d'authentification ultérieures de cet utilisateur sont ensuite desservies à partir du cache RADIUS jusqu'à expiration de l'entrée. Si le serveur RADIUS refuse le nom d'utilisateur et le mot de passe, le navigateur de l'utilisateur présente un message signalant l'échec de l'autorisation et lui demande à nouveau de saisir un nom d'utilisateur et un mot de passe.

Content Gateway prend en charge un serveur RADIUS principal et un serveur RADIUS secondaire pour le basculement. Si le serveur principal ne répond pas à la requête du proxy avant le délai d'expiration spécifié (60 secondes par défaut), Content Gateway tente à nouveau de vérifier le nom d'utilisateur et le mot de passe. Lorsqu'aucune réponse du serveur RADIUS principal n'est reçue quand le nombre maximal de nouvelles tentatives est atteint (10 par défaut), le proxy contacte le serveur RADIUS secondaire. Si Content Gateway ne peut pas contacter le serveur RADIUS secondaire, l'utilisateur est de nouveau invité à saisir son nom d'utilisateur et son mot de passe.

Le cache RADIUS est conservé en mémoire et stocké sur disque. Content Gateway met les données sur disque à jour toutes les 60 secondes. Par ailleurs, Content Gateway stocke les entrées de nom d'utilisateur et de mot de passe dans le cache RADIUS pendant 60 minutes. Lorsqu'une entrée de mot de passe et de nom d'utilisateur du cache RADIUS arrive à expiration, Content Gateway contacte le serveur RADIUS pour accepter ou refuser le nom d'utilisateur et le mot de passe.

Pour configurer Content Gateway en tant que client RADIUS :

- Activez l'option RADIUS.
- Définissez le nom d'hôte ou l'adresse IP des serveurs RADIUS principal et secondaire (facultatif), puis le port et la clé partagée que Content Gateway utilise pour communiquer avec les serveurs RADIUS.

Voir *Configuration de Content Gateway en tant que client RADIUS*, page 191.

Configuration de Content Gateway en tant que client RADIUS

1. Sélectionnez **Configurer > Mon proxy > De base > Général**.
2. Dans la section Authentification, cliquez sur Radius **On (Activé)**, puis sur **Appliquer**.
3. Sélectionnez **Configurer > Sécurité > Access Control (Contrôle d'accès) > Radius**.
4. Entrez le nom d'hôte de votre serveur RADIUS principal.
5. Entrez le numéro du port par lequel Content Gateway communique avec le serveur RADIUS principal.
6. Entrez la clé d'encodage utilisée.
7. Si vous utilisez un serveur RADIUS secondaire, entrez son nom d'hôte, son port et sa clé partagée dans les champs appropriés du volet **Secondary Radius Server (Optional) (Serveur Radius secondaire (facultatif))**.
8. Cliquez sur **Appliquer**.

9. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

> **Remarque**
> En plus de ces procédures, vous devez ajouter l'ordinateur Content Gateway en tant que client approuvé sur les serveurs RADIUS principal et secondaire et fournir la clé partagée que vous souhaitez utiliser pour l'ordinateur Content Gateway (cette clé doit correspondre à celle que vous avez spécifiée dans la procédure ci-dessous). Reportez-vous à la documentation de votre serveur RADIUS.

Définition du cache RADIUS et des options d'expiration des serveurs

Par défaut, le cache RADIUS et les options d'expiration des serveurs RADIUS sont configurés comme suit :

- Le cache RADIUS est configuré pour stocker 1 000 entrées, chacune d'elles étant considérée comme récente pendant 60 minutes.
- Content Gateway peut tenter de rétablir la connexion au serveur RADIUS lorsque celle-ci reste inactive pendant 10 secondes et à 10 reprises au maximum.

Pour changer ces valeurs par défaut, modifiez le fichier **records.config**.

1. Ouvrez le fichier **records.config** situé dans le répertoire **config** de Content Gateway (**/opt/WCG/config**).

2. Modifiez les variables suivantes :

Variable	Description
`proxy.config.radius.auth.expiration_mini`	Définissez la durée (en secondes) pendant laquelle la connexion établie entre Content Gateway et le serveur RADIUS peut rester inactive avant que Content Gateway ne ferme la connexion.
`proxy.config.radius.auth.tentatives_maxi`	Définissez le nombre maximal de tentatives de connexion au serveur RADIUS par Content Gateway.
`proxy.config.radius.cache.size`	Définissez le nombre d'entrées autorisées dans le cache RADIUS. La valeur minimale est 256 entrées. Si vous saisissez une valeur inférieure à 256, Content Gateway signale une erreur SEGV.
`proxy.config.radius.auth.ttl_value`	Définissez la durée (en minutes) pendant laquelle Content Gateway peut stocker les entrées de nom d'utilisateur et de mot de passe dans le cache RADIUS.
`proxy.config.radius.cache.taille_stockage`	Définissez le volume maximal d'espace que peut occuper le cache RADIUS sur le disque. Cette valeur doit être d'au moins 100 fois le nombre d'entrées. Il est recommandé d'utiliser la quantité d'espace disque maximale possible.

3. Enregistrez et fermez le fichier.
4. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**), exécutez la commande **content_line -L** pour redémarrer Content Gateway dans le nœud local ou **content_line -M** pour redémarrer WCG dans tous les nœuds d'un cluster.

Authentification dans plusieurs domaines Kerberos

Rubriques connexes :

- *Paramètres de l'authentification transparente du proxy*, page 178
- *Options d'authentification globales*, page 198
- *Authentification dans plusieurs domaines Kerberos : Domaines*, page 197
- *Création d'une règle de domaine Kerberos accessible via l'authentification Windows intégrée*, page 199
- *Création d'une règle de domaine Kerberos accessible via l'authentification LDAP*, page 202
- *Utilisation des règles d'authentification dans plusieurs domaines Kerberos*, page 204
- *Cas d'utilisation de l'authentification dans plusieurs domaines Kerberos*, page 205
- *Résolution des problèmes liés à l'authentification dans plusieurs domaines Kerberos*, page 207

L'authentification dans plusieurs domaines Kerberos est destinée à authentifier les utilisateurs au sein des environnements qui utilisent plusieurs domaines avant tout isolés du fait du manque de relations mutuelles entrantes et sortantes approuvées. En conséquence, les utilisateurs de ces domaines doivent être authentifiés par un contrôleur de domaine situé dans leur propre domaine. Par rapport à cette fonction, ces domaines sont appelés **domaines Kerberos**.

Remarque

Si tous les utilisateurs de votre réseau peuvent être authentifiés par des contrôleurs de domaine partageant des relations de confiance, vous n'avez pas besoin de créer des règles d'authentification dans plusieurs domaines Kerberos. Dans ce cas, la meilleure pratique consiste à utiliser la méthode d'authentification la mieux adaptée à votre service d'annuaire.

L'authentification dans plusieurs domaines Kerberos permet d'écrire des règles d'authentification distinctes pour chaque domaine, donc de prendre en charge simultanément plusieurs méthodes d'authentification (IWA, NTLM héritée, LDAP). Par exemple, le DomaineKerberosA peut être un domaine Active Directory dont les utilisateurs doivent être authentifiés à l'aide de l'Authentification Windows intégrée. Le DomaineKerberosB peut être un domaine LDAP dont les utilisateurs doivent être authentifiés via LDAP. L'authentification dans plusieurs domaines Kerberos simplifie dans ce cas cette opération. Trois scénarios hypothétiques sont proposés à la section *Cas d'utilisation de l'authentification dans plusieurs domaines Kerberos*, page 205.

Dans les environnements de proxy explicite, il est possible d'écrire des règles d'authentification pour le trafic entrant sur des ports spécifiques. Cela permet d'utiliser des règles d'authentification spécifiant le port du proxy, les adresses IP sources, la méthode d'authentification et le domaine Kerberos.

Important

Dans un environnement à plusieurs domaines Kerberos, Content Gateway peut authentifier les utilisateurs que Web Security ne connaît pas (c'est-à-dire situés hors du domaine principal des services des utilisateurs). Dans ce cas, Content Gateway peut être configuré pour envoyer un nom d'utilisateur « alias » que Web Security connaît ou pour appliquer la stratégie par défaut, sans envoyer de nom. Cette sélection doit être effectuée dans les options avancées de chaque règle que vous définissez.

Une description plus détaillée est disponible à la section *Utilisateurs inconnus et option 'alias'*, ci-dessous.

Fonctionnement de la prise en charge de l'authentification dans plusieurs domaines Kerberos

Dans les réseaux avec plusieurs domaines Kerberos, des règles définissent la redirection des jeux d'adresse IP ou le trafic passant par des ports spécifiques vers des contrôleurs de domaine distincts. Ces règles sont définies dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**. Ces règles sont stockées dans le *Fichier de configuration auth.config*.

- Des règles d'authentification dans plusieurs domaines Kerberos peuvent être définies pour des sources IWA, NTLM héritée et LDAP.
- Une ou plusieurs règles d'authentification peuvent être définies pour chaque domaine Kerberos.
- Les spécificateurs utilisés dans chaque type de règle de domaine Kerberos (IWA, NTLM héritée, LDAP) diffèrent.
- **Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas. La première correspondance étant appliquée en premier. Lorsque l'adresse IP ne correspond à aucune règle, aucune authentification n'est tentée.**
- Les transactions sont enregistrées dans le journal en fonction du nom utilisé par le service de filtrage.
- Des statistiques d'authentification du proxy sont collectées et indiquées discrètement pour chaque méthode d'authentification. Voir *Sécurité*, page 242 section Statistiques.

Important

Content Gateway doit être configuré avec un serveur DNS capable de résoudre le nom de domaine complet (FQDN) de Content Gateway pour chaque domaine Kerberos utilisé par l'Authentification Windows intégrée. Si ce n'est pas le cas, les règles IWA ne fonctionnent pas. Il revient à l'administrateur réseau de configurer le serveur DNS de la manière appropriée. Une possibilité consiste à configurer une zone de transfert DNS (sous-zone) entre le serveur DNS principal de Content Gateway et le serveur DNS de chaque domaine Kerberos d'authentification.

Utilisateurs inconnus et option ‘alias’

Dans les environnements de plusieurs domaines Kerberos, Content Gateway peut authentifier un utilisateur qui n’est pas reconnu lorsqu’il est transmis à Web Security parce que son nom n’est pas dans l’annuaire des services d’utilisateurs. Lorsqu’un nom d’utilisateur authentifié est transmis à Web Security et qu’aucune correspondance n’est détectée, la stratégie par défaut est appliquée. Plusieurs méthodes permet d’effectuer cette opération :

- Modifiez la configuration des services d’utilisateurs de Web Security pour afficher et ajouter les noms dans l’annuaire.
- Ajoutez les noms non reconnus dans le domaine principal de Web Security. Les noms doivent être exactement les mêmes. Définissez des stratégies pour les nouveaux noms.
- Pour les utilisateurs qui correspondent à une règle d’un domaine Kerberos particulier, transmettez un alias et ajoutez ce dernier dans le domaine principal de Web Security. Les noms doivent être exactement les mêmes. Définissez une stratégie pour cet alias.
- Si la stratégie Web Security utilisée par défaut est suffisante, ne faites rien ou, pour chaque utilisateur correspondant à une règle d’un domaine particulier, utilisez un alias vide dans cette règle.

Quelques cas d’utilisation représentatifs sont fournis à la section *Cas d’utilisation de l’authentification dans plusieurs domaines Kerberos*.

Résumé de la configuration de l’authentification dans plusieurs domaines Kerberos

- Joignez tous les domaines Windows à utiliser avec des règles d’Authentification Windows intégrée (des domaines peuvent ensuite être ajoutés ou supprimés, mais aucune règle ne peut être créée pour un domaine dont la jonction n’a pas été effectuée). Voir *Authentification dans plusieurs domaines Kerberos : Domaines*, page 197.
- Si Content Gateway est un proxy explicite et que vous souhaitez transmettre le trafic sur plusieurs ports, définissez ces ports dans l’onglet **Configurer > Protocole > HTTP**.

  Remarque

  - Vous devez également configurer vos clients pour qu’ils utilisent le port approprié.

- Si Content Gateway est un proxy transparent, configurez les *Paramètres de l’authentification transparente du proxy*, page 178.
- Configurez les *Options d’authentification globales*, page 198.
- Créez des règles d’authentification.
  - *Création d’une règle de domaine Kerberos accessible via l’authentification Windows intégrée*, page 199
  - *Création d’une règle de domaine Kerberos accessible via l’authentification NTLM*, page 200
  - *Création d’une règle de domaine Kerberos accessible via l’authentification LDAP*, page 202

Authentification dans plusieurs domaines Kerberos : Domaines

Avant de créer une règle de domaine Kerberos accessible via l'Authentification Windows intégrée, vous devez effectuer la jonction de chaque domaine du domaine Kerberos.

> **Important**
> Tous les clients devant être authentifiés dans un domaine donné doivent être joints à ce domaine.

Pour pouvoir joindre un domaine :

- Content Gateway doit pouvoir résoudre ce nom de domaine.
- L'heure système de Content Gateway doit être synchronisée avec celle du contrôleur de domaine, plus ou moins 1 minute.
- Les nom et mot de passe appropriés de l'administrateur de domaine doivent être spécifiés.
- Il doit exister une connectivité TCP/UDP vers le(s) contrôleur(s) de domaine (ports 88, 389, 445).
- Lorsque des contrôleurs de domaine de sauvegarde sont configurés, Content Gateway doit pouvoir y accéder sur le réseau, de même qu'à leurs services KDC (Kerberos Distribution Center).

Pour joindre un domaine :

1. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentification Windows intégrée**.
2. Dans le champ **Nom de domaine**, entrez le nom de domaine complet.
3. Dans le champ **Nom d'administrateur**, entrez le nom d'utilisateur de l'administrateur Windows.
4. Dans le champ **Mot de passe d'administrateur**, entrez le mot de passe de l'administrateur Windows.

   Le nom et le mot de passe ne sont utilisés que pour la jonction et ne sont pas stockés.
5. Indiquez comment localiser le contrôleur de domaine :
   - **Auto-detect using DNS (Auto-détection via DNS)**
   - **DC name or IP address (Nom ou adresse IP du contrôleur de domaine)**

     Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules, sans espace.
6. Cliquez sur **Join Domain (Joindre le domaine)**.

La section **Joined Domains (Domaines joints)** contient la liste des domaines dont la jonction a été effectuée et contrôle l'annulation de la jonction et la modification de la méthode de localisation d'un domaine.

Vous trouverez des conseils de dépannage à la section *Échec de la jonction du domaine*.

Pour annuler la jonction d'un domaine :

Dans la section **Joined Domains (Domaines joints)**, sélectionnez le domaine dont vous souhaitez annuler la jonction, puis cliquez sur **Unjoin Domain (Annuler la jonction du domaine)**.

Pour modifier le mode de détection du contrôleur de domaine :

1. Dans la section **Joined Domains (Domaines joints)**, indiquez comment localiser le contrôleur de domaine :
   - **Auto-detect using DNS (Auto-détection via DNS)**
   - **DC name or IP address (Nom ou adresse IP du contrôleur de domaine)**

     Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules, sans espace.
2. Cliquez sur **Appliquer**.

Options d'authentification globales

Ces paramètres s'appliquent lorsque IWA négocie une authentification NTLM ou revient à l'authentification NTLM ou lorsque l'authentification NTLM héritée est utilisée.

1. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Global Authentication Options (Options d'authentification globales)**.
2. L'option **Fail Open (Échec ouvert)** est activée par défaut. Cette option autorise le traitement des requêtes lorsque l'authentification échoue dans les cas suivants :
   - Aucune réponse du contrôleur de domaine
   - Messages malformés provenant du client
   - Réponses SMB non valides

   Avec l'option Fail Open (Échec ouvert), lorsque le filtrage Web est utilisé avec le proxy et qu'un agent XID est configuré, le demandeur peut encore être identifié par l'agent XID et la stratégie appropriée être appliquée en cas d'échec de l'authentification NTLM.

   Désactivez cette option si vous souhaitez que les requêtes ne soient pas envoyées vers Internet lorsque les conditions d'échec d'authentification répertoriées ci-dessus se produisent.
3. L'option **Credential Caching (Mise en cache des informations d'identification)** est activée par défaut. La mise en cache des informations d'identification s'applique uniquement lorsque Content Gateway est déployé en tant que proxy explicite. Les informations d'identification ne sont mises en cache que si l'authentification réussit. Pour désactiver la mise en cache des informations d'authentification, sélectionnez **Désactiver**.
4. L'option **Caching TTL (Durée de vie de la mise en cache)** définit la durée de vie des entrées stockées dans le cache des informations d'identification. La valeur par défaut est 900 secondes (15 minutes). Pour modifier cette durée, saisissez une nouvelle valeur dans le champ. La plage des valeurs prises en charge va de 300 à 86 400 secondes.
5. Si certains utilisateurs se servent de serveurs Terminal Server pour accéder à Internet via le proxy (ex. : serveurs Citrix), vous devez dresser la liste de ces serveurs dans le champ **Multi-user IP Exclusions (Exclusion des adresses IP d'utilisateurs)**. Les informations d'identification de ces utilisateurs ne sont pas mises en cache. Entrez une liste d'adresses IP ou de plages d'adresses IP séparées par des virgules.

> **Remarque**
>
> Content Gateway prend en charge l'authentification transparente dans les clusters de proxy a l'aide de l'équilibrage de la charge WCCP. Toutefois, l'attribut de distribution de la méthode d'affectation doit être l'adresse IP source. Pour plus d'informations, consultez la section *Configuration des groupes de services dans Content Gateway Manager*, page 60.

Création d'une règle de domaine Kerberos accessible via l'authentification Windows intégrée

Avant de créer une règle pour un domaine Kerberos accessible via l'authentification Windows intégrée, vous devez joindre ce domaine. Vous devez également connaître les éléments suivants :

- Le nom du domaine auquel la règle s'applique
- Le jeu d'adresses IP sources à partir desquelles les clients seront authentifiés. Il peut s'agir d'une combinaison d'adresses IP individuelles et/ou de plages d'adresses IP.
- Ou le numéro de port unique sur lequel le trafic est entrant (proxy explicite uniquement)
- Ou une combinaison des deux options précédentes (proxy explicite uniquement)

> **Remarque**
>
> Après avoir saisi tous les spécificateurs, vous devez cliquer sur **Ajouter** avant de cliquer sur **Appliquer**. Si vous cliquez d'abord sur Appliquer, ou si vous fermez la fenêtre d'édition, tous les champs de saisie sont effacés.

1. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès)** et vérifiez ou spécifiez le **Domaine**, les **Options d'authentification globales** et, le cas échéant, les paramètres **Transparent Proxy Authentication (Authentification du proxy transparent)**.
2. Ajoutez au besoin le nouveau domaine (Kerberos) dans l'onglet **Domaines**.
3. Ouvrez l'onglet **Configurer> Sécurité> Access Control (Contrôle d'accès)> Authentication Realms (Authentification des domaines Kerberos)**. La liste de toutes les règles d'authentification des domaines Kerberos apparaît en haut de la page.
4. Cliquez sur **Edit file (Modifier le fichier)** pour ouvrir l'éditeur de règle.
5. Sélectionnez **Authentification Windows intégrée** dans la liste déroulante **Rule Type (Type de règle)**.
6. Sélectionnez **Enable (Activer)** si vous souhaitez que la règle soit active à la fin du processus de définition (une fois que la règle a été ajoutée et que le proxy a redémarré, étapes 12 et 14 ci-dessous).
7. Donnez un **non unique** à la règle. Un nombre bref et descriptif simplifie l'identification et l'administration des règles.

8. Si la règle doit s'appliquer à des adresses IP spécifiques, saisissez une liste d'adresses IP individuelles et de plages d'adresses IP séparées par des virgules dans le champ **Source IP (Adresse IP source)**. N'utilisez pas d'espace. Par exemple :

   10.4.1.1,10.12.1.1-10.12.254.254

   Les plages d'adresses IP sources peuvent se chevaucher. Le chevauchement des plages peut se révéler utile pour identifier les sous-groupes d'un pool plus vaste.

   Dans le cas de plages se chevauchant, la première correspondance est utilisée.
9. Si la règle doit s'appliquer au trafic passant par un port spécifique, sélectionnez **Proxy Port (Port du proxy)** dans la liste déroulante (valide pour un proxy explicite uniquement).
10. Pour définir un nom d'alias à envoyer au service de filtrage (Filtering Service), ouvrez les **paramètres avancés** et sélectionnez **Aliasing (Alias)**. Définissez le nom à utiliser dans le champ. Lorsqu'aucun nom n'est spécifié (le champ est vide), Web Security adopte le même comportement que lorsqu'il répond à des demandes qui n'incluent pas de nom d'utilisateur. Pour plus d'informations sur les alias, consultez la section *Utilisateurs inconnus et option 'alias'*.
11. Dans la liste déroulante **Domain/Realm (Domaine/Domaine Kerberos)** de la section **Integrated Windows Authentication Specifiers (Spécificateurs de l'Authentification Windows intégrée)**, sélectionnez le domaine Kerberos auquel la règle s'applique.
12. Cliquez sur **Ajouter** pour ajouter la règle.
13. En haut de la page, vérifiez, puis ajustez la position de cette règle dans la liste. La première règle correspondante s'applique.
14. Cliquez sur **Appliquer**, puis redémarrez Content Gateway afin que cette règle entre en vigueur.

Avertissement

Lorsqu'une règle contient des valeurs non valides, un message d'avertissement s'affiche et l'identifie.

Création d'une règle de domaine Kerberos accessible via l'authentification NTLM

Avant de créer une règle pour un domaine Kerberos accessible via l'authentification NTLM, vous devez connaître les éléments suivants :

- Le jeu d'adresses IP sources à partir desquelles les clients seront authentifiés. Il peut s'agir d'une combinaison d'adresses IP individuelles et de plages d'adresses IP.
- Ou le numéro de port unique sur lequel le trafic est entrant (proxy explicite uniquement)
- Ou une combinaison des deux options précédentes (proxy explicite uniquement)
- Le nom ou l'adresse IP et le numéro de port du contrôleur de domaine principal et des contrôleurs de domaine secondaires à utiliser pour l'équilibrage de la charge ou le basculement

Remarque

Après avoir saisi tous les spécificateurs, vous devez cliquer sur **Ajouter** avant de cliquer sur **Appliquer**. Si vous cliquez d'abord sur Appliquer, ou si vous fermez la fenêtre d'édition, tous les champs de saisie sont effacés.

1. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès)** et vérifiez ou spécifiez le **Domaine**, les **Options d'authentification globales** et, le cas échéant, les paramètres **Transparent Proxy Authentication (Authentification du proxy transparent)**.
2. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**. La liste de toutes les règles d'authentification des domaines Kerberos apparaît en haut de la page.
3. Cliquez sur **Edit file (Modifier le fichier)** pour ouvrir l'éditeur de règle.
4. Sélectionnez **NTLM** dans la liste déroulante **Rule Type (Type de règle)**.
5. Sélectionnez **Enable (Activer)** si vous souhaitez que la règle soit active à la fin du processus de définition (une fois que la règle a été ajoutée et que le proxy a redémarré, étapes 12 et 14 ci-dessous).
6. Donnez un **non unique** à la règle. Un nombre bref et descriptif simplifie l'identification et l'administration des règles.
7. Si la règle doit s'appliquer à des adresses IP spécifiques, saisissez une liste d'adresses IP individuelles et de plages d'adresses IP séparées par des virgules dans le champ **Source IP (Adresse IP source)**. N'utilisez pas d'espace. Par exemple :

   10.4.1.1,10.12.1.1-10.12.254.254

   Les plages d'adresses IP sources peuvent se chevaucher. Le chevauchement des plages peut se révéler utile pour identifier les sous-groupes d'un pool plus vaste.

   Dans le cas de plages se chevauchant, la première correspondance est utilisée.
8. Si la règle doit s'appliquer au trafic passant par un port spécifique, sélectionnez **Proxy Port (Port du proxy)** dans la liste déroulante.
9. Pour définir un nom d'alias à envoyer au service de filtrage (Filtering Service), ouvrez les **paramètres avancés** et sélectionnez **Aliasing (Alias)**. Définissez le nom à utiliser dans le champ. Lorsqu'aucun nom n'est spécifié (le champ est vide), Web Security adopte le même comportement que lorsqu'il répond à des demandes qui n'incluent pas de nom d'utilisateur. Pour plus d'informations sur les alias, consultez la section *Utilisateurs inconnus et option 'alias'*.
10. Dans **DC List (Liste des contrôleurs de domaine)**, entrez l'adresse IP et le numéro de port du contrôleur de domaine principal. Lorsqu'aucun port n'est spécifié, Content Gateway utilise le port 139.

    Vous pouvez également spécifier des contrôleurs de domaine secondaires dans une liste séparée par des virgules. Les formats pris en charge sont :

    nom_hôte[:port][%nom_netbios]

    adresse_IP[:port][%nom_netbios]

    Le **nom_netbios** est requis avec Active Directory 2008.
11. Sélectionnez **DC Load Balance (Équilibrage de la charge des contrôleurs de domaine)** pour activer l'équilibrage de la charge entre les contrôleurs de domaine.

> **Remarque**
>
> Lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé.

12. Cliquez sur **Ajouter** pour ajouter la règle.
13. En haut de la page, vérifiez, puis ajustez la position de cette règle dans la liste. La première règle correspondante s'applique.
14. Cliquez sur **Appliquer**, puis redémarrez Content Gateway afin que cette règle entre en vigueur.

> **Avertissement**
> Lorsqu'une règle contient des valeurs non valides, un message d'avertissement s'affiche et l'identifie.

Création d'une règle de domaine Kerberos accessible via l'authentification LDAP

Avant de créer une règle de domaine Kerberos accessible via l'authentification LDAP, vous devez connaître les éléments suivants :

- Le jeu d'adresses IP sources à envoyer au serveur LDAP. Il peut s'agir d'une combinaison d'adresses IP individuelles et de plages d'adresses IP.
- Ou le numéro de port unique sur lequel le trafic est entrant (proxy explicite uniquement)
- Ou une combinaison des deux options précédentes (proxy explicite uniquement)
- Le nom et le numéro de port du serveur LDAP
- Le nom unique de la base de recherche LDAP
- Le nom unique et le mot de passe de la liaison LDAP
- Le cas échéant, le nom et la valeur de l'attribut LDAP

> **Remarque**
> Après avoir saisi tous les spécificateurs, vous devez cliquer sur **Ajouter** avant de cliquer sur **Appliquer**. Si vous cliquez d'abord sur Appliquer, ou si vous fermez la fenêtre d'édition, tous les champs de saisie sont effacés.

1. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès)** et vérifiez ou spécifiez le **Domaine**, les **Options d'authentification globales** et, le cas échéant, les paramètres **Transparent Proxy Authentication (Authentification du proxy transparent)**.
2. Ouvrez l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**. La liste de toutes les règles d'authentification des domaines Kerberos apparaît en haut de la page.
3. Cliquez sur **Edit file (Modifier le fichier)** pour ouvrir l'éditeur de règle.
4. Sélectionnez **LDAP** dans la liste déroulante **Rule Type (Type de règle)**.
5. Sélectionnez **Enable (Activer)** si vous souhaitez que la règle soit active à la fin du processus de définition (une fois que la règle a été ajoutée et que le proxy a redémarré, étapes 19 et 21 ci-dessous).
6. Donnez un **non unique** à la règle. Un nombre bref et descriptif simplifie l'identification et l'administration des règles.

7. Si la règle doit s'appliquer à des adresses IP spécifiques, saisissez une liste d'adresses IP individuelles et de plages d'adresses IP séparées par des virgules dans le champ **Source IP (Adresse IP source)**. N'utilisez pas d'espace. Par exemple :

   10.4.1.1,10.12.1.1-10.12.254.254

   Les plages d'adresses IP sources peuvent se chevaucher. Le chevauchement des plages peut se révéler utile pour identifier les sous-groupes d'un pool plus vaste.

   Dans le cas de plages se chevauchant, la première correspondance est utilisée.
8. Si la règle doit s'appliquer au trafic entrant par un port spécifique, sélectionnez **Proxy Port (Port du proxy)** dans la liste déroulante.
9. Pour définir un nom d'alias à envoyer au service de filtrage (Filtering Service), ouvrez les **paramètres avancés** et sélectionnez **Aliasing (Alias)**. Définissez le nom à utiliser dans le champ. Lorsqu'aucun nom n'est spécifié (le champ est vide), Web Security adopte le même comportement que lorsqu'il répond à des demandes qui n'incluent pas de nom d'utilisateur. Pour plus d'informations sur les alias, consultez la section *Utilisateurs inconnus et option 'alias'*.
10. Dans le champ **LDAP Server Name (Nom du serveur LDAP)**, entrez le nom de domaine complet et le numéro de port ou l'adresse IP du serveur LDAP.
11. Si le port du serveur LDAP n'est pas le port par défaut (389), saisissez-le dans le champ **LDAP Server Port (Port du serveur LDAP)**.
12. Entrez le **LDAP Base Distinguished Name (Nom unique de la base de recherche LDAP)**. Demandez cette valeur à votre administrateur LDAP.
13. Entrez éventuellement le filtre UID LDAP. Servez-vous de ce champ pour définir le type de serveur lorsque ce dernier ne correspond pas à la valeur **Server Type (Type de serveur)** définie dans l'onglet **LDAP** (valeur par défaut). Entrez **sAMAccountName** pour Active Directory ou **uid** pour les autres services.
14. Dans le champ **Bind DN (Nom distinctif de liaison)**, entrez le nom distinctif de liaison. Il doit s'agir du nom distinctif complet d'un utilisateur du service d'annuaire LDAP. Par exemple :

    CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
15. Dans le champ **Bind Password (Mot de passe de liaison)**, entrez le mot de passe du nom saisi dans le champ **Bind DN (Nom distinctif de liaison)**.
16. Si vous voulez que le proxy communique de manière sécurisée avec le serveur LDAP, activez l'option **Secure LDAP (LDAP sécurisé)**.
17. Saisissez éventuellement un nom d'attribut LDAP.
18. Saisissez éventuellement une valeur d'attribut LDAP.
19. Cliquez sur **Ajouter** pour ajouter la règle.
20. En haut de la page, vérifiez, puis ajustez la position de cette règle dans la liste. La première règle correspondante s'applique.
21. Cliquez sur **Appliquer**, puis redémarrez Content Gateway afin que cette règle entre en vigueur.

Avertissement

Lorsqu'une règle contient des valeurs non valides, un message d'avertissement s'affiche et l'identifie.

Utilisation des règles d'authentification dans plusieurs domaines Kerberos

Modification d'une règle

1. Dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**, cliquez sur **Edit File (Modifier le fichier)**.
2. Dans le tableau des règles, cliquez sur la règle à modifier. Ses valeurs apparaissent dans les champs du volet de définition.
3. Apportez les modifications nécessaires, puis cliquez sur **Set (Définir)** et sur **Appliquer**.
4. Cliquez sur **Fermer** pour revenir dans l'onglet **Authentication Realms (Authentification des domaines Kerberos)**.
5. **Redémarrez** Content Gateway afin que vos modifications entrent en vigueur.

Réorganisation de la liste des règles

Les règles d'authentification dans plusieurs domaines Kerberos s'appliquent selon leur ordre d'apparition dans la liste, de haut en bas.

1. Dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**, cliquez sur **Edit File (Modifier le fichier)**.
2. Dans le tableau des règles, cliquez sur celle que vous souhaitez repositionner dans la liste, puis sur les flèches haut ou bas pour la déplacer.
3. Lorsque l'ordre des règles vous convient, cliquez sur **Appliquer**.
4. Cliquez sur **Fermer** pour revenir dans l'onglet **Authentication Realms (Authentification des domaines Kerberos)**.
5. **Redémarrez** Content Gateway afin que vos modifications entrent en vigueur.

Suppression d'une règle

1. Dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**, cliquez sur **Edit File (Modifier le fichier)**.
2. Dans le tableau des règles, cliquez sur la règle à supprimer, puis sur le bouton « X » à gauche.
3. Lorsque la suppression des règles est terminée, cliquez sur **Appliquer**.
4. Cliquez sur **Fermer** pour revenir dans l'onglet **Authentication Realms (Authentification des domaines Kerberos)**.
5. **Redémarrez** Content Gateway afin que vos modifications entrent en vigueur.

Cas d'utilisation de l'authentification dans plusieurs domaines Kerberos

Cas d'utilisation 1 :

Cette section présente un cas courant dans lequel un second domaine est ajouté dans un environnement à un seul domaine. Content Gateway est un proxy explicite. Les clients utilisent un fichier PAC.

Une entreprise, appelons-la Quality Corp, utilise une installation logicielle de Content Gateway. Elle ne dispose que d'un seul domaine (QCORP) et un contrôleur de domaine. Elle utilise NTLM pour authentifier ses utilisateurs.

Quality Corp fait l'acquisition de New Corp, qui dispose de son propre domaine (NCORP) et d'un contrôleur de domaine. L'authentification des utilisateurs est effectuée via LDAP.

Quality Corp souhaite gérer l'ensemble des employés dans un domaine unique, mais n'est pas prête à modifier son infrastructure en conséquence. En attendant que cette opération soit possible, elle voudrait exploiter une stratégie d'utilisation distincte pour les utilisateurs de New Corp (c'est-à-dire ne pas utiliser l'utilisateur par défaut du domaine QCORP).

Cette opération est rendue possible par la fonction d'authentification dans plusieurs domaines Kerberos.

Pour configurer la solution, Quality Corp doit :

1. Activer l'authentification dans plusieurs domaines Kerberos
2. Ajouter un second port HTTP non défini par défaut (**Configurer > Protocoles > HTTP**). Ce port sera utilisé par tous les membres de NCORP.
3. Créer un fichier PAC pour les membres de NCORP les obligeant à se connecter à Content Gateway sur le nouveau second port
4. Créer des règles d'authentification dans plusieurs domaines Kerberos, une pour chacun des domaines QCORP et NCORP :
    a. Définir une règle NCORP pour les connexions sur le second port. Spécifier dans les paramètres avancés que l'identification de l'utilisateur à choisir est la chaîne statique « NCorpUser ».
    b. Définir la règle QCORP pour la gestion de toutes les autres connexions
5. Ajouter « NCorpUser » dans le domaine QCORP en tant qu'utilisateur valide et créer une stratégie pour cet utilisateur dans TRITON—Web Security

À ce stade, tous les utilisateurs se connectant à Content Gateway à partir de NCORP s'authentifient auprès du contrôleur de domaine NCORP et obtiennent la stratégie de groupe associée à NCorpUser. Notez que ce scénario n'autorise pas l'utilisation de stratégies ou de fonctions basées sur l'utilisateur individuel, telles que le temps contingenté. Les transactions sont enregistrées dans le journal en tant que NCorpUser. Cette configuration est effectuée sans aucun impact sur l'authentification, la stratégie ou la connexion des utilisateurs du domaine QCORP.

Cas d'utilisation 2 :

Cette section présente un cas courant dans lequel un second domaine est ajouté dans un environnement à un seul domaine. Content Gateway est un proxy explicite. Les clients utilisent un fichier PAC.

Une entreprise, appelons-la BigStars, utilise une installation logicielle de Content Gateway. Elle ne dispose que d'un seul domaine (BIG) et un contrôleur de domaine. Elle utilise NTLM pour authentifier ses utilisateurs.

Un groupe de la société remplace ses ordinateurs par des ordinateurs Apple, pour lesquels l'authentification NTLM n'est pas possible. Le service informatique installe un serveur LDAP et crée un nouveau domaine (BIGAPL) pour les utilisateurs Apple.

Comme ce groupe d'utilisateurs existait déjà auparavant et était géré au niveau du domaine principal (BIG), le service informatique s'attend à ce que la stratégie basée sur l'utilisateur et la journalisation s'appliquent toujours.

Cette opération est rendue possible par la fonction d'authentification dans plusieurs domaines Kerberos.

Pour configurer la solution, BigStars doit :

1. Vérifier que tous les utilisateurs de BIGAPL sont également dans BIG avec le même nom d'utilisateur
2. Activer l'authentification dans plusieurs domaines Kerberos
3. Ajouter un second port HTTP non défini par défaut (**Configurer > Protocoles > HTTP**). Ce port sera utilisé par tous les membres de BIGAPL.
4. Créer un fichier PAC pour les membres de BIGAPL les obligeant à se connecter à Content Gateway sur le nouveau second port
5. Créer des règles d'authentification dans plusieurs domaines Kerberos, une pour chacun des domaines BIGAPL et BIG
    a. Définir la règle BIGAPL pour les connexions sur le second port
    b. Définir la règle BIG pour la gestion de toutes les autres connexions

À ce stade, tous les membres de BIGAPL sont authentifiés via LDAP, mais conservent leur stratégie individuelle telle que spécifiée par leurs autres identités NTLM. Les journaux et les rapports font également référence à ce même utilisateur.

Cas d'utilisation 3 :

Cette section présente un cas courant dans lequel un second domaine à objectif particulier est ajouté dans un environnement à un seul domaine. Content Gateway est un proxy transparent qui utilise WCCP v2.

Une entreprise, appelons-la Creative Corp, utilise une installation logicielle de Content Gateway. Elle ne dispose que d'un seul domaine (CCORP) et un contrôleur de domaine. Elle utilise NTLM pour authentifier ses utilisateurs.

Creative Corp est sur le point de commercialiser un nouveau produit et souhaite faire un tabac. Elle décide de faire une journée porte ouverte, avec kiosques, démonstrations et présentateurs. Les kiosques doivent servir à la démonstration du nouveau produit et n'ont donc besoin que de la stratégie Internet par défaut. Le responsable informatique préfère que le réseau des kiosques soit aussi isolé du réseau intranet de l'entreprise que possible. Dans ce scénario, la journalisation des utilisateurs individuels n'est pas requise.

Cette opération est rendue possible par la fonction d'authentification dans plusieurs domaines Kerberos.

Pour configurer la solution, Creative Corp doit :

1. Créer un nouveau réseau temporaire complet disposant de son propre contrôleur de domaine. Appelons ce domaine CTEMP.
2. Ajouter un ou plusieurs utilisateurs dans CTEMP. Elle peut établir une correspondance une à une sur les utilisateurs existants dans le domaine principal ou une correspondance d'un ou plusieurs utilisateurs génériques destinée aux présentateurs.
3. Rediriger le trafic Internet sur CTEMP vers Content Gateway avec WCCP v2
4. Activer l'authentification dans plusieurs domaines Kerberos
5. Créer des règles d'authentification dans plusieurs domaines Kerberos, une pour chacun des domaines CTEMP et CCORP :
    a. Définir la règle CTEMP devant s'appliquer à toutes les connexions provenant de la plage d'adresses IP attribuée au domaine CTEMP. Dans les paramètres avancés, définir l'utilisation des alias et ne pas renseigner le champ. Le résultat de l'application de la stratégie par défaut s'appliquera alors à tous les utilisateurs de CTEMP.
    b. Définir la règle CCORP pour la gestion de toutes les autres connexions

À ce stade, toute personne utilisant Internet via l'un des kiosques est authentifiée sur le réseau CTEMP et la stratégie par défaut s'applique à ses requêtes.

Résolution des problèmes liés à l'authentification dans plusieurs domaines Kerberos

Dans l'authentification dans plusieurs domaines Kerberos, les problèmes courants sont les suivants :

- Les utilisateurs ne sont *pas* invités à s'authentifier alors qu'ils le devraient.
- Les utilisateurs *sont* invités à s'authentifier alors qu'ils ne le devraient pas.
- L'authentification des utilisateurs ne s'effectue pas sur le bon domaine.

Ces problèmes surviennent dans l'une des phases suivantes du traitement de l'authentification des utilisateurs :

- Logique générale d'authentification des utilisateurs (décrite ci-dessous)
- Définition et correspondance des règles de domaine Kerberos
- Traitement des protocoles d'authentification des utilisateurs (IWA, NTLM, LDAP). Pour le dépannage d'IWA, consultez la section *Résolution des problèmes liés à l'Authentification Windows intégrée*.

Logique de l'authentification dans plusieurs domaines Kerberos

L'authentification dans plusieurs domaines Kerberos suit toujours la logique suivante :

1. Les règles du fichier **filter.config** sont vérifiées et appliquées. Cette action est toujours la première étape quel que soit le type d'authentification utilisé par Content Gateway. Lorsqu'une règle de filtrage correspond, cette règle s'applique et le traitement de l'authentification des utilisateurs cesse. Voir *Règles de filtrage*, page 167.

2. Lorsqu'aucune règle de filtrage ne correspond, la correspondance de règle de domaine Kerberos est effectuée. L'adresse IP du demandeur est comparée à l'ensemble des règles, de haut en bas. Si l'adresse IP correspond à une règle, le port source est vérifié lorsque la règle en définit un. La première règle correspondante s'applique. **Lorsqu'aucune règle ne correspond, aucune authentification n'est tentée.**
3. Lorsqu'une règle correspond, le protocole d'authentification défini s'applique au domaine spécifié. Tous les détails de la configuration de la règle s'appliquent.
4. Lorsque l'utilisateur est authentifié, la requête est traitée ou refusée conformément à la stratégie Web Security.
5. La transaction est enregistrée dans un journal.

Pour comprendre comment la logique s'applique dans un environnement de production, vous pouvez activer temporairement le résultat du débogage pour l'authentification des utilisateurs. Entre autres détails, le résultat du débogage présente l'analyse des règles et des correspondances. Voir *Activation et désactivation des résultats du débogage de l'authentification des utilisateurs*.

Dépannage

Lorsque l'authentification dans plusieurs domaines Kerberos ne donne pas les résultats escomptés, il est préférable de résoudre les problèmes dans l'ordre suivant :

1. **Vérifier la traduction d'adresses réseau (NAT)**

   Vérifiez que la traduction des adresses réseau fonctionne comme prévu. Cette traduction remplace l'adresse IP source d'origine par une autre adresse avant l'authentification des utilisateurs. Dans Content Gateway Manager, sélectionnez **Configurer > Networking (Mise en réseau) > ARM > Général** et examinez les règles définies dans le fichier **ipnat.config**.
2. **Vérifier les règles définies dans le fichier filter.config**

   Vérifiez que les correspondances des règles définies dans le fichier **filter.config** fonctionnent comme prévu. Les règles définies dans le fichier filter.config peuvent servir entre autres à contourner l'authentification des utilisateurs. Voir *Règles de filtrage*.
3. **Vérifier les correspondances de règles de domaine Kerberos**

   En utilisant l'adresse IP d'un utilisateur invité ou non à s'authentifier comme prévu, parcourez chaque règle de domaine Kerberos, de haut en bas, en examinant les paramètres pour identifier la première correspondance. Montrez-vous méticuleux dans votre analyse. Il arrive souvent que l'adresse IP appartienne à une plage d'adresses IP trop vaste.

   Si la règle utilise un alias, vérifiez que cet alias est présent dans le service des utilisateurs du contrôleur de domaine principal.

   Dans le cas des clients explicites configurés pour envoyer le trafic vers un port spécifique, vérifiez à la fois la règle et la configuration du navigateur du client.
4. **Vérifier le domaine**

   Si vous obtenez la correspondance prévue, vérifiez que le domaine est accessible et que l'utilisateur est bien membre de ce domaine. Dans l'affirmative, dépannez le problème au niveau du protocole d'authentification. Pour IWA, consultez la section *Résolution des problèmes liés à l'Authentification Windows intégrée*.

5. **Lorsque Content Gateway est une chaîne de proxy**

   Si Content Gateway est membre d'une chaîne de proxy, vérifiez que les en-têtes X-Forwarded-For sont envoyés par le proxy en aval et lus par Content Gateway.

   - Utilisez un analyseur de paquets pour examinez les paquets entrants provenant du proxy en aval. Recherchez des en-têtes X-Forwarded-For correctement mis en forme.
   - Dans Content Gateway Manager, sélectionnez **Configurer > Mon proxy > De base**, faites défiler l'écran jusqu'au bas de la page et vérifiez que l'option **Read authentication from child proxy (Lire l'authentification à partir du proxy enfant)** est bien activée. Si ce n'est pas le cas, sélectionnez **On (Activer)**, cliquez sur **Appliquer**, puis redémarrez Content Gateway.

Activation et désactivation des résultats du débogage de l'authentification des utilisateurs

Avertissement

Il est préférable de ne pas activer en permanence les résultats du débogage. Cette option ralentit les performances du proxy et peut inonder le système de fichiers de journaux de résultats.

Les informations du journal de débogage sont stockées dans : **/opt/WCG/logs/content_gateway.out**.

Pour activer les informations du débogage de l'authentification des utilisateurs, modifiez : **/opt/WCG/config/records.config**

```
(racine)# vi /opt/WCG/config/records.config
```

Localisez et modifiez les paramètres suivants en leur attribuant les valeurs telles qu'indiquées :

```
CONFIG proxy.config.diags.debug.enabled INT 1
CONFIG proxy.config.diags.debug.tags STRING
   auth_* | winauth.* | ldap.* | ntlm.*
```

Enregistrez et fermez le fichier. Obligez Content Gateway à relire le fichier via la commande suivante :

```
(racine)# /opt/WCG/bin/content_line -x
```

Pour suivre le flux des informations du débogage, utilisez la commande **tail -f** :

```
(racine)# tail -f /opt/WCG/logs/content_gateway.out
```

Pour mettre fin à la commande, utilisez **Ctrl+C**.

Lorsque vous avez collecté les résultats du débogage désiré (à la fin d'un ou plusieurs processus d'authentification d'utilisateurs), désactivez les résultats du débogage en modifiant à nouveau le fichier **records.config** et la valeur des paramètres tel qu'indiqué.

```
(racine)# CONFIG proxy.config.diags.debug.enabled INT 0
```

Enregistrez et fermez le fichier. Obligez Content Gateway à relire le fichier via la commande suivante :

```
(racine)# /opt/WCG/bin/content_line -x
```

15 Utilisation des fichiers journaux

Rubriques connexes :

- *Fichiers journaux d'événements*, page 212
- *Gestion des fichiers journaux d'événements*, page 213
- *Formats des fichiers journaux d'événements*, page 215
- *Rotation des fichiers journaux d'événements*, page 221
- *Division des fichiers journaux d'événements*, page 224
- *Collecte des fichiers journaux d'événements*, page 226
- *Affichage des statistiques de journalisation*, page 230
- *Affichage des fichiers journaux*, page 230
- *Exemple d'entrées de fichier journal d'événements*, page 232

Websense Content Gateway conserve 3 types de fichiers journaux :

- Les *fichiers journaux système* stockent les informations relatives au système, ce qui comprend les messages liés à l'état de Content Gateway et les erreurs ou avertissements éventuellement générés. Ces informations peuvent inclure une note précisant que les fichiers journaux d'événements ont fait l'objet d'une rotation, un avertissement indiquant que la communication du cluster a expiré ou une erreur signalant que Content Gateway a redémarré. (Content Gateway publie des alarmes révélant des conditions d'erreur dans Content Gateway Manager. Pour plus d'informations, consultez la section *Utilisation des alarmes*, page 113.)

  Tous les messages d'information du système sont enregistrés via le mécanisme de journalisation de l'ensemble du système **syslog** dans l'utilitaire du démon. Le fichier de configuration **syslog.conf** (stocké dans le répertoire **/etc**) indique où ces messages sont enregistrés. L'emplacement est généralement **/var/log/messages**.

  Fonctionnant à l'échelle du système, le processus **syslog** est le seul référentiel de messages pour tous les processus de Content Gateway, **content_gateway**, **content_manager** et **content_cop** compris.

  Chaque entrée du journal contient des informations sur la date et l'heure auxquelles l'erreur a été enregistrée, le nom d'hôte du serveur proxy ayant signalé l'erreur et la description de l'erreur ou de l'avertissement.

  Pour obtenir la liste des messages d'information système enregistrés par Content Gateway, consultez la section *Messages d'erreur de Websense Content Gateway*, page 453.

- Les *fichiers journaux d'erreurs* enregistrent des informations sur la raison pour laquelle une transaction a généré une erreur.
- Les *fichiers journaux d'événements* (également appelés *fichiers journaux de l'accès*) enregistrent des informations sur l'état de chaque transaction traitée par Content Gateway.

Content Gateway crée des fichiers journaux d'erreurs et d'événements et enregistre les informations relatives au système dans les fichiers journaux système. Vous pouvez désactiver la journalisation des événements et/ou des erreurs. Il est recommandé de n'enregistrer les erreurs ou de ne désactiver la journalisation que pendant les heures de pointe.

▶ Dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation)**, sélectionnez l'une des options suivantes : **Log Transactions and Errors (Enregistrer les transactions et les erreurs)**, **Log Transactions Only (Enregistrer les transactions uniquement)**, **Log Errors Only (Enregistrer les erreurs uniquement)** ou **Disabled (Désactivé)**.

Fichiers journaux d'événements

Les fichiers journaux d'événements enregistrent des informations sur toutes les requêtes traitées par Websense Content Gateway. L'analyse des fichiers journaux vous permet de déterminer le nombre de personnes utilisant le proxy, le volume d'informations demandée par chaque personne, les pages les plus populaires, etc.

Content Gateway reconnaît plusieurs formats de fichier journal standard, tels que Squid et Netscape, et les formats personnalisés définis par l'utilisateur. Vous pouvez analyser les fichiers journaux de format standard à l'aide de packages d'analyse prêts à l'emploi. Pour simplifier l'analyse des fichiers journaux, vous pouvez les classer de sorte qu'ils contiennent des informations propres au protocole ou aux hôtes. Vous pouvez également configurer Content Gateway pour qu'il effectue automatiquement la rotation des fichiers journaux à intervalles spécifiques au cours de la journée.

Les sections suivantes décrivent comment :

- Gérer les fichiers journaux d'événements

  Vous pouvez sélectionner un emplacement central de stockage des fichiers journaux et définir la quantité d'espace disque réservée à ces fichiers journaux et leu mode et leur fréquence de rotation. Voir *Gestion des fichiers journaux d'événements*, page 213.
- Choisir les différents formats des fichiers journaux d'événements

  Vous pouvez choisir les formats de fichiers journaux standard à utiliser pour l'analyse du trafic (par exemple, Squid ou Netscape). Vous pouvez aussi utiliser le format personnalisé de Content Gateway, un format de type XML qui vous permet de mieux contrôler le type d'informations enregistré dans les fichiers journaux. Voir *Formats des fichiers journaux d'événements*, page 215.
- Définir la rotation automatique des fichiers journaux d'événements

  Vous pouvez configurer Content Gateway pour qu'il fasse tourner les fichiers journaux d'événements à intervalles spécifiques tout au long de la journée de manière à pouvoir identifier et gérer les fichiers journaux inactifs. Voir *Rotation des fichiers journaux d'événements*, page 221.

- Différencier les fichiers journaux selon les hôtes

  Vous pouvez configurer le proxy pour qu'il crée des fichiers journaux distincts pour les différents protocoles en fonction de l'hôte. Voir *Division des fichiers journaux d'événements*, page 224.
- Collecter des fichiers journaux à partir des différents nœuds

  Vous pouvez désigner un ou plusieurs nœuds du réseau devant agir en tant que serveurs de collecte des journaux. Ces serveurs, qui peuvent être autonomes ou faire partie de Content Gateway, vous permettent de stocker l'ensemble des informations enregistrées dans des emplacements bien définis. Voir *Collecte des fichiers journaux d'événements*, page 226.
- Afficher des statistiques sur le système de journalisation

  Content Gateway fournit des statistiques sur le système de journalisation. Vous pouvez y accéder via Content Gateway Manager ou par le biais de l'interface de ligne de commande. Voir *Affichage des statistiques de journalisation*, page 230.
- Afficher les fichiers journaux

  Vous pouvez afficher les fichiers journaux système, d'événements et d'erreurs créés par Content Gateway. Vous pouvez afficher un fichier journal dans son intégralité, un nombre donné de lignes récentes du fichier journal ou toutes les lignes contenant une chaîne définie.
- Interpréter les entrées des fichiers journaux pour les formats de fichier standard. Voir *Exemple d'entrées de fichier journal d'événements*, page 232.

Gestion des fichiers journaux d'événements

Vous pouvez gérer vos fichiers journaux d'événements et contrôler leur emplacement, le volume d'espace disque qu'ils utilisent et le mode de gestion du manque d'espace disque dans le répertoire de journalisation.

Choix du répertoire de journalisation

Par défaut, Content Gateway stocke tous les fichiers journaux d'événements dans le répertoire **logs**, situé dans le répertoire d'installation de Content Gateway. Pour utiliser un autre répertoire, consultez la section *Définition des options de gestion des fichiers journaux*, page 214.

Contrôle de l'espace réservé à la journalisation

Vous pouvez contrôler le volume d'espace disque réservé au répertoire de journalisation. Cela permet au système de mieux fonctionner au sein de la fenêtre d'espace défini pendant une longue période.

Lorsque vous définissez une limite d'espace, Content Gateway continue de surveiller l'espace disponible dans le répertoire de journalisation. Lorsque l'espace disque se rapproche de la limite disponible (voir *Définition des options de gestion des fichiers journaux*, page 214), Content Gateway passe en état d'espace faible et prend les mesures suivantes :

- Si l'option de suppression automatique (détaillée à la section *Rotation des fichiers journaux d'événements*, page 221) est *activée*, Content Gateway identifie les fichiers journaux ayant déjà fait l'objet d'une rotation (fichiers journaux avec extension **.old**) et commence à supprimer les fichiers un par un, en commençant par le plus ancien, jusqu'à ce qu'il ne soit plus dans cet état. Content Gateway conserve un enregistrement de tous les fichiers supprimés dans le journal des erreurs système.
- Si l'option de suppression automatique est *désactivée* ou lorsque le nombre d'anciens fichiers journaux pouvant être supprimés ne permet pas au système de sortir de cet état d'espace insuffisant, Content Gateway émet un avertissement et poursuit la journalisation jusqu'à ce que tout l'espace disponible soit utilisé. Content Gateway reprend ensuite la journalisation des événements lorsqu'il dispose à nouveau de suffisamment d'espace pour sortir de cet état d'espace disponible faible. Pour récupérer de l'espace, vous pouvez supprimer des fichiers dans le répertoire de journalisation ou augmenter le volume d'espace réservé à la journalisation.

Vous pouvez exécuter un script **cron** combiné à Content Gateway pour supprimer automatiquement les anciens fichiers journaux du répertoire de journalisation (avant que Content Gateway ne passe en état d'espace insuffisant) et les stocker dans une partition temporaire. Après avoir déplacé les fichiers, vous pouvez exécuter des scripts d'analyse de journal sur ces fichiers, puis compresser les journaux et les stocker dans un espace d'archivage ou les supprimer.

Définition des options de gestion des fichiers journaux

1. Sélectionnez **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation)**.
2. Dans le champ **Log Directory (Répertoire des journaux)**, entrez le chemin d'accès du répertoire dans lequel vous souhaitez stocker les fichiers journaux d'événements. Il peut s'agir d'un chemin absolu ou relatif conduisant au répertoire d'installation de Content Gateway. Le répertoire par défaut est le répertoire **logs**, situé dans le répertoire d'installation de Content Gateway.

   Remarque

   Le répertoire que vous spécifiez doit déjà exister.

   L'utilisateur Websense doit disposer d'autorisations en lecture/écriture sur le répertoire de stockage des fichiers journaux.

3. Dans le champ **Limite** du volet **Log Space (Espace des journaux)**, entrez la quantité maximale d'espace à attribuer au répertoire de journalisation.

   Lorsque Content Gateway est installé dans un dispositif V-series, la taille est définie sur 5 120 (5 Go) et n'est pas modifiable.

   Lorsque Content Gateway est installé dans un serveur autonome, la taille par défaut est de 20 480 (20 Go) et peut être configurée.

   Remarque

   Tous les fichiers du répertoire de journalisation contribuent à l'espace consommé, y compris lorsqu'il n'y a pas de fichiers journaux.

4. Dans le champ **Headroom (Marge)**, saisissez la marge de tolérance associée à la limite d'espace à la disposition des journaux. La valeur par défaut est 100 Mo.

   Lorsque l'option **Auto-Delete Rolled Files (Supprimer automatiquement les fichiers après leur rotation)** est activée dans la section **Log Rolling (Rotation des journaux)**, la suppression automatique intervient lorsque le volume d'espace disponible dans le répertoire de journalisation est inférieure à la marge définie. Pour plus d'informations sur la rotation des fichiers journaux, consultez la section *Rotation des fichiers journaux d'événements*, page 221.

5. Cliquez sur **Appliquer**.

Formats des fichiers journaux d'événements

Websense Content Gateway prend en charge les formats de fichiers journaux suivants :

- *Formats standard*, tels que Squid ou Netscape (voir *Utilisation des formats standard*, page 216)
- *Format personnalisé* de Content Gateway (voir *Format personnalisé*, page 216)

Outre les formats de fichiers journaux standard et personnalisés, vous devez indiquer si les fichiers journaux doivent être enregistrés au format *binaire* ou *ASCII*. Voir *Choix du mode binaire ou ASCII*, page 219.

Important

Les fichiers journaux d'événements consomment une grande quantité d'espace disque. La création simultanée d'entrées de journal dans plusieurs formats peut très rapidement consommer l'ensemble des ressources disponibles et affecter les performances du proxy.

Important

Lorsqu'IPv6 est activé, les entrées du journal des événements sont normalisées au format IPv6.

Par exemple, l'entrée « 10.10.41.200 » est journalisée sous la forme « ::ffff:10.10.41.200 ».

Pour récupérer le client « 10.10.41.200 » dans un journal personnalisé, utilisez le filtre suivant :

```
<LogFilter>
   <Name = "Machine_Test_IPv6"/>
   <Condition =
       "chi MATCH ::ffff:10.10.41.200"/>
   <Action = "ACCEPT"/>
</LogFilter>
```

Utilisation des formats standard

Les formats de journaux standard incluent Squid, Netscape Common, Netscape Extended et Netscape Extended-2.

Un large éventail de packages d'analyse prêts à l'emploi permettent d'analyser les formats de fichiers journaux standard. À moins que ces formats ne fournissent les informations dont vous avez besoin, il est préférable d'utiliser l'un des formats de journaux d'événements standard. Voir *Format personnalisé*, page 216.

Par défaut, Content Gateway est configuré pour utiliser uniquement le format de fichier journal Netscape Extended.

Définitions des options de formats de fichiers journaux standard

1. Sélectionnez **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Formats**.
2. Activez le format que vous souhaitez utiliser.
3. Sélectionnez un type de fichier journal (**ASCII** ou **binaire**).
4. Dans le champ **Nom de fichier**, saisissez le nom à utiliser pour vos fichiers journaux d'événements.
5. Dans le champ **En-tête**, saisissez le texte de l'en-tête devant s'afficher en haut des fichiers journaux d'événements. Si vous ne souhaitez pas utiliser d'en-tête, ne renseignez pas ce champ.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **Redémarrer** dans **Configurer > Mon proxy > De base > Général**.

Format personnalisé

Le format XML des journaux personnalisés est plus souple que les formats de fichiers journaux standard et vous permet de mieux contrôler le type d'informations enregistrées. Si vous avez besoin d'analyser des données non disponibles dans les formats standard, créez un format de journal personnalisé. Vous pouvez choisir les informations enregistrées pour chaque transaction Content Gateway et créer des filtres pour choisir quelles transactions enregistrer dans le journal.

Le cœur de la fonction de journalisation personnalisée est un fichier de configuration de type XML (**logs_xml.config**) qui vous permet de créer une description modulaire des objets enregistrés. Pour créer des fichiers journaux personnalisés, le fichier **logs_xml.config** utilise trois types d'objets :

- L'objet **LogFormat** définit le contenu du fichier journal à l'aide de chaînes de format printf-style.
- L'objet **LogFilter** définit un filtre qui vous permet d'inclure ou d'exclure certaines informations dans le fichier journal.
- L'objet **LogObject** définit l'ensemble des informations requises pour produire un fichier journal. Par exemple :
  - Le nom du fichier journal (obligatoire)
  - Le format à utiliser (obligatoire). Il peut s'agir d'un format standard (Squid ou Netscape) ou d'un format personnalisé défini précédemment (un objet **LogFormat** déjà défini).

- Le mode du fichier (ASCII, Binaire ou ASCII_PIPE). Le mode par défaut est ASCII.

  Le mode ASCII_PIPE écrit les entrées du journal dans un canal UNIX nommé (tampon en mémoire). Les autres processus peuvent ensuite lire les données à l'aide des fonctions d'E/S standard. L'avantage de cette option est que Content Gateway n'a pas besoin d'écrire sur le disque, ce qui libère l'espace et la bande passante pour d'autres tâches.

> **Remarque**
> Lorsque la mémoire tampon est pleine, Content Gateway abandonne les entrées du journal et publie un message d'erreur précisant le nombre d'entrées abandonnées. Content Gateway n'écrivant dans le canal que les entrées de journal complètes, seuls les enregistrements complets sont abandonnés.

- Les filtres que vous souhaitez utiliser (objets **LogFilter** définis précédemment)
- Les serveurs de collecte devant recevoir les fichiers journaux
- Les protocoles que vous souhaitez enregistrer (Lorsque la balise des protocoles est utilisée, Content Gateway n'enregistre que les transactions des protocoles répertoriés. Sinon, toutes les transactions sont enregistrées pour tous les protocoles.)
- Les serveurs d'origine que vous souhaitez enregistrer (Si la balise des serveurs est utilisée, Content Gateway n'enregistre que les transactions des serveurs d'origine répertoriés. Sinon les transactions sont enregistrées pour tous les serveurs d'origine.)
- Le texte d'en-tête à insérer dans les fichiers journaux. Ce texte s'affiche au début du fichier journal, juste avant le premier enregistrement.
- Les options de rotation des fichiers journaux

> **Remarque**
> Pour générer un format de journal personnalisé, vous devez spécifier au moins une définition **LogObject**. Un fichier journal est généré pour chaque définition **LogObject**. Pour créer un format de journal personnalisé, vous pouvez utiliser Content Gateway Manager ou modifier un fichier de configuration.

1. Dans **Configurer** > **Subsystems (Sous-systèmes)** > **Logging (Journalisation)** > **Custom (Personnaliser)**, activez l'option **Custom Logging (Journalisation personnalisée)**.
2. Le volet **Custom Log File Definitions (Définitions du fichier journal personnalisé)** affiche le fichier `logs_xml.config`. Ajoutez des spécifications **LogFormat**, **LogFilter** et **LogObject** dans ce fichier de configuration.

   Pour plus d'informations sur le fichier **logs_xml.config** et les spécifications d'objets associées, consultez la section *Fichier de configuration logs_xml.config*, page 364.

3. Cliquez sur **Appliquer**.

Création de fichiers journaux résumés

Content Gateway exécutant plusieurs centaines d'opérations par seconde, les fichiers journaux d'événements peuvent devenir assez volumineux. L'utilisation d'opérateurs de regroupement de type SQL vous permet de configurer Content Gateway de sorte qu'il crée des fichiers journaux résumés récapitulant un ensemble d'entrées du journal sur une période définie. Cette opération permet de réduire la taille des fichiers journaux générés.

Pour générer un fichier journal résumé, créez un objet **LogFormat** dans le fichier de configuration de la journalisation XML (**logs_xml.config**) a l'aide des opérateurs de regroupement de type SQL suivants :

- **COUNT**
- **SUM**
- **AVERAGE**
- **FIRST**
- **LAST**

Vous pouvez appliquer chacun de ces opérateurs à des champs spécifiques, en lui demandant de fonctionner sur l'intervalle défini.

Les fichiers journaux résumés sont un bon compromis entre l'utilité et la granularité des informations. Le fait que vous deviez spécifier l'intervalle au cours duquel seul un unique enregistrement est généré implique que vous pouvez perdre des informations. Lorsque vous voulez que les journaux résumés soient utiles tout en souhaitant le niveau de détail d'un fichier journal traditionnel, pensez à créer et à activer deux formats de journaux personnalisés, l'un avec des opérateurs de regroupement et l'autre sans.

Pour créer un format de fichier journal résumé :

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Logging (Journalisation)** > **Custom (Personnaliser)** pour afficher le fichier **logs_xml.config**.
2. Définissez le format du fichier journal comme suit :

```
<LogFormat>
   <Name = "Résumé"/>
   <Format = "%<opérateur(champ)> : %<opérateur(champ)>"/
   >
   <Interval = "n"/>
</Format>
```

où :

opérateur représente l'un des cinq opérateurs de regroupement (**COUNT**, **SUM**, **AVERAGE**, **FIRST**, **LAST**). Plusieurs opérateurs peuvent être définis dans la ligne du format.

champ représente le champ de journalisation que vous souhaitez regrouper.

n représente l'intervalle (en secondes) séparant les entrées du journal résumé.

Pour plus d'informations, consultez la section *Fichier de configuration logs_xml.config*, page 364.

Le format suivant génère par exemple une entrée toutes les 10 secondes, chaque entrée résumant l'horodatage de la dernière entrée de l'intervalle, le nombre d'entrées détectées au cours de cet intervalle de 10 secondes et la somme de tous les octets envoyés au client :

```
<LogFormat>
   <Name = "Résumé"/>
   <Format = "%<LAST(cqts)> : %<COUNT(*)> :
   %<SUM(psql)>"/>
   <Interval = "10"/>
</Format>
```

Important

Vous ne pouvez pas créer de spécification de format contenant à la fois des opérateurs de regroupement et des champs ordinaires. Par exemple, la spécification suivante ne serait pas valide :

```
<Format = "%<LAST(cqts)> : %<COUNT(*)> :
%<SUM(psql)> : %<cqu>"/>
```

3. Définissez un objet **LogObject** utilisant ce format.
4. Cliquez sur **Appliquer**.

Choix du mode binaire ou ASCII

Vous pouvez configurer Content Gateway pour qu'il crée les fichiers journaux d'événements dans l'un des modes suivants :

- **ASCII** : ces fichiers peuvent être traités à l'aide d'outils d'analyse prêts à l'emploi standard. Content Gateway doit cependant effectuer un traitement supplémentaire pour créer les fichiers au format ASCII, ce qui augmente la charge de travail. Par ailleurs, les fichiers ASCII sont généralement plus volumineux que leurs équivalents binaires. Les fichiers journaux ASCII présentent par défaut une extension de fichier **.log**.
- **Binaire** : ces fichiers réduisent la charge de travail du système et occupent généralement moins d'espace disque, selon le type d'informations enregistrées. Une application de conversion est toutefois nécessaire pour lire ou analyser ces fichiers à l'aide d'outils standard. Les fichiers journaux binaires présentent par défaut une extension de fichier **.blog**.

Si les fichiers journaux binaires occupent généralement moins d'espace disque, ce n'est pas toujours le cas. Par exemple, le stockage de la valeur 0 (zéro) ne demande qu'un octet en ASCII, mais quatre au format binaire. Lorsque vous définissez un format personnalisé enregistrant des adresses IP, un fichier journal binaire ne demande que 4 octets de stockage par adresse de 32 bits. Toutefois, le stockage de cette même adresse IP en notation par points demande environ 15 caractères (octets) dans un fichier journal ASCII.

Pour les formats de journaux standard, vous devez sélectionner le mode **Binaire** ou **ASCII** dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging**

(Journalisation) > Formats de Content Gateway Manager. Voir *Définitions des options de formats de fichiers journaux standard*, page 216. Pour le format de journal personnalisé, vous devez définir le mode ASCII ou Binaire dans l'objet **LogObject**. Reportez-vous à la section *Format personnalisé*, page 216.

Remarque

Dans le cas des fichiers journaux personnalisés, outre les options ASCII et Binaire, vous pouvez également écrire les entrées du journal dans un canal UNIX nommé (tampon en mémoire). Les autres processus peuvent ensuite lire les données à l'aide des fonctions d'E/S standard. L'avantage de cette option est que Content Gateway n'a pas besoin d'écrire sur le disque, ce qui libère l'espace et la bande passante pour d'autres tâches. Par ailleurs, l'écriture dans un canal ne s'interrompt pas lorsque l'espace réservé à la journalisation commence à manquer puisque ce canal n'utilise pas d'espace disque. Pour plus d'informations sur l'option ASCII_PIPE, consultez la section *Fichier de configuration logs_xml.config*, page 364.

Avant de sélectionner le mode ASCII ou binaire pour vos fichiers journaux, tenez compte du type de données à enregistrer. Essayez la journalisation en ASCII pendant une journée, puis en mode binaire le jour suivant. En supposant que le nombre de requêtes soit à peu près identique pour les deux jours, vous pouvez à peu près comparer les deux formats.

Utilisation de l'application logcat pour convertir des journaux binaires en ASCII

Pour pouvoir analyser un fichier journal binaire à l'aide d'outils standard, vous devez d'abord le convertir au format ASCII.

1. Accédez au répertoire contenant le fichier journal binaire.
2. Assurez-vous que l'utilitaire **logcat** soit dans ce répertoire.
3. Entrez la commande suivante :

   ```
   logcat options nomfichier_entrée...
   ```

Le tableau suivant présente les options de ligne de commande.

Option	Description
-o fichier_sortie	Indique où le résultat de la commande est envoyé

-a	Génère automatiquement le nom du fichier de sortie en fonction du nom du fichier d'entrée. Si l'entrée provient de **stdin**, cette option est ignorée.
	Par exemple :
	`logcat -a squid-1.blog squid-2.blog squid-3.blog`
	génère :
	`squid-1.log, squid-2.log, squid-3.log`

-S	Tente de transformer l'entrée au format Squid, si possible
-C	Tente de transformer l'entrée au format Netscape Common, si possible
-E	Tente de transformer l'entrée au format Netscape Extended, si possible
-2	Tente de transformer l'entrée au format Netscape Extended-2, si possible

Remarque
À tout moment, n'utilisez qu'une seule des options suivantes : **-S**, **-C**, **-E** ou **-2**.

Lorsqu'aucun fichier d'entrée n'est défini, l'utilitaire **logcat** lit l'entrée standard (**stdin**). Si vous ne spécifiez pas de fichier de sortie, **logcat** écrit dans la sortie standard (**stdout**).

Par exemple, pour convertir un fichier journal binaire en fichier ASCII, vous pouvez utiliser la commande **logcat** avec l'une des options suivantes :

```
logcat fichier_binaire > fichier_ascii
logcat -o fichier_ascii fichier_binaire
```

Cette commande ne modifie pas le fichier journal binaire.

Rotation des fichiers journaux d'événements

Websense Content Gateway effectue une rotation automatique des fichiers journaux. Cela signifie qu'à intervalle donné, tout au long de la journée, Content Gateway ferme le jeu de fichiers journaux en cours pour en ouvrir de nouveaux.

La rotation des fichiers journaux présente les avantages suivants :

- Elle définit l'intervalle d'analyse des fichiers journaux.
- Elle empêche un même fichier journal de devenir trop volumineux et permet au système de journalisation de ne pas dépasser les limites d'espace définies.

- Elle permet d'identifier facilement les fichiers qui ne sont plus utilisés de sorte qu'un script automatisé puisse ensuite nettoyer le répertoire de journalisation et exécuter les programmes d'analyse.

Il est préférable d'effectuer plusieurs rotations des fichiers journaux par jour. Une rotation toutes les six heures est généralement conseillée.

Format des noms de fichiers journaux ayant subi une rotation

Pour simplifier l'identification des fichiers, Websense Content Gateway donne un format de nom logique aux fichiers journaux qui ont subi une rotation.

Lorsque Content Gateway effectue la rotation d'un fichier journal, il enregistre et ferme l'ancien fichier pour en créer un nouveau. Dans ce cas, Content Gateway renomme l'ancien fichier pour inclure les informations suivantes :

- Le format du fichier (par exemple, **squid.log**)
- Le nom d'hôte du serveur Content Gateway ayant généré ce fichier journal
- Deux horodatages séparés par un tiret (**-**). Le premier horodatage correspond à la limite inférieure de l'horodatage du premier enregistrement dans le fichier journal. La limite inférieure est l'heure à laquelle le nouveau tampon des enregistrements du journal a été créé. Lorsque la charge est faible, le premier horodatage indiqué dans ce nom de fichier peut différer de celui de la première entrée. Lorsque la charge est normale, le premier horodatage du nom de fichier et celui de la première entrée sont identiques.

  Le second horodatage correspond à la limite supérieure de l'horodatage du dernier enregistrement présent dans le fichier journal (il s'agit généralement de l'heure de la rotation)
- Le suffixe **.old**, qui simplifie l'identification des fichiers journaux ayant subi une rotation par les scripts automatisés

Le format des horodatages est le suivant :

```
%A%M%J.%Hh%Mm%Ss-%A%M%J.%Hh%Mm%Ss
```

Le tableau suivant présente ce format :

Code	Définition	Exemple
%A	Année sur quatre chiffres	2000
%M	Mois sur deux chiffres, de 01 à 12	07
%D	Jour sur deux chiffres, de 01 à 31	19
%H	Heure sur deux chiffres, de 00 à 23	21
%M	Minute sur deux chiffres, de 00 à 59	52
%S	Seconde sur deux chiffres, de 00 à 59	36

Voici un exemple de nom de fichier journal ayant subi une rotation :

```
squid.log.monordinateur.20000912.12h00m00s-
20000913.12h00m00s.old
```

Dans cet exemple, le fichier est au format Squid et l'ordinateur hôte est monordinateur. Le premier horodatage désigne la date et l'heure de l'année 2000, le mois de septembre et le jour 12 à 12:00 (midi). Le second horodatage désigne la date et l'heure de l'année 2000, le mois de septembre et le jour 13 à 12:00 (midi). Le fichier se termine par le suffixe .old.

Le système de journalisation place les enregistrements du journal en mémoire tampon avant de les écrire sur le disque. Lors de la rotation d'un fichier journal, la mémoire tampon peut être partiellement remplie. Dans ce cas, l'horodatage de la première entrée du nouveau fichier journal sera antérieure à l'heure de la rotation. Lors de la rotation du nouveau fichier journal, son horodatage sera la limite inférieure de l'horodatage de la première entrée. Supposons par exemple que la rotation des journaux intervienne toutes les trois heures et que le premier fichier journal subissant la rotation soit :

```
squid.log.monordinateur.19980912.12h00m00s-
19980912.03h00m00s.old
```

Si la limite inférieure de la première entrée stockée dans la mémoire tampon à 3:00:00 est 2:59:47, le fichier journal suivant présente l'horodatage suivant lors de sa rotation :

```
squid.log.monordinateur.19980912.02h59m47s-
19980912.06h00m00s.old
```

Le contenu d'un fichier journal est toujours placé entre les deux horodatages. Les entrées des fichiers journaux ne se chevauchent pas, même lorsque les horodatages successifs semblent le faire.

Intervalles de rotation

Les fichiers journaux subissent une rotation à intervalles spécifiques en fonction de l'heure de la journée. Deux options permettent de contrôler la rotation des fichiers journaux :

- L'heure de décalage, qui correspond à une heure comprise entre 0 (minuit) et 23
- L'intervalle de rotation

L'heure de décalage et l'intervalle de rotation déterminent tous deux le début de la rotation des fichiers journaux. La rotation intervient à chaque intervalle défini *et* à l'heure de décalage.

Par exemple, si l'intervalle de rotation est de six heures et l'heure de décalage 0 (minuit), la rotation des journaux intervient à minuit (00:00), 06:00, 12:00 et 18:00 chaque jour. Si l'intervalle de rotation est de 12 heures et l'heure de décalage 3, la rotation des journaux intervient à 03:00 et 15:00 tous les jours.

Définition des options de rotation des fichiers journaux

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Logging (Journalisation) > Général**.
2. Dans la section **Log Rolling (Rotation des journaux)**, vérifiez que l'option **Log Rolling (Rotation des journaux)** est activée (par défaut).
3. Dans le champ **Offset Hour (Heure de décalage)**, entrez l'heure de la journée à laquelle la rotation des fichiers journaux doit survenir. Content Gateway impose chaque jour la rotation des fichiers journaux à l'heure de décalage.

   Vous pouvez entrer n'importe quelle heure de la plage 0 (minuit) à 23.
4. Dans le champ **Intervalle**, entrez le délai pendant lequel Content Gateway écrit les données dans les fichiers journaux avant que la rotation n'intervienne.

La valeur minimale est 300 secondes (cinq minutes). La valeur maximale est 86 400 secondes (un jour).

> **Remarque**
> Si vous démarrez Content Gateway quelques minutes avant la prochaine rotation, celle-ci peut ne pas intervenir avant l'heure de rotation suivante.

5. Vérifiez que l'option **Auto-Delete Rolled Files (Supprimer automatiquement les fichiers après leur rotation)** est activée (par défaut). Cette option entraîne la suppression automatique des fichiers journaux ayant subi une rotation lorsque l'espace disponible commence à manquer dans le répertoire des journaux.

   La suppression automatique commence lorsque la quantité d'espace disponible dans le répertoire de journalisation est inférieure à la marge définie.
6. Cliquez sur **Appliquer**.

> **Remarque**
> Vous pouvez ajuster les paramètres de rotation d'un fichier journal personnalisé dans la spécification **LogObject** du fichier **logs_xml.config**. Le fichier journal personnalisé utilise les paramètres de rotation de sa spécification **LogObject**, en ignorant les paramètres par défaut définis dans Content Gateway Manager ou dans le fichier **records.config** décrit ci-dessus.

Division des fichiers journaux d'événements

Par défaut, Websense Content Gateway utilise les formats de journaux standard et génère les fichiers journaux contenant des transactions HTTP et FTP dans le même fichier. Vous pouvez toutefois activer la division des journaux par hôte si vous préférez enregistrer les transactions des différents serveurs d'origine dans des fichiers journaux distincts.

Division des journaux des hôtes HTTP

La division des journaux des hôtes HTTP vous permet d'enregistrer les transactions HTTP et FTP des différents serveurs d'origine dans des fichiers journaux distincts. Lorsque la division des journaux des hôtes HTTP est activée, Content Gateway crée un fichier journal distinct pour chaque serveur d'origine répertorié dans le fichier **log_hosts.config** (voir *Modification du fichier log_hosts.config*, page 225).

Lorsque la division des journaux des hôtes HTTP est activée, Content Gateway génère des fichiers journaux distincts pour les transactions HTTP/FTP, en fonction du serveur d'origine.

Par exemple, si le fichier **log_hosts.config** contient les serveurs d'origine **uni.edu** et **entreprise.com** et que le format Squid est activé, Content Gateway génère les fichiers journaux suivants :

Nom du fichier journal	Description
`squid-uni.edu.log`	Toutes les transactions HTTP et FTP du serveur **uni.edu**
`squid-entreprise.com.log`	Toutes les transactions HTTP et FTP du serveur **entreprise.com**
`squid.log`	Toutes les transactions HTTP et FTP des autres hôtes

Content Gateway vous autorise également à créer des formats de journaux personnalisés de type XML qui vous permettent de contrôler encore davantage la génération des fichiers journaux en fonction du protocole et du nom d'hôte. Voir *Format personnalisé*, page 216.

Définition des options de division des journaux

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Logging (Journalisation) > Splitting (Division)**.
2. Activez l'option **Split Host Logs (Diviser les journaux par hôte)** pour enregistrer toutes les transactions HTTP et FTP de chaque serveur d'origine répertorié dans le fichier **log_hosts.config** dans un fichier journal distinct. Désactivez l'option **Split Host Logs (Diviser les journaux par hôte)** pour enregistrer toutes les transactions HTTP et FTP de chaque serveur d'origine répertorié dans le fichier **log_hosts.config** dans le même fichier journal.
3. Cliquez sur **Appliquer**.

Modification du fichier log_hosts.config

Le fichier **log_hosts.config** par défaut est stocké dans **/opt/WCG/config**. Pour enregistrer les transactions HTTP et FTP des différents serveurs d'origine dans des fichiers journaux distincts, vous devez spécifier le nom d'hôte de chaque serveur d'origine dans une ligne distincte de ce fichier.

> **Remarque**
> Vous pouvez spécifier des mots-clés dans le fichier **log_hosts.config** afin d'enregistrer dans un fichier journal distinct l'ensemble des transactions des serveurs d'origine dont le nom contient les mots-clés définis. Par exemple, si vous spécifiez le mot-clé **sports**, Content Gateway enregistre toutes les transactions HTTP et FTP provenant des serveurs **sports.yahoo.com** et **www.foxsports.com** dans un fichier journal appelé **squid-sports.log** (si le format Squid est activé).

> **Remarque**
> Lorsque Content Gateway est dans un cluster et que vous activez la collecte des fichiers journaux, il est préférable d'utiliser le même fichier **log_hosts.config** dans chaque nœud du cluster.

1. Ouvrez le fichier **log_hosts.config** stocké dans le répertoire **/opt/WCG/config**.
2. Entrez le nom de chaque serveur d'origine sur une ligne distincte du fichier. Par exemple :

   ```
   serveurweb1
   serveurweb2
   serveurweb3
   ```

3. Enregistrez et fermez le fichier.
4. Pour appliquer vos modifications, exécutez la commande suivante dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) :

   ```
   ./content_line -x
   ```

Collecte des fichiers journaux d'événements

Vous pouvez utiliser la fonction de collecte des fichiers journaux pour stocker toutes les informations enregistrées en un même emplacement. Vous pouvez alors analyser Content Gateway dans son intégralité et non pas par nœud individuel et utiliser un disque volumineux uniquement situé dans l'un des nœuds du cluster.

Content Gateway collecte des fichiers journaux en définissant un ou plusieurs nœuds en tant que serveurs de collecte et tous les nœuds restants en tant que clients de la collecte. Lorsqu'un nœud génère une mémoire tampon d'entrées de journaux d'événements, il détermine s'il s'agit du serveur de collecte ou d'un client de collecte. Le nœud du serveur de collecte se contente d'écrire l'intégralité des journaux dans la mémoire tampon de son disque local, de la même façon que si la collecte des journaux n'était pas activée.

Les nœuds des clients de collecte préparent le transfert de leurs tampons de journaux via le réseau et les envoient au serveur de collecte. Lorsque le serveur de collecte reçoit la mémoire tampon des journaux d'un client, il l'écrit dans son propre fichier journal comme si ces entrées avaient été générées localement. Lorsque les clients de journaux ne peuvent pas contacter leur serveur de collecte, ils écrivent le contenu de leur mémoire tampon dans leurs disques locaux, au sein de fichiers journaux *orphelins*. Les fichiers journaux orphelins doivent être collectés manuellement.

Les serveurs de collecte des journaux peuvent être autonomes ou faire partie d'un nœud exécutant Content Gateway.

> **Remarque**
> La collecte des journaux peut avoir un impact sur les performances du réseau. Tous les nœuds transmettant les données de leur mémoire tampon à un même serveur de collecte, le réseau peut alors être engorgé lorsque le volume envoyé à même un nœud du réseau dépasse les capacités de traitement de ce dernier.

> **Remarque**
> Chaque entrée des fichiers journaux collectés contient des informations d'horodatage, mais ces entrées ne s'affichent pas par ordre chronologique strict dans les fichiers. Vous pouvez donc classer les fichiers journaux collectés avant de commencer les analyses.

Configuration de Content Gateway en tant que serveur de collecte

1. Sélectionnez **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Collation (Collecte)**.
2. Dans la section **Collation Mode (Mode de collecte)**, activez l'option **Be A Collation Server (CG en tant que serveur de collecte)**.
3. Dans le champ **Log Collation Port (Port de collecte des journaux)**, entrez le numéro du port utilisé pour la communication avec les clients de collecte. Le numéro de port par défaut est le 8085.
4. Dans le champ **Log Collation Secret (Mot de passe de collecte des journaux)**, saisissez le mot de passe utilisé pour valider les données de la journalisation et empêcher tout échange d'informations aléatoires.

   > **Remarque**
   > Tous les clients de collecte doivent utiliser ce même mot de passe.

5. Cliquez sur **Appliquer**.

   > **Important**
   > Si vous modifiez le port ou le mot de passe de collecte après l'établissement des connexions reliant le serveur et les clients de collecte, vous devrez redémarrer Content Gateway.

Configuration de Content Gateway en tant que client de collecte

1. Sélectionnez **Configurer** > **Subsystems (Sous-systèmes)** > **Logging (Journalisation) > Collation (Collecte)**.
2. Dans la section **Collation Mode (Mode de collecte)**, activez l'option **Be a Collation Client (CG en tant que client de collecte)** pour définir le nœud Content Gateway en tant que client de collecte et envoyer les entrées de journaux au format standard actif (tel que Squid ou Netscape) au serveur de collecte des journaux.

> **Remarque**
> Pour envoyer les entrées de journaux au serveur de collecte au format XML, vous devez ajouter une spécification d'objet de journal dans le fichier **logs_xml.config**. Voir *Format personnalisé*, page 216.

3. Dans le champ **To Collation Server (Au serveur de collecte)**, entrez le nom d'hôte du serveur de collecte. Il peut s'agir du serveur de collecte Content Gateway ou d'un serveur de collecte autonome.
4. Dans le champ **Log Collation Port (Port de collecte des journaux)**, entrez le numéro du port utilisé pour la communication avec le serveur de collecte. Le numéro de port par défaut est le 8085.
5. Dans le champ **Log Collation Secret (Mot de passe de collecte des journaux)**, saisissez le mot de passe utilisé pour valider les données de la journalisation et empêcher tout échange d'informations aléatoires. Ce mot de passe doit être identique à celui que vous avez défini dans le serveur de collecte.
6. Activez l'option **Log Collation Host Tagged (Collecte des journaux d'hôtes balisés)** si vous souhaitez conserver les entrées d'origine des journaux dans les fichiers collectés.
7. Dans le champ **Log Collation Orphan Space (Espace de stockage des fichiers journaux orphelins)**, entrez la quantité maximale d'espace (en méga-octets) à allouer au répertoire de journalisation pour le stockage des fichiers journaux orphelins dans le client de collecte. (Ces fichiers journaux orphelins sont créés lorsque le serveur de collecte n'est pas accessible.) La valeur par défaut est 25 Mo.
8. Cliquez sur **Appliquer**.

> **Important**
> Si vous modifiez le port ou le mot de passe de collecte après l'établissement des connexions reliant les clients de collecte au serveur de collecte, vous devrez redémarrer Content Gateway.

Utilisation d'un collecteur autonome

Lorsque vous ne voulez pas que le serveur de collecte des journaux soit un nœud Content Gateway, vous pouvez installer et configurer un collecteur autonome (SAC) capable de dédier davantage de puissance à la collecte, au traitement et à l'écriture des fichiers journaux.

> **Remarque**
> Le collecteur autonome n'est pour l'instant disponible que pour la plateforme Linux.

1. Configurez vos nœuds Content Gateway en tant que clients de collecte de journaux. Voir *Configuration de Content Gateway en tant que client de collecte*, page 228.
2. Copiez le fichier binaire **sac** situé dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) dans l'ordinateur désigné comme collecteur autonome.
3. Créez un répertoire **config** dans le répertoire qui contient le fichier binaire **sac**.
4. Créez un répertoire nommé **internal** dans le répertoire **config** que vous avez créé à l'Etape 3. Le collecteur autonome utilisera ce répertoire en interne pour stocker les fichiers journaux.
5. Dans le collecteur autonome, copiez le fichier **records.config** (**/opt/WCG/config**) d'un nœud Content Gateway configuré en tant que client de collecte des journaux dans le répertoire **config** que vous avez créé à l'Etape 3.

   Le fichier **records.config** contient le mot de passe et le port de collecte des journaux que vous avez définis lors de la configuration des nœuds en tant que clients de collecte. Le mot de passe et le port de collecte doivent être identiques pour tous les clients et serveurs de collecte.
6. Dans le collecteur autonome, ouvrez le fichier **records.config** et modifiez la variable suivante :

Variable	Description
proxy.config.log2.logfile_dir	Spécifiez le répertoire dans lequel vous souhaitez stocker les fichiers journaux. Vous pouvez spécifier un chemin absolu ou relatif conduisant au répertoire à partir duquel le fichier binaire **sac** doit être exécuté. Remarque : ce répertoire doit déjà exister dans l'ordinateur désigné comme collecteur autonome.

7. Enregistrez et fermez le fichier.
8. Entrez la commande suivante :

```
sac -c config
```

Affichage des statistiques de journalisation

Les statistiques générées par Content Gateway sur le système de journalisation simplifient l'affichage des informations suivantes :

- Nombre de fichiers journaux (formats) en cours d'écriture
- Volume d'espace actuellement utilisé par le répertoire de journalisation, contenant la totalité des journaux d'événements et d'erreurs
- Nombre d'événements d'accès écrits dans les fichiers journaux depuis l'installation de Content Gateway. Ce nombre correspond à une entrée dans un fichier. Lorsque plusieurs formats sont écrits, un même événement génère plusieurs entrées dans les journaux d'événements
- Nombre d'événements d'accès ignorés (à cause du filtrage) depuis l'installation de Content Gateway
- Nombre d'événements d'accès écrits dans le journal des erreurs depuis l'installation de Content Gateway

Vous pouvez afficher ces statistiques dans l'onglet Monitor (Surveiller) de Content Gateway Manager ou les récupérer via l'interface de ligne de commande. Voir *Surveillance du trafic*, page 109.

Affichage des fichiers journaux

Rubriques connexes :

- *Format Squid*, page 232
- *Exemples Netscape*, page 233

Dans Content Gateway Manager, vous pouvez afficher les fichiers journaux système, d'événements et d'erreurs créés par Content Gateway. Vous pouvez afficher un fichier journal dans son intégralité, un nombre donné de lignes récentes du fichier journal ou toutes les lignes contenant une chaîne définie.

Vous pouvez également supprimer un fichier journal ou le copier dans votre système local.

Remarque

Pour copier et supprimer des fichiers journaux, vous devez disposer des autorisations d'utilisateur appropriées.

Remarque

Content Gateway affiche uniquement le premier 1 Mo de données du fichier journal. Lorsque la taille du fichier sélectionné dépasse 1 Mo, Content Gateway tronque le fichier et affiche un avertissement qui précise qu'il est trop volumineux.

Vous pouvez à présent accéder aux fichiers journaux via Content Gateway Manager.

1. Sélectionnez **Configurer** > **Mon proxy > Logs (Journaux) > System (Système)**.
2. Pour afficher, copier ou supprimer un fichier journal système, passez à l'Etape 3.

   Pour afficher, copier ou supprimer un fichier journal d'événements ou d'erreurs, ouvrez l'onglet **Access (Accès)**.
3. Dans la liste déroulante **Log File (Fichier journal)**, sélectionnez le fichier journal à afficher, copier ou supprimer.

   Content Gateway répertorie les fichiers journaux système enregistrés via le mécanisme de journalisation à l'échelle du système **syslog** dans l'utilitaire du démon.

   Content Gateway répertorie les fichiers journaux d'événements situés dans le répertoire défini dans le champ **Logging Directory (Répertoire de journalisation)** de l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Général** ou par la variable de configuration **proxy.config.log2.logfile_dir** du fichier **records.config**. Par défaut, il s'agit du répertoire **logs** situé dans le répertoire d'installation de Content Gateway.
4. Dans le volet **Action**, sélectionnez l'une des options suivantes :
   - **Display the selected log file (Afficher le fichier journal sélectionné)** pour afficher le fichier journal dans son intégralité. Si la taille du fichier dépasse 1 Mo, seul le premier méga de données s'affiche.
   - **Display last lines of the selected file (Afficher les dernières lignes du fichier sélectionné)** pour afficher les dernières lignes du fichier journal. Saisissez le nombre de lignes à afficher dans le champ fourni.
   - **Display lines that match in the selected log file (Afficher les lignes correspondantes du fichier journal sélectionné)** pour afficher toutes les lignes du fichier journal correspondant à une chaîne donnée. Entrez la chaîne désirée dans le champ fourni.
   - **Remove the selected log file (Supprimer le fichier journal sélectionné)** pour supprimer le fichier journal sélectionné du système Content Gateway.
   - **Save the selected log file in local filesystem (Enregistrer le fichier journal sélectionné dans le système de fichiers local)** pour enregistrer une copie du fichier journal sélectionné dans votre système local.
5. Cliquez sur **Appliquer**.

   Lorsque vous choisissez d'afficher le fichier journal, Content Gateway l'affiche à la fin de la page.

   Lorsque vous choisissez de supprimer le fichier journal, Content Gateway supprime le fichier. Vous n'êtes pas invité à confirmer la suppression.

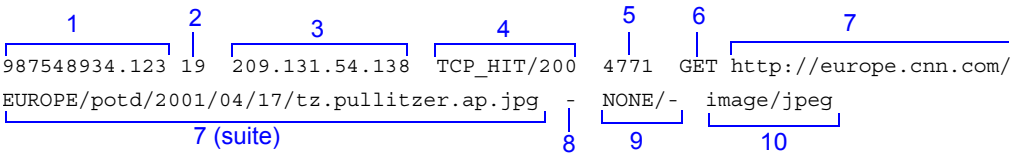
   Lorsque vous choisissez d'enregistrer le fichier journal, vous êtes invité à saisir l'emplacement dans lequel vous souhaitez l'enregistrer dans votre système local.

Exemple d'entrées de fichier journal d'événements

Cette section présente des exemples d'entrée de fichier journal pour chaque format de journal standard pris en charge par Content Gateway :

Format Squid

La figure suivante présente un exemple d'entrée de journal dans un fichier **squid.log**. Les différents champs sont décrits dans le tableau suivant.

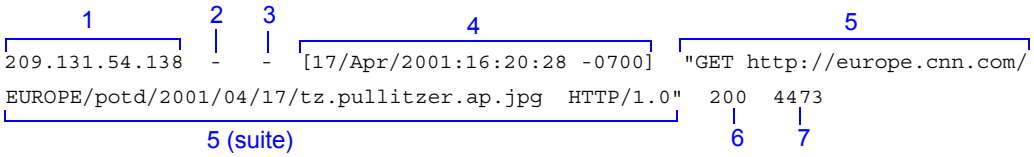


Champ	Description
1	Horodatage de la requête du client au format Squid ; heure de la requête du client en secondes à compter du 1er janvier 1970 UTC (avec une résolution en millisecondes)
2	Temps consacré par le proxy au traitement de la requête du client ; nombre de millisecondes écoulé entre le moment où le client a établi la connexion au proxy et le moment où le proxy lui a renvoyé le dernier octet de la réponse
3	Adresse IP de l'ordinateur hôte du client
4	Code de résultat du cache ; mode de réponse du cache à la requête : accès fructueux (HIT), accès infructueux (MISS), etc. Les différents codes de résultat du cache sont décrits à la section *Dans les fichiers journaux au format Squid ou Netscape, que signifient les codes de résultat du cache ?*, page 467. Code d'état de la réponse du proxy (code d'état de la réponse HTTP envoyée par Content Gateway au client)
5	Longueur de la réponse envoyée par Content Gateway au client en octets, en-têtes et contenu compris
6	Méthode de la requête du client : GET, POST, etc.
7	URL canonique (CNAME) de la requête du client ; les espaces et autres caractères susceptibles de ne pas être analysés par les outils des journaux sont remplacés par des séquences d'échappement. La séquence d'échappement est un symbole de pourcentage suivi par le code ASCII (en hexadécimal) du caractère remplacé.
8	Nom d'utilisateur du client authentifié. Un tiret (-) indique qu'aucune authentification n'était requise.
9	Itinéraire hiérarchique du proxy ; itinéraire suivi par Content Gateway pour récupérer l'objet. Nom du serveur de la requête envoyée au proxy ; nom du serveur qui a satisfait la requête. Si la requête correspondait à un accès fructueux au cache, ce champ contient un tiret (-).
10	Type de contenu de la réponse du proxy ; type de contenu de l'objet récupéré dans l'en-tête de la réponse de Content Gateway

Exemples Netscape

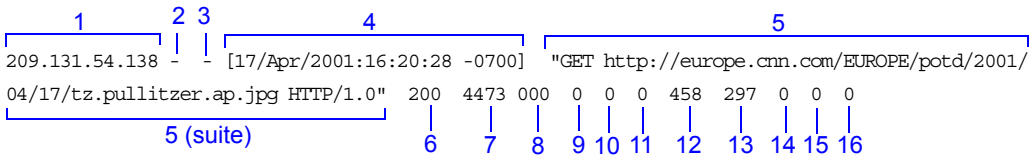
Format Netscape Common

La figure suivante présente un exemple d'entrée de journal dans un fichier **common.log**. Les différents champs sont décrits dans le tableau suivant.



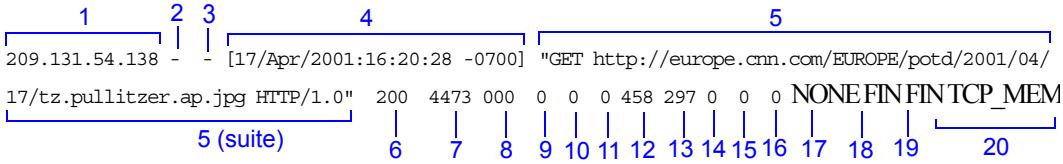
Format Netscape Extended

La figure suivante présente un exemple d'entrée de journal dans un fichier **extended.log**. Les différents champs sont décrits dans le tableau suivant.



Format Netscape Extended-2

La figure suivante présente un exemple d'entrée de journal dans un fichier **extended2.log**. Les différents champs sont décrits dans le tableau suivant.



Champ	Description
	Netscape Common
1	Adresse IP de l'ordinateur hôte du client
2	Ce tiret (-) est toujours présent dans les entrées de journal Netscape.
3	Nom d'utilisateur du client authentifié. Un tiret (-) indique qu'aucune authentification n'était requise.
4	Date et heure de la requête du client, entre crochets
5	Ligne de la requête, entre guillemets

Champ	Description
6	Code d'état de la réponse du proxy (code de la réponse HTTP)
7	Longueur de la réponse envoyée par Content Gateway au client (en octets)
	Netscape Extended
8	Code d'état de la réponse du serveur d'origine
9	Longueur du transfert de la réponse du serveur ; taille du corps de la réponse du serveur d'origine envoyée au proxy, en octets
10	Longueur du transfert de la requête du client ; taille du corps de la requête envoyée au proxy, en octets
11	Longueur du transfert de la requête du proxy ; taille du corps de la requête du proxy envoyée au serveur d'origine
12	Longueur de l'en-tête de la requête du client ; taille de l'en-tête de la requête envoyée au proxy
13	Longueur de l'en-tête de la réponse envoyée au proxy ; longueur de l'en-tête de la réponse du proxy envoyée au client
14	Longueur de l'en-tête de la requête du proxy ; longueur de l'en-tête de la requête du proxy envoyée au serveur d'origine
15	Longueur de l'en-tête de la réponse du serveur ; longueur de l'en-tête de la réponse du serveur d'origine envoyée au proxy
16	Temps consacré par Content Gateway au traitement de la requête du client ; nombre de secondes écoulé entre le moment où le client établit la connexion au proxy et le moment où ce dernier lui renvoie le dernier octet de la réponse
	Netscape Extended-2
17	Itinéraire hiérarchique du proxy ; itinéraire suivi par Content Gateway pour récupérer l'objet
18	Code d'état de finalité du client : FIN si la demande du client envoyée au proxy a été entièrement satisfaite ou INTR si elle a été interrompue.
19	Code d'état de finalité du proxy : FIN si la demande envoyée au proxy par Content Gateway a été entièrement satisfaite ou INTR si elle a été interrompue.
20	Code de résultat du cache ; mode de réponse du cache Content Gateway à la requête : accès fructueux (HIT), accès infructueux (MISS), etc. Les différents codes de résultat du cache sont décrits à la section *Dans les fichiers journaux au format Squid ou Netscape, que signifient les codes de résultat du cache ?*, page 467.

A Statistiques

Cette annexe décrit les statistiques disponibles dans l'onglet Monitor (Surveiller) de Content Gateway Manager :

Mon proxy

Les statistiques de Mon proxy sont réparties dans les catégories suivantes :

Résumé

Statistique/Champ	Description
	Détails de l'abonnement
Feature (Fonction)	Liste des fonctions acquises, telles que SSL Manager, et les options d'analyse. Pour plus d'informations sur SSL Manager, consultez la section *Utilisation des données cryptées*, page 129 et la section *Analyse du contenu à l'aide des options d'analyse* de l'Aide en ligne de TRITON - Web Security.
Purchased Status (État d'acquisition)	Indique si une fonction a été achetée ou non
Date d'expiration	Lorsqu'une fonction a été achetée, présente la date d'expiration de l'abonnement

Statistique/Champ	Description
	More Detail (Autres détails)
Clé d'abonnement	Présente la clé de votre abonnement. Voir *Saisie de votre clé d'abonnement*, page 14.
Last successful subscription download time (Heure du dernier téléchargement d'abonnement réussi)	Présente l'heure de la dernière validation réussie de votre clé d'abonnement. Cette vérification a lieu une fois par jour.
Connection status (État de la connexion)	Indique l'état de la connexion de Content Gateway à Policy Server, Policy Broker et Filtering Service
Registration status (État de l'enregistrement)	Indique l'état de l'enregistrement de Content Gateway auprès du référentiel d'analyses (Forensics Repository)
	Analyse des fichiers de données
Engine Name (Nom du moteur)	Présente le nom de chaque moteur d'analyse
Engine Version (Version du moteur)	Présente le numéro de version du moteur d'analyse
Data File Version (Version du fichier de données)	Présente le numéro de version du fichier de données actuellement utilisé par le moteur d'analyse
Content Classification Analytics library version (Version de la bibliothèque d'analyses de classification du contenu)	Présente le numéro de version de la bibliothèque d'analyses de classification du contenu
Last update (Dernière mise à jour)	Présente l'heure et la date auxquelles Content Gateway a réussi à charger les fichiers de données, les paramètres et les stratégies d'analyse
Last time Content Gateway loaded data (Dernier chargement des données par Content Gateway)	Présente l'heure et la date auxquelles Content Gateway a réussi à charger les bases de données, les paramètres et les stratégies
Last time Content Gateway checked for updates (Dernière vérification des mises à jour par Content Gateway)	Présente l'heure et la date auxquelles Content Gateway a réussi à communiquer avec le serveur de téléchargement Websense pour la dernière fois afin de vérifier la présence de mises à jour des fichiers de données
	Détails du nœud
Node (Nœud)	Nom du nœud ou du cluster Content Gateway
On/Off (Activé/ Désactivé)	Indique si le proxy est en cours d'exécution (le proxy et les services Manager s'exécutent)
Objects Served (Objets desservis)	Nombre total d'objets desservis par le nœud Content Gateway

Statistique/Champ	Description
Ops/Sec	Nombre d'opérations traitées par seconde par le nœud Content Gateway
Hit Rate (Taux d'accès)	Pourcentage de requêtes HTTP desservies à partir du cache, calculé en moyenne sur les 10 dernières secondes
Throughput (Mbit/sec) (Débit (en Mbits/sec))	Nombre de mégabits transmis par seconde via le nœud Content Gateway (et le cluster)
HTTP Hit (ms) (Accès HTTP fructueux au cache)	Délai nécessaire pour envoyer un objet HTTP récent du cache au client
HTTP Miss (ms) (Accès HTTP infructueux au cache)	Délai nécessaire pour envoyer au client un objet HTTP non présent dans le cache ou présent dans le cache mais périmé
SSL Manager Configuration Server (Serveur de configuration de SSL Manager)	Lorsque plusieurs nœuds Content Gateway sont déployés dans un cluster et que la mise en cluster de la gestion SSL est activée, ce champ présente l'adresse IP du serveur de configuration de SSL Manager. Lorsque l'adresse correspond à un lien, le système en cours n'est **pas** le serveur. Cliquez sur ce lien pour vous connecter au Serveur de configuration de SSL Manager.
	Autres détails
cache hit rate (taux d'accès fructueux au cache)	Pourcentage de requêtes HTTP desservies à partir du cache, calculé en moyenne sur les 10 dernières secondes. Cette valeur est actualisée toutes les 10 secondes.
errors (erreurs)	Pourcentage de requêtes se terminant par une interruption précoce
aborts (abandons)	Pourcentage de requêtes abandonnées
active clients (clients actifs)	Nombre actuel de connexions de clients ouvertes
active servers (serveurs actifs)	Nombre actuel de connexions de serveurs d'origine ouvertes
node IP address (adresse IP du nœud)	Adresse IP attribuée au nœud. Lorsque l'adressage IP virtuel est activé, plusieurs adresses IP virtuelles peuvent être affectées à ce nœud.
cache free space (espace disponible dans le cache)	Volume d'espace disponible dans le cache
HostDB hit rate (taux d'accès à la base de données des hôtes)	Rapport d'accès fructueux à la base de données des hôtes par rapport au nombre total de recherches effectuées dans cette base de données, calculé en moyenne sur une période de 10 secondes

Nœud

Statistique	Description
	Résumé du nœud
Statut (État)	Indique si Content Gateway s'exécute sur ce nœud (actif ou inactif)
Up Since (Actif depuis)	Date et heure de démarrage de Content Gateway

Statistique	Description
Clustering (Mise en cluster)	Indique si la mise en cluster est activée ou non dans ce nœud
	Cache
Document Hit Rate (Taux d'accès fructueux aux documents)	Accès fructueux au cache par rapport au nombre total de requêtes, calculé en moyenne sur une période de 10 secondes. Cette valeur est actualisée toutes les 10 secondes.
Bandwidth Savings (Économies de bande passante)	Ratio d'octets desservis à partir du cache par rapport au nombre total d'octets demandés, calculé en moyenne sur une période de 10 secondes. Cette valeur est actualisée toutes les 10 secondes.
Cache Percent Free (Pourcentage de cache disponible)	Ratio d'espace disponible dans le cache par rapport à l'espace total du cache
	En cours
Open Server Connections (Connexions de serveurs ouvertes)	Nombre de connexions de serveurs d'origine actuellement ouvertes
Open Client Connections (Connexions de clients ouvertes)	Nombre de connexions de clients actuellement ouvertes
Cache Transfers in Progress (Nombre de transferts du cache en cours)	Nombre de transferts du cache (lectures et écritures dans le cache) en cours
	Réseau
Client Throughput (Mbit/Sec) (Débit du client (en Mbits/sec))	Nombre de mégabits transmis par seconde via le nœud (et le cluster)
Transactions per Second (Transactions par seconde)	Nombre de transactions HTTP par seconde
	Résolution de noms
Host Database Hit Rate (Taux d'accès fructueux à la base de données des hôtes)	Rapport d'accès fructueux à la base de données des hôtes par rapport au nombre total de recherches effectuées dans cette base de données, calculé en moyenne sur une période de 10 secondes. Cette valeur est actualisée toutes les 10 secondes.
DNS Lookups per Second (Recherches DNS par seconde)	Nombre de recherches DNS par seconde

Graphiques

La page Graphs (Graphiques) présente les mêmes statistiques que celles répertoriées dans la page *Nœud* (performances du cache, connexions et transfert en cours, réseau et résolution de noms), mais sous forme de graphiques. Vous pouvez choisir les statistiques à inclure dans un graphique. Voir *Affichage des statistiques*, page 109.

Alarmes

Websense Content Gateway émet une alarme lorsqu'il détecte un problème (par exemple lorsque l'espace affecté aux journaux d'événements devient insuffisant ou lorsqu'il ne parvient pas à écrire dans un fichier de configuration) et décrit cette alarme dans la fenêtre des messages d'alarme. La barre **Alarm! [pending] (Alarme ! [en attente])** située en haut de l'écran Content Gateway Manager signale par ailleurs que des alarmes ont été détectées et combien.

Lorsque vous avez lu le message d'une alarme, cliquez sur **Effacer** dans la fenêtre du message pour la faire disparaître. L'option **Effacer** fait uniquement disparaître les messages d'alarme et n'en résout pas les causes.

Pour plus d'informations sur l'utilisation des alarmes, consultez la section *Utilisation des alarmes*, page 113.

Protocoles

Les statistiques concernant les protocoles sont réparties dans les catégories suivantes :

HTTP

Statistique	Description
	Général
Client	
Total Document Bytes (Total des octets de documents)	Volume total de données HTTP envoyées aux clients depuis l'installation
Total Header Bytes (Nombre total d'octets d'en-tête)	Volume total de données d'en-tête HTTP envoyées aux clients depuis l'installation
Total Connections (Nombre total de connexions)	Nombre total de connexions de clients HTTP depuis l'installation
Current Connections (Connexions en cours)	Nombre de connexions de clients HTTP actuellement ouvertes
Transactions in Progress (Nombre de transactions en cours)	Nombre total de transactions de clients HTTP en cours

Statistique	Description
Serveur	
Total Document Bytes (Total des octets de documents)	Volume total de données HTTP envoyées par les serveurs d'origine depuis l'installation
Total Header Bytes (Nombre total d'octets d'en-tête)	Volume total de données d'en-tête HTTP envoyées par les serveurs d'origine depuis l'installation
Total Connections (Nombre total de connexions)	Nombre total de connexions de serveurs HTTP depuis l'installation
Current Connections (Connexions en cours)	Nombre de connexions de serveurs HTTP actuellement ouvertes
Transactions in Progress (Nombre de transactions en cours)	Nombre total de connexions de serveurs HTTP actuellement en cours
	Transaction
Accès fructueux au cache	
Fresh (Récents)	Pourcentage d'accès fructueux au cache considérés comme récents, et durée moyenne des transactions
Stale Revalidated (Éléments périmés revalidés)	Pourcentage d'accès fructueux au cache considérés comme périmés et revalidés s'étant révélés comme récents et ayant été desservis, et durée moyenne des transactions
Accès infructueux au cache	
Now Cached (À présent mis en cache)	Pourcentage de demandes de documents non présents dans le cache (mais qui y sont désormais) et durée moyenne des transactions
Server No Cache (En-têtes de serveur no-cache)	Pourcentage de demandes d'objets HTTP non présents dans le cache, associés à des en-têtes de serveur no-cache (ne pouvant pas être mis en cache) et durée moyenne des transactions
Stale Reloaded (Rechargement d'éléments périmés)	Pourcentage d'accès infructueux revalidés s'étant révélés comme ayant été modifiés, rechargés et desservis et durée moyenne des transactions
Client No Cache (En-têtes de client no-cache)	Pourcentage d'accès infructueux associés à des en-têtes de client no-cache et durée moyenne des transactions
Erreurs	
Connection Failures (Échecs de connexion)	Pourcentage d'erreurs de connexion et durée moyenne des transactions
Other Errors (Autres erreurs)	Pourcentage d'autres erreurs de connexion et durée moyenne des transactions

Statistique	Description
Transactions abandonnées	
Client Aborts (Abandons de clients)	Pourcentage de transactions abandonnées par les clients et durée moyenne des transactions
Questionable Client Aborts (Abandons de clients contestables)	Pourcentage de transactions ayant pu être abandonnées par le client et durée moyenne des transactions
Partial Request Hangups (Interruptions de requêtes partielles)	Pourcentage d'interruptions précoces (faisant suite à des demandes partielles) et durée moyenne des transactions
Pre-Request Hangups (Interruptions avant requêtes)	Pourcentage de transactions interrompues avant la requête et durée moyenne des transactions
Pre-Connect Hangups (Interruptions avant connexion)	Pourcentage de transactions interrompues avant la connexion et durée moyenne des transactions
Autres transactions	
Unclassified (Non classées)	Pourcentage de transactions non classées et durée moyenne des transactions
	FTP sur HTTP
Connexions	
Open Server Connections (Connexions de serveurs ouvertes)	Nombre de connexions ouvertes sur le serveur FTP
Successful PASV Connections (Nombre de connexions PASV réussies)	Nombre de connexions PASV réussies depuis l'installation
Failed PASV Connections (Nombre d'échecs de connexions PASV)	Nombre d'échecs de connexions PASV depuis l'installation
Successful PORT Connections (Nombre de connexions réussies au port)	Nombre de connexions réussies au port depuis l'installation
Failed PORT Connections (Nombre d'échecs de connexions au port)	Nombre d'échecs de connexions au port depuis l'installation
Statistiques du cache	
Accès fructueux au cache	Nombre de demandes HTTP d'objets FTP desservis à partir du cache
Accès infructueux au cache	Nombre de demandes HTTP d'objets FTP directement transmises au serveur d'origine du fait de l'absence de l'objet dans le cache ou de son état périmé
Lookups (Recherches)	Nombre de fois où Content Gateway a recherché un objet FTP dans le cache pour une requête HTTP

FTP

Statistique	Description
	Client
Open Connections (Connexions ouvertes)	Nombre de connexions de clients actuellement ouvertes
Bytes Read (Nombre d'octets lus)	Nombre d'octets de requêtes de clients lus depuis l'installation
Bytes Written (Nombre d'octets écrits)	Nombre d'octets de requêtes de clients écrits depuis l'installation
	Serveur
Open Connections (Connexions ouvertes)	Nombre de connexions de serveurs FTP actuellement ouvertes
Bytes Read (Nombre d'octets lus)	Nombre d'octets lus à partir des serveurs FTP depuis l'installation
Bytes Written (Nombre d'octets écrits)	Nombre d'octets écrits dans le cache depuis l'installation

Sécurité

Les statistiques concernant la sécurité sont réparties dans les catégories suivantes :

- *Authentification Windows intégrée*, page 243
- *LDAP*, page 245
- *Authentification NTLM héritée*, page 245
- *SOCKS*, page 246
- *Sécurité des données*, page 246

> **Remarque**
> Même lorsque des règles d'authentification dans plusieurs domaines Kerberos sont utilisées, Content Gateway génère en toute discrétion des statistiques d'authentification pour chaque méthode d'authentification (IWA, LDAP, NTLM héritée).

Authentification Windows intégrée

Statistique	Description
	Test de diagnostic Cette fonction exécute des tests de diagnostic sur la connexion Kerberos au domaine sélectionné. Les résultats s'affichent à l'écran et sont consignés dans les fichiers /opt/WCG/logs/content_gateway.out et / opt/WCG/logs/smbadmin.log.
Champ déroulant Domaine	Sélectionnez un domaine joint. À moins que l'authentification dans plusieurs domaines Kerberos ne soit configurée, il n'y a qu'un seul domaine joint.
Bouton Run Test (Exécuter un test)	Cliquez sur ce bouton pour démarrer le test.
	Nombre de requêtes Kerberos
Total Kerberos requests (Nombre total de requêtes Kerberos)	Nombre total de requêtes d'authentification Kerberos
Authentication succeeded (Authentification réussie)	Nombre de requêtes d'authentification Kerberos ayant entraîné une authentification réussie
Authentication failed (Échecs d'authentification)	Nombre de requêtes d'authentification Kerberos ayant entraîné un échec d'authentification
Kerberos errors (Erreurs Kerberos)	Nombre d'erreurs de traitement Kerberos
	Nombre de requêtes NTLM
Total NTLM requests (Nombre total de requêtes NTLM)	Nombre total de requêtes d'authentification NTLM
Authentication succeeded (Authentification réussie)	Nombre de requêtes d'authentification NTLM ayant entraîné une authentification réussie
Authentication failed (Échecs d'authentification)	Nombre de requêtes d'authentification NTLM ayant entraîné un échec d'authentification
NTLM request errors (Erreurs de requêtes NTLM)	Nombre d'erreurs de traitement NTLM
NTLM within negotiate requests (Authentification NTLM dans les requêtes négociées)	Nombre de requêtes NTLM encapsulées dans des requêtes de négociation

Statistique	Description
	Nombre de requêtes d'authentification de base
Total basic authentication requests (Nombre total de requêtes d'authentification de base)	Nombre total de requêtes d'authentification de base
Authentication succeeded (Authentification réussie)	Nombre de requêtes d'authentification de base ayant entraîné une authentification réussie
Authentication failed (Échecs d'authentification)	Nombre de requêtes d'authentification de base ayant entraîné un échec d'authentification
Basic authentication request errors (Erreurs de requêtes d'authentification de base)	Nombre d'erreurs de traitement de l'authentification de base
	Compteurs de performances
Kerberos - Average time per transaction (Délai moyen par transaction)	Durée moyenne, en millisecondes, d'une transaction Kerberos complète
NTLM - Average time per transaction (Délai moyen par transaction)	Durée moyenne, en millisecondes, d'une transaction NTLM complète
Basic - Average time per transaction (De base - Délai moyen par transaction)	Durée moyenne, en millisecondes, d'une transaction de base complète
Average helper latency per transaction (Retard moyen de l'assistant par transaction)	Délai moyens requis par Samba pour traiter une requête d'authentification
Time authentication spent offline (Temps hors connexion des authentifications)	Délai, en secondes, pendant lequel Content Gateway n'a pas pu effectuer d'authentification NTLM à cause des défaillances d'un service ou de la connexion. (Cette mesure ne s'applique pas à Kerberos, car aucune communication n'est nécessaire avec le contrôleur de domaine.) Si l'option Global Fail Open (Échec ouvert global) est activée, les requêtes sont traitées sans authentification. Le compteur est incrémenté lorsque la connectivité est rétablie après une défaillance.
Number of times authentication servers or services went offline (Nombre de fois où des serveurs d'authentification ou des services étaient hors connexion)	Nombre de pertes de connexion aux serveurs d'authentification ou aux services

LDAP

Statistique	Description
	Cache
Hits (Accès fructueux au cache)	Nombre d'accès fructueux au cache LDAP
Misses (Accès infructueux au cache)	Nombre d'accès infructueux au cache LDAP
	Erreurs
Serveur	Nombre d'erreurs de serveur LDAP
	Échecs d'authentification
Authorization Denied (Autorisation refusée)	Nombre de fois où le serveur LDAP a refusé l'autorisation
Authorization Timeouts (Expiration des autorisations)	Nombre de fois où l'autorisation est arrivée à expiration
Authentication Cancelled (Authentification annulée)	Nombre de fois où l'authentification a été interrompue après le démarrage de l'authentification LDAP et avant la fin de l'opération **Remarque :** ce chiffre ne tient **pas** compte du nombre de fois où une demande d'authentification a été annulée par le client via un clic sur Annuler dans la boîte de dialogue demandant les informations d'authentification.

Authentification NTLM héritée

Statistique	Description
	Cache
Hits (Accès fructueux au cache)	Nombre d'accès fructueux au cache NTLM
Misses (Accès infructueux au cache)	Nombre d'accès infructueux au cache NTLM
	Erreurs
Serveur	Nombre d'erreurs de serveur NTLM
	Échecs d'authentification
Authorization Denied (Autorisation refusée)	Nombre de fois où le serveur NTLM a refusé l'autorisation
Authentication Cancelled (Authentification annulée)	Nombre de fois où l'authentification a été annulée
Authentication Rejected (Authentification refusée)	Nombre de fois où l'authentification a échoué parce que la file d'attente était pleine
	Taille de la file d'attente
Authentication Queued (File d'attente des authentifications)	Nombre de requêtes actuellement en file d'attente parce que tous les contrôleurs de domaine sont occupés

SOCKS

Statistique	Description
Serveur SOCKS sur dispositif (lorsque Content Gateway est installé dans un dispositif V-Series)	Indique si le serveur SOCKS sur dispositif est activé ou désactivé
Unsuccessful Connections (Nombre de connexions en échec)	Nombre d'échecs de connexion au serveur SOCKS depuis le démarrage de Content Gateway
Successful Connections (Nombre de connexions réussies)	Nombre de connexions réussies au serveur SOCKS depuis le démarrage de Content Gateway
Connections in Progress (Nombre de connexions en cours)	Nombre de connexions au serveur SOCKS actuellement en cours

Sécurité des données

Statistique	Description
Total Posts (Nombre total de publications)	Nombre total de publications envoyées à Data Security
Total Analyzed (Nombre total de publications analysées)	Nombre total de publications analysées par Data Security
FTP Analyzed (Nombre de requêtes FTP analysées)	Nombre total de requêtes FTP analysées par Data Security
Blocked Requests (Requêtes bloquées)	Nombre total de requêtes bloquées après analyse et application de la stratégie
Allowed Requests (Requêtes autorisées)	Nombre total de requêtes autorisées après analyse et application de la stratégie
Failed Requests (Échecs de requêtes)	Nombre total de publications envoyées à Data Security et arrivées à expiration ou n'ayant pas pu être terminées
Huge Requests (Requêtes volumineuses)	Nombre total de requêtes dont la taille dépassait la taille de transaction maximale
Tiny Requests (Petites requêtes)	Nombre total de requête dont la taille était inférieure à la taille de transaction minimale
Decrypted Requests (Requêtes décryptées)	Nombre total de requêtes SSL décryptées et envoyées à Data Security
Total Bytes Scanned (Nombre total d'octets analysés)	Nombre total d'octets analysés par Data Security
Average Response Time (Temps moyen de réponse)	Temps moyen requis par Data Security pour terminer une analyse depuis le dernier démarrage de Content Gateway

Sous-systèmes

Les statistiques concernant les sous-systèmes sont réparties dans les catégories suivantes :

Cache

> **Remarque**
> Il est possible que les statistiques de cache ne soient pas nulles, y compris lorsque l'ensemble du contenu envoyé à Content Gateway n'est pas mis en cache. Content Gateway effectue une lecture du cache, même si le client envoie un en-tête de contrôle no-cache.

Statistique	Description
	Général
Bytes Used (Nombre d'octets utilisés)	Nombre d'octets actuellement utilisés par le cache
Cache Size (Taille du cache)	Nombre d'octets alloués au cache
	Cache de mémoire RAM
Octets	Taille totale du cache de mémoire RAM, en octets
Hits (Accès fructueux au cache)	Nombre d'accès aux documents à partir du cache de mémoire RAM
Misses (Accès infructueux au cache)	Nombre d'accès infructueux aux documents à partir du cache de mémoire RAM. Les documents peuvent être des accès fructueux à partir du cache sur disque.
	Lectures
In Progress (En cours)	Nombre de lectures du cache en cours (HTTP et FTP)
Hits (Accès fructueux au cache)	Nombre de lectures du cache terminées depuis le démarrage de Content Gateway (HTTP et FTP)
Misses (Accès infructueux au cache)	Nombre de lectures du cache infructueuses depuis le démarrage de Content Gateway (HTTP et FTP)

Statistique	Description
	Écritures
In Progress (En cours)	Nombre d'écritures du cache en cours (HTTP et FTP)
Successes (Succès)	Nombre d'écritures fructueuses dans le cache depuis le démarrage de Content Gateway (HTTP et FTP)
Failures (Échecs)	Nombre d'échecs d'écritures dans le cache depuis le démarrage de Content Gateway (HTTP et FTP)
	Mises à jour
In Progress (En cours)	Nombre de mises à jour de documents HTTP en cours. Une mise à jour intervient lorsque Content Gateway revalide un objet, s'aperçoit qu'il est récent et met à jour l'en-tête de l'objet.
Successes (Succès)	Nombre de mises à jour HTTP réussies dans le cache depuis le démarrage de Content Gateway
Failures (Échecs)	Nombre d'échecs de mises à jour HTTP dans le cache depuis le démarrage de Content Gateway
	Suppressions
In Progress (En cours)	Nombre suppressions de documents en cours. Une suppression intervient lorsque Content Gateway revalide un document, s'aperçoit qu'il a été supprimé sur le serveur d'origine et le supprime dans le cache (suppressions HTTP et FTP comprises).
Successes (Succès)	Nombre de suppressions réussies dans le cache depuis le démarrage de Content Gateway (HTTP et FTP)
Failures (Échecs)	Nombre d'échecs de suppressions dans le cache depuis le démarrage de Content Gateway (HTTP et FTP)

Mise en cluster

Statistique	Description
Clustering Nodes (Nœuds du cluster)	Nombre de nœuds dans le cluster

Journalisation

Statistique	Description
Currently Open Log Files (Nombre de journaux actuellement ouverts)	Nombre de fichiers journaux d'événements (formats) en cours d'écriture
Space Used for Log Files (Espace occupé par les journaux)	Volume d'espace actuellement utilisé par le répertoire de journalisation, contenant l'ensemble des journaux d'événements et d'erreurs

Statistique	Description
Number of Access Events Logged (Nombre d'événements d'accès journalisés)	Nombre d'événements d'accès écrits dans les fichiers journaux depuis l'installation de Content Gateway. Ce nombre correspond à une entrée dans un fichier. Lorsque plusieurs formats sont écrits, un même accès crée plusieurs entrées dans le journal d'événements.
Number of Access Events Skipped (Nombre d'événements d'accès ignorés)	Nombre d'événements d'accès ignorés (à cause du filtrage) depuis l'installation de Content Gateway
Number of Error Events Logged (Nombre d'événements d'erreur journalisés)	Nombre d'événements d'accès écrits dans le journal des erreurs d'événements depuis l'installation de Content Gateway

Mise en réseau

Les statistiques concernant la mise en réseau sont réparties dans les catégories suivantes :

- *Système*, page 249
- *ARM*, page 250
- *ICAP*, page 251
- *WCCP*, page 252
- *Résolveur DNS*, page 253
- *IP virtuel*, page 253

Système

Statistique/Champ	Description
	Général
Nom d'hôte	Nom d'hôte affecté à cet ordinateur Content Gateway
Search Domain (Domaine de recherche)	Domaine de recherche utilisé par cet ordinateur Content Gateway
IPv4 ou IPv6	
Passerelle par défaut	Adresse IP de la passerelle utilisée par défaut pour transmettre les paquets de cet ordinateur Content Gateway vers d'autres réseaux ou sous-réseaux
Primary DNS (DNS principal)	Adresse IP du serveur DNS principal utilisé par cet ordinateur Content Gateway pour résoudre les noms d'hôte
Secondary DNS (DNS secondaire)	Serveur DNS secondaire utilisé par cet ordinateur Content Gateway pour résoudre les noms d'hôte
Tertiary DNS (DNS tertiaire)	Serveur DNS tertiaire utilisé par cet ordinateur Content Gateway pour résoudre les noms d'hôte

Statistique/Champ	Description
	Carte réseau <*nom_interface*>
Statut (État)	Indique si la carte réseau est active ou inactive
Start on Boot (Lancer au démarrage)	Indique si la carte réseau est configurée pour s'activer au démarrage
IPv4 ou IPv6	
Adresse IP	Adresse IP affectée à la carte réseau
Masque de sous-réseau	Masque de sous-réseau associé à l'adresse IP
Passerelle	Adresse IP de la passerelle configurée par défaut pour la carte réseau

ARM

Statistique	Description
	Statistiques de traduction d'adresses réseau (NAT)
Client Connections Natted (Connexions de client traduites)	Nombre de connexions de client redirigées en transparence par le module ARM
Client Connections in Progress (Nombre de connexions de clients en cours)	Nombre de connexions de clients actuellement en cours avec le module ARM
Total Packets Natted (Nombre total de paquets traduits)	Nombre de paquets traduits par le module ARM
DNS Packets Natted (Nombre de paquets DNS traduits)	Nombre de paquets DNS traduits par le module ARM
	Statistiques de contournement
Total Connections Bypassed (Nombre total de connexions ignorées)	Nombre total de connexions ignorées par le module ARM
Connections Dynamically Bypassed (Nombre de connexions ignorées dynamiquement)	Nombre total de connexions ignorées dynamiquement. Voir *Règles de contournement dynamique*, page 68.
DNS Packets Bypassed (Nombre de paquets DNS ignorés)	Nombre de paquets DNS ignorés par le module ARM
Connections Shed (Nombre de pertes de connexion)	Nombre total de pertes de connexion. Voir *Délestage de la charge de connexion*, page 70.

Statistique	Description
	Statistiques de contournement HTTP
Bypass on Bad Client Request (Contournement sur requête de client incorrecte)	Nombre de requêtes transmises directement au serveur d'origine à cause d'une erreur de trafic non HTTP rencontrée par Content Gateway sur le port 80
Bypass on 400 (Contournement sur erreur 400)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 400
Bypass on 401 (Contournement sur erreur 401)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 401
Bypass on 403 (Contournement sur erreur 403)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 403
Bypass on 405 (Contournement sur erreur 405)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 405
Bypass on 406 (Contournement sur erreur 406)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 406
Bypass on 408 (Contournement sur erreur 408)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 408
Bypass on 500 (Contournement sur erreur 500)	Nombre de requêtes transmises directement au serveur d'origine parce qu'un serveur d'origine a renvoyé une erreur 500

ICAP

Statistique	Description
Total Posts (Nombre total de publications)	Nombre total de publications envoyées à Data Security
Total Analyzed (Nombre total de publications analysées)	Nombre total de publications analysées par Data Security
FTP Analyzed (Nombre de requêtes FTP analysées)	Nombre total de requêtes FTP analysées par Data Security
Blocked Requests (Requêtes bloquées)	Nombre total de requêtes bloquées après analyse et application de la stratégie
Allowed Requests (Requêtes autorisées)	Nombre total de requêtes autorisées après analyse et application de la stratégie
Failed Requests (Échecs de requêtes)	Nombre total de publications envoyées à Data Security et arrivées à expiration ou n'ayant pas pu être terminées
Huge Requests (Requêtes volumineuses)	Nombre total de requêtes dont la taille dépassait la taille de transaction maximale
Decrypted Requests (Requêtes décryptées)	Nombre total de requêtes SSL décryptées et envoyées à Data Security

WCCP

Les statistiques WCCP v2 ne s'affichent que si WCCP version v2 est activé.

Statistique/Champ	Description
	Statistiques WCCP v2.0
Fragmentation WCCP	
Total Fragments (Nombre total de fragments)	Nombre total de fragments WCCP
Entrées de la table de fragmentation	Nombre d'entrées dans la table de fragmentation
Out of Order Fragments (Fragments hors service)	Nombre de fragments hors service
Matches (Correspondances)	Nombre de fragments correspondant à un fragment de la table de fragmentation
Service Group Name (Nom du groupe de services)	
Service Group ID (ID du groupe de services)	ID du groupe de services desservi par le protocole
Configured mode (Mode Configuré)	Paramètres de transmission, retour et affectation
Adresse IP	Adresse IP à laquelle le routeur envoie le trafic
Leader's IP Address (Adresse IP du leader)	Adresse IP du leader de la ferme de caches WCCP
Number of Buckets Assigned (Nombre de compartiments affectés)	Nombre de compartiments affectés à ce nœud Content Gateway. Déterminé selon la valeur du poids et les nœuds actuellement actifs.
Number of Caches (Nombre de caches)	Nombre de caches présents dans la ferme de caches WCCP
Number of Routers (Nombre de routeurs)	Nombre de routeurs envoyant du trafic à ce nœud Content Gateway
Router IP Address (Adresse IP du routeur)	Adresse IP du routeur WCCP envoyant du trafic à Content Gateway. **Remarque :** si le routeur WCCP est configuré avec plusieurs adresses IP, par exemple lorsqu'il est configuré pour prendre en charge plusieurs réseaux VLAN, l'adresse IP indiquée dans les statistiques **Monitor (Surveiller) > Networking (Mise en réseau) > WCCP** et dans les captures de paquets peut ne pas être la même que l'adresse IP configurée ici. En effet, le routeur signale systématiquement le trafic de l'adresse IP active la plus élevée. Pour que le routeur indique systématiquement la même adresse IP, une méthode consiste à définir l'adresse de bouclage sur une valeur supérieure à l'adresse IP du routeur. Il s'agit là de la configuration recommandée.

Statistique/Champ	Description
Router ID Received (ID de routeur reçus)	Nombre de fois où Content Gateway a reçu des messages de protocole WCCP envoyés par le(s) routeur(s)
Router Negotiated mode (Mode négocié avec le routeur)	Modes de retour, transmission et affectation négociés avec le routeur

Proxy DNS

Statistique	Description
Total Requests (Nombre total de requêtes)	Nombre total de requêtes DNS reçues des clients
Hits (Accès fructueux au cache)	Nombre d'accès fructueux au cache DNS
Misses (Accès infructueux au cache)	Nombre d'accès infructueux au cache DNS

Résolveur DNS

Statistique	Description
	Résolveur DNS
Total Lookups (Nombre total de recherches)	Nombre total de recherches DNS (requêtes destinées au serveurs de noms) depuis l'installation
Successes (Succès)	Nombre total de recherches DNS réussies depuis installation
Average Lookup Time (ms) (Durée moyenne des recherches (en millisecondes))	Durée moyenne d'une recherche DNS
	Base de données des hôtes
Total Lookups (Nombre total de recherches)	Nombre total de recherches effectuées dans la base de données des hôtes de Content Gateway depuis l'installation
Total Hits (Nombre total d'accès fructueux)	Nombre total d'accès fructueux à la base de données des hôtes depuis l'installation
Average TTL (min) (Durée de vie moyenne) (en minutes)	Durée de vie moyenne en minutes

IP virtuel

Le tableau des adresses IP virtuelles présente les adresses IP virtuelles gérées par les proxy du cluster.

Performances

Les graphiques de performances vous permettent de surveiller les performances de Websense Content Gateway et d'analyser le trafic réseau. Les graphiques de performances donnent également des informations sur l'utilisation de la mémoire virtuelle, les connexions des clients, les taux de présences et d'absences dans le cache, etc. Les graphiques de performances sont créés par l'outil MRTG (Multi Router Traffic Grapher). L'outil MRTG accumule les statistiques par intervalles de cinq minutes.

Les graphiques de performances fournissent les informations suivantes.

Statistique	Description
Overview (Vue d'ensemble)	Présente un sous-ensemble des graphiques disponibles
Daily (Quotidien)	Affiche des graphiques donnant des informations historiques sur la journée en cours
Weekly (Hebdomadaire)	Affiche des graphiques donnant des informations historiques sur la semaine en cours
Monthly (Mensuel)	Affiche des graphiques donnant des informations historiques sur le mois en cours
Yearly (Annuel)	Affiche des graphiques donnant des informations historiques sur l'année en cours

Important

Pour exécuter l'outil MRTG (Multi Router Traffic Grapher) sous Linux, vous devez avoir installé le logiciel Perl version 5.005 ou ultérieure dans votre système Content Gateway.

Une description est donnée à côté de chaque graphique. Cliquez sur un graphique pour afficher les statistiques quotidiennes, hebdomadaires, mensuelles et annuelles à l'écran.

Les graphiques suivants sont générés, et classés par ordre alphabétique :

- Active Client Connections (Nombre de connexions de clients actives)
- Active Native FTP Client Connections (Nombre de connexions de clients FTP natifs actives)
- Active Origin Server Connections (Nombre de connexions de serveurs d'origine actives)
- Active Parent Proxy Connections (Nombre de connexions de proxy parent actives)
- Bandwidth Savings (Économies de bande passante)
- Cache Read (Nombre de lectures dans le cache)
- Cache Reads Per Second (Nombre de lectures dans le cache par seconde)
- Cache Writes (Nombre d'écritures dans le cache)
- Cache Writes Per Second (Nombre d'écritures dans le cache par seconde)
- Client Transactions Per Second (Nombre de transactions de clients par seconde)

- Content Gateway Manager Memory Usage (Utilisation de la mémoire de Content Gateway Manager)
- Content Gateway Uptime (Durée d'activité de Content Gateway)
- CPU Available (Processeur disponible)
- CPU Busy (Processeur occupé)
- Data Security Module Memory Usage (Utilisation de la mémoire du module Data Security)
- Disk Cache Usage (Utilisation du cache disque)
- DNS Cache Usage (Utilisation du cache DNS)
- HTTP Abort Latency (Latence des abandons HTTP)
- HTTP and HTTPS Transactions Per Second (Nombre de transactions HTTP et HTTPS par seconde)
- HTTP Cache Hit Latency (Latence des accès fructueux au cache HTTP)
- HTTP Cache Miss Latency (Latence des accès infructueux au cache HTTP)
- HTTP Connection Errors & Aborts (Count) (Nombre d'abandons et d'erreurs de connexion HTTP)
- HTTP Connection Errors & Aborts (Percentage) (Pourcentage d'abandons et d'erreurs de connexion HTTP)
- HTTP Document Hit Rate (Taux d'accès fructueux aux documents HTTP)
- HTTP Error Latency (Latence des erreurs HTTP)
- HTTP Hits & Misses (Count) (Nombre d'accès fructueux et infructueux au cache HTTP)
- HTTP Hits & Misses (Percentage) (Pourcentage d'accès fructueux et infructueux au cache HTTP)
- HTTP POST and FTP PUT Transactions Per Second (Nombre de transactions HTTP POST et FTP PUT par seconde)
- Microsoft Internet Explorer Browser Requests (Percentage) (Pourcentage de requêtes du navigateur Microsoft Internet Explorer)
- MRTG Runtime (Exécution de l'outil MRTG)
- Network Reads (Lectures réseau)
- Network Writes (Écritures réseau)
- RAM Cache Read I/O Hit Rate (Taux d'E/S de lecture du cache de mémoire RAM)
- RAM Cache Usage (Utilisation du cache de mémoire RAM)
- SSL Manager Memory Usage (Utilisation de la mémoire de SSL Manager)
- TCP CLOSE_WAIT Connections (Connexions TCP CLOSE_WAIT)
- TCP Connect Rate (Taux de connexions TCP)
- TCP ESTABLISHED Connections (Connexions TCP ESTABLISHED)
- TCP FIN_WAIT_1 Connections (Connexions TCP FIN_WAIT_1)
- TCP FIN_WAIT_2 Connections (Connexions TCP FIN_WAIT_2)
- TCP LAST_ACK Connections (Connexions TCP LAST_ACK)
- TCP Segments Transmitted (Nombre de segments TCP transmis)
- TCP Throughput (Débit TCP)
- TCP TIME_WAIT Connections (Connexions TCP TIME_WAIT)
- Transaction Buffer Memory Usage (Utilisation de la mémoire tampon pour les transactions)
- WCCP Exceptional Input Fragments (Fragments d'entrée WCCP exceptionnels)
- WCCP Fragment Table Size (Taille de la table des fragments WCCP)

- WCCP Input Fragments (Fragments d'entrée WCCP)
- Web Security Scanned Transactions (Percentage) (Pourcentage de transactions analysées par Web Security)
- Web Security Slow Scanned Transactions (Transactions lentes analysées par Web Security)
- Web Security Slow Transactions (Transactions Web Security lentes)
- Websense Content Gateway Memory Usage (Utilisation de la mémoire de Websense Content Gateway)

SSL

Les onglets suivants sont pris en charge par SSL Manager :

SSL Key Data (Données des clés SSL), page 256

Statistiques CRL, page 257

Rapports, page 257

SSL Key Data (Données des clés SSL)

Ces champs donnent des informations sur l'état de la connexion SSL et sur l'activité entre le client et SSL Manager et entre SSL Manager et le serveur de destination.

Statistique/Champ	Description
	SSL Key Data (Données des clés SSL entrantes)
Is alive (Est actif)	Indique que SSL Manager est activé
Current SSL connections (Connexions SSL en cours)	Number of active inbound (browser to SSL Manager) SSL requests (Nombre de requêtes SSL actives entrantes (navigateur vers SSL Manager))
Total SSL server connections (Nombre total de connexions au serveur SSL)	Nombre de requêtes de navigateur
Total finished SSL server connections (Nombre total de connexions du serveur SSL terminées)	Nombre de requêtes de navigateur dont les données ont été envoyées à SSL Manager pour décryptage
Total SSL server renegotiation requests (Nombre total de requêtes de renégociation du serveur SSL)	Nombre de requêtes de navigateur renégociées du fait de l'échec du protocole standard ou de certificats non valides entre le navigateur et SSL Manager
	Données clés SSL sortantes
Is alive (Est actif)	Indique que SSL Manager est activé
Current SSL connections (Connexions SSL en cours)	Nombre de requêtes SSL actives sortantes (SSL Manager vers le serveur désigné)

Statistique/Champ	Description
Total SSL client connections (Nombre total de connexions de clients SSL)	Nombre de requêtes de navigateur
Total finished SSL client connections (Nombre total de connexions de clients SSL terminées)	Nombre de requêtes dont les données ont été envoyées de SSL Manager au serveur de destination
Total SSL client renegotiation requests (Nombre total de requêtes de renégociation de clients SSL)	Nombre de requêtes renégociées du fait de l'échec du protocole standard ou de certificats non valides entre SSL Manager et le serveur de destination
Total SSL session cache hits (Nombre total d'accès fructueux au cache de session SSL)	Nombre de fois où une requête a été validée par une clé du cache de session
Total SSL session cache misses (Nombre total d'accès infructueux au cache de session SSL)	Nombre de fois ou une requête n'a pas pu être validée par une clé du cache de session
Total SSL session cache timeouts (Nombre total d'expirations du cache de session SSL)	Nombres de fois où des clés ont été supprimées dans le cache de session à cause de l'expiration de la période

Statistiques CRL

Les champs suivants donnent des informations sur l'état des certificats.

Statistique/Champ	Description
	Statistiques CRL
CRL list count (Nombre de listes CRL)	Nombre de certificats présents dans la Liste de révocation des certificats (CRL). Cette liste est téléchargée chaque nuit. Voir *Actualisation des informations de révocation*, page 151.
	Statistiques OCSP
OCSP good count (Nombre de réponses OCSP valides)	Nombre de réponses confirmant la validité des certificats
OCSP unknown count (Nombre de réponses OCSP inconnues)	Nombre de réponses OCSP indiquant que le certificat n'a pas pu être vérifié
OCSP revoked count (Nombre de révocations OCSP)	Nombre de certificats identifiés comme révoqués (CRL & OCSP)

Rapports

Pour plus d'informations sur la création des rapports sur les autorités de certification ou les incidents, consultez la section *Création de rapports via SSL Manager*, page 116.

B Commandes et variables

Commandes de Websense Content Gateway

Pour exécuter des commandes individuelles ou des scripts de plusieurs commandes dans un Shell, utilisez la ligne de commande.

Pour exécuter des commandes, devenez utilisateur racine :

```
su
```

Exécutez les commandes de Content Gateway à partir du répertoire **bin** de Content Gateway.

> **Remarque**
> Si le répertoire **bin** de Content Gateway ne fait pas partie de votre chemin, précédez la commande de :
>
> ```
> ./
> ```
>
> Par exemple :
>
> ```
> ./content_line -p
> ```

Commande	Description
`WCGAdmin start`	Démarre le service Content Gateway
`WCGAdmin stop`	Arrête le service Content Gateway
`WCGAdmin restart`	Arrête le service Content Gateway et le redémarre
`WCGAdmin status`	Affiche l'état (en exécution ou en arrêt) des services Content Gateway : Content Gateway, Content Gateway Manager et **content_cop**
`WCGAdmin help`	Affiche la liste des commandes WCGAdmin
`content_line -p socket_path`	Spécifie l'emplacement (répertoire et chemin d'accès) du fichier utilisé pour la ligne de commande de Content Gateway et la communication avec Content Gateway Manager. Le chemin par défaut est **répertoire_installation/config/cli**.

Commande	Description
`content_line -r variable`	Affiche certaines statistiques de performances ou un paramètre de la configuration actuelle. Vous trouverez la liste des variables disponibles à la section *Variables de Websense Content Gateway*, page 260.
`content_line -s variable -v valeur`	Définit les variables de configuration. *variable* désigne la variable de configuration que vous souhaitez modifier et *valeur* désigne sa nouvelle valeur. Vous trouverez la liste des variables disponibles à la section *Fichier de configuration records.config*, page 377.
`content_line -h`	Affiche la liste des commandes Content Gateway
`content_line -x`	Déclenche la relecture d'un fichier de configuration de Content Gateway. L'exécution de cette commande est l'équivalent d'un clic sur **Appliquer** dans Content Gateway Manager.
`content_line -M`	Redémarre les processus **content_manager** et **content_gateway** dans tous les nœuds d'un cluster
`content_line -L`	Redémarre les processus **content_manager** et **content_gateway** dans le nœud local
`content_line -S`	Ferme Content Gateway dans le nœud local
`content_line -U`	Démarre Content Gateway dans le nœud local
`content_line -B`	Renvoie Content Gateway à l'échelle du cluster. Ce « rebond » de Content Gateway arrête et redémarre immédiatement le proxy nœud par nœud.
`content_line -b`	Renvoie Content Gateway dans le nœud local. Ce « rebond » de Content Gateway arrête et redémarre immédiatement le proxy dans le nœud local.

Variables de Websense Content Gateway

Vous pouvez changer la valeur d'une variable de configuration à l'invite à l'aide de la commande **content_line -s**. Les variables disponibles sont décrites à la section *Fichier de configuration records.config*, page 377.

Vous pouvez afficher les statistiques relatives à certaines variables à l'invite à l'aide de la commande **content_line -r**. Vous trouverez la liste des variables disponibles ci-dessous.

Voir également *Affichage des statistiques depuis la ligne de commande*, page 112, et *Interface de ligne de commande*, page 103.

Statistiques

Le tableau suivant énumère la liste des variables que vous pouvez spécifier à l'invite de commande pour afficher des statistiques individuelles. Pour plus d'informations, consultez la section *Statistiques*, page 235.

Pour afficher une statistique, à l'invite, entrez :

```
content_line -r variable
```

Statistique	Variable
	Résumé
Nom du nœud	*proxy.node.hostname*
Objets desservis	*proxy.node.user_agents_total_documents_served*
Nombre de transactions par seconde	*proxy.node.user_agent_xacts_per_second*
	Nœud
Taux d'accès aux documents	*proxy.node.cache_hit_ratio_avg_10s* *proxy.cluster.cache_hit_ratio_avg_10s*
Économies de bande passante	*proxy.node.bandwidth_hit_ratio_avg_10s* *proxy.cluster.bandwidth_hit_ratio_avg_10s*
Pourcentage de cache disponible	*proxy.node.cache.percent_free* *proxy.cluster.cache.percent_free*
Nombre de connexions ouvertes sur le serveur d'origine	*proxy.node.current_server_connections* *proxy.cluster.current_server_connections*
Nombre de connexions ouvertes par les clients	*proxy.node.current_client_connections* *proxy.cluster.current_client_connections*
Nombre de transferts du cache en cours	*proxy.node.current_cache_connections* *proxy.cluster.current_cache_connections*
Débit du client (en Mbits/sec)	*proxy.node.client_throughput_out* *proxy.cluster.client_throughput_out*
Nombre de transactions par seconde	*proxy.node.http.user_agent_xacts_per_second* *proxy.cluster.http.user_agent_xacts_per_second*
Nombre de recherches DNS par seconde	*proxy.node.dns.lookups_per_second* *proxy.cluster.dns.lookups_per_second*
Taux d'accès à la base de données des hôtes	*proxy.node.hostdb.hit_ratio_avg_10s* *proxy.cluster.hostdb.hit_ratio_avg_10s*
	HTTP
Nombre total d'octets de document provenant du client	*proxy.process.http.* *user_agent_response_document_total_size*
Nombre total d'octets d'en-tête provenant du client	*proxy.process.http.* *user_agent_response_header_total_size*
Nombre total d'octets d'en-tête de réponse entre le client et le cache	*proxy.process.http.* *user_agent_response_from_cache_header_total_size*
Nombre total d'octets de document de réponse entre le client et le cache	*proxy.process.http.user_agent_response_* *from_cache_document_total_size*

Statistique	Variable
Nombre total de connexions au client	*proxy.process.http.current_client_connections*
Nombre de clients uniques actuellement connectés	*proxy.process.http.client.unique_clients.active*
Nombre total de clients uniques s'étant connectés	*proxy.process.http.client.unique_clients.total*
Nombre total de clients dépassant la limite	*proxy.process.http.client.exceeding_limit*
Nombre total de clients dont les connexions ont été fermées	*proxy.process.http.client.closed_connections*
Nombre de connexions HTTP ouvertes par les clients	*proxy.process.http.current_active_http_client_connections*
Nombre de connexions HTTPS ouvertes par les clients	*proxy.node.process.http.current_active_https_client_connections*
Nombre de requêtes des clients (IPv4 et IPv6)	*proxy.process.http.real_client_requests*
Nombre de requêtes IPv6 des clients	*proxy.process.http.real_client_ipv6_requests*
Nombre de transactions de client en cours	*proxy.process.http.current_client_transactions*
Nombre total d'octets de document provenant du serveur d'origine	*proxy.process.http.origin_server_response_document_total_size*
Nombre total d'octets d'en-tête provenant du serveur d'origine	*proxy.process.http.origin_server_response_header_total_size*
Nombre total de connexions au serveur d'origine	*proxy.process.http.current_server_connections*
Nombre de transactions en cours du serveur d'origine	*proxy.process.http.current_server_transactions*
	FTP
Nombre de connexions FTP actuellement ouvertes	*proxy.process.ftp.connections_currently_open*
Nombre de connexions PASV réussies	*proxy.process.ftp.connections_successful_pasv*
Nombre de connexions PASV en échec	*proxy.process.ftp.connections_failed_pasv*
Nombre de connexions réussies au port	*proxy.process.ftp.connections_successful_port*
Nombre de connexions en échec au port	*proxy.process.ftp.connections_failed_port*
	WCCP
Activé	*proxy.config.wccp.enabled*
Interface WCCP	*proxy.local.wccp2.ethernet_interface*

Statistique	Variable
	Cache
Nombre d'octets utilisés	*proxy.process.cache.bytes_used*
Taille du cache	*proxy.process.cache.bytes_total*
Nombre de recherches en cours	*proxy.process.cache.lookup.active*
Nombre de recherches terminées	*proxy.process.cache.lookup.success*
Nombre de recherches infructueuses	*proxy.process.cache.lookup.failure*
Nombre de lectures en cours	*proxy.process.cache.read.active*
Nombre de lectures terminées	*proxy.process.cache.read.success*
Nombre de lectures infructueuses	*proxy.process.cache.read.failure*
Nombre d'écritures en cours	*proxy.process.cache.write.active*
Nombre d'écritures terminées	*proxy.process.cache.write.success*
Nombre d'écritures en échec	*proxy.process.cache.write.failure*
Nombre de mises à jour en cours	*proxy.process.cache.update.active*
Nombre de mises à jour terminées	*proxy.process.cache.update.success*
Nombre de mises à jour en échec	*proxy.process.cache.update.failure*
Nombre de suppressions en cours	*proxy.process.cache.remove.active*
Nombre de suppressions réussies	*proxy.process.cache.remove.success*
Nombre de suppressions en échec	*proxy.process.cache.remove.failure*
	Base de données des hôtes
Nombre total de recherches	*proxy.process.hostdb.total_lookups*
Nombre total d'accès	*proxy.process.hostdb.total_hits*
Durée de vie (TTL, time-to-live) (en minutes)	*proxy.process.hostdb.ttl*
	DNS
Nombre total de recherches DNS	*proxy.process.dns.total_dns_lookups*
Durée moyenne des recherches (en millisecondes)	*proxy.process.dns.lookup_avg_time*
Nombre de recherches DNS réussies	*proxy.process.dns.lookup_successes*

Statistique	Variable
	Cluster
Nombre d'octets lus	*proxy.process.cluster.read_bytes*
Nombre d'octets écrits	*proxy.process.cluster.write_bytes*
Nombre de connexions ouvertes	*proxy.process.cluster.connections_open*
Nombre total d'opérations	*proxy.process.cluster.connections_opened*
Sauvegardes réseau	*proxy.process.cluster.net_backup*
Nœuds du cluster	*proxy.process.cluster.nodes*
	SOCKS
Nombre de connexions en échec	*proxy.process.socks.connections_unsuccessful*
Nombre de connexions réussies	*proxy.process.socks.connections_successful*
Nombre de connexions en cours	*proxy.process.socks.connections_currently_open*
	Journalisation
Nombre de journaux actuellement ouverts	*proxy.process.log2.log_files_open*
Espace occupé par les journaux	*proxy.process.log2.log_files_space_used*
Nombre d'événements d'accès journalisés	*proxy.process.log2.event_log_access*
Nombre d'événements d'accès ignorés	*proxy.process.log2.event_log_access_skip*
Nombre d'événements d'erreur journalisés	*proxy.process.log2.event_log_error*

C Options de configuration

Sur le côté gauche du volet de configuration, les options sont regroupées comme suit :

Mon proxy

Les options de Mon proxy sont regroupées comme suit :

De base

Option	Description
	Général
Redémarrer	Cette option redémarre le proxy et les services Manager (processus **content_gateway** et **content_manager**). Après la modification de certaines options de configuration, le redémarrage du proxy et des services Manager est nécessaire. Dans une configuration en cluster, le bouton **Redémarrer** redémarre le proxy et les services Manager dans tous les nœuds du cluster.
Nom du proxy	Indique le nom de votre nœud Content Gateway. Par défaut, il s'agit du nom d'hôte de l'ordinateur exécutant Content Gateway. Lorsque ce nœud fait partie d'un cluster, cette option spécifie le nom du cluster Content Gateway. Dans un cluster Content Gateway, tous les nœuds doivent partager le même nom.
Alarm email (Envoyer les alarmes par e-mail)	Spécifie l'adresse électronique à laquelle Content Gateway envoie les notifications d'alarme
Fonctions	
Protocoles : FTP	Lorsque cette option est activée, Content Gateway accepte les requêtes FTP des clients FTP. Si cette option est modifiée, vous devez redémarrer Content Gateway.
Protocoles : HTTPS	Active/désactive le traitement des requêtes HTTPS (données cryptées) par SSL Manager. Après la sélection de HTTPS **On (Activer)**, vous devez fournir d'autres informations dans les pages **Configurer > Protocoles > HTTPS** et **Configurer > SSL**. Voir *Utilisation des données cryptées*, page 129.
Networking (Mise en réseau) : WCCP	Activez cette option pour utiliser un routeur de type WCCP v2 pour la redirection transparente vers Content Gateway. WCCP v1 n'est **pas** pris en charge. Voir *Interception transparente avec dispositifs WCCP v2*, page 50. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Networking (Mise en réseau) : Proxy DNS	Lorsque cette option est activée, Content Gateway résout les requêtes DNS au nom des clients. Cette option décharge les serveurs DNS distants et accélère les recherches DNS. Voir *Mise en cache du proxy DNS*, page 95.
Networking (Mise en réseau) : IP virtuel	Lorsque cette option est activée, Content Gateway conserve un pool d'adresses IP virtuelles qu'il affecte aux nœuds du cluster en fonction des besoins. Voir *Basculement IP virtuel*, page 83.

Option	Description
Networking (Mise en réseau) : IPv6	Lorsque cette option est activée, Content Gateway assure une prise en charge limitée du protocole IPv6. Cette prise en charge est fournie uniquement pour un proxy explicite. Les adresses IPv6 peuvent être utilisées sur une interface Ethernet à double pile desservant les clients et/ou le trafic Internet. Des adresses IPv4 peuvent être utilisées pour communiquer avec tous les composants TRITON. Voir *Prise en charge d'IPv6 par Content Gateway version 7.7.0*, page 45.
Networking (Mise en réseau) : Data Security	Active une connexion à Websense Data Security. Deux options sont disponibles : • Enregistrement automatique auprès du serveur de gestion de Data Security (version 7.7 requise) • Communication ICAP avec un déploiement Data Security Suite distant (version 7.1 ou antérieure) Voir *Utilisation de Websense Data Security*, page 119. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Networking (Mise en réseau) : Data Security : Integrated on-box (Intégration prête à l'emploi)	Active l'enregistrement auprès des composants Data Security prêts à l'emploi et du serveur de gestion de Data Security. Voir *Enregistrement et configuration de Data Security*, page 121.
Networking (Mise en réseau) : Data Security : ICAP	Active l'utilisation d'ICAP avec Data Security Suite. Voir *Configuration du client ICAP*, page 125.
Sécurité : SOCKS	Lorsque l'option SOCKS est activée, Content Gateway communique avec vos serveurs SOCKS. Voir *Configuration de l'intégration du pare-feu SOCKS*, page 171. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Authentification : Aucune	Content Gateway prend en charge plusieurs types d'authentification des utilisateurs. Lorsque cette option est activée, le proxy n'authentifie pas les utilisateurs. Il s'agit là du paramètre par défaut.
Authentification : Authentification Windows intégrée	Lorsque l'Authentification Windows intégrée (IWA) est activée, les utilisateurs sont authentifiés par IWA avant de pouvoir accéder au contenu. Voir *Authentification Windows intégrée*, page 179. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Authentification : LDAP	Lorsque l'authentification LDAP est activée, les utilisateurs sont authentifiés par un serveur LDAP avant de pouvoir accéder au contenu. Voir *Authentification LDAP*, page 188. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Option	Description
Authentification : Radius	Lorsque l'authentification RADIUS est activée, les utilisateurs sont authentifiés par un serveur RADIUS avant de pouvoir accéder au contenu. Voir *Authentification RADIUS*, page 190. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Authentification : Authentification NTLM héritée	Lorsque l'authentification NTLM héritée (NTLMSSP) est activée, les utilisateurs d'un réseau Windows sont authentifiés par un contrôleur de domaine avant de pouvoir accéder au contenu. Voir *Authentification NTLM héritée*, page 185. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Authentification : Multiple Realm Authentication (Authentification dans plusieurs domaines Kerberos)	Active ou désactive l'authentification dans plusieurs domaines Kerberos. L'authentification dans plusieurs domaines Kerberos prend en charge les environnements constitués de plusieurs domaines ne partageant pas de relations de confiance et pour lesquels les utilisateurs doivent être authentifiés par des contrôleurs de domaine spécifiques. Voir *Authentification dans plusieurs domaines Kerberos*, page 194. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Authentification : Read authentication from child proxy (Lire l'authentification à partir du proxy enfant)	Active ou désactive la lecture des valeurs d'en-tête X-Authenticated-User et X-Forwarded-For présentes dans les requêtes entrantes. Cette option est désactivée par défaut. Activez cette option lorsque Content Gateway est le proxy parent (en amont) dans une chaîne et que le proxy enfant (en aval) envoie des valeurs d'en-tête X-Authenticated-User et X-Forwarded-For pour simplifier l'authentification.
Authentification : Send authentication to parent proxy (Envoyer l'authentification au proxy parent)	Active ou désactive l'insertion des valeurs d'en-tête X-Authenticated-User dans les requêtes sortantes. Cette option est désactivée par défaut. Activez cette option lorsque Content Gateway est le proxy enfant (en aval) dans une chaîne et que le proxy parent (en amont) réclame des valeurs d'en-tête X-Authenticated-User pour simplifier l'authentification.
	Mise en cluster
Cluster : Type	Spécifie le mode de clustering : Sélectionnez **Single Node (Nœud unique)** pour que ce serveur Content Gateway s'exécute en tant que nœud unique. Ce nœud ne fera pas partie d'un cluster. Sélectionnez **Management Clustering (Gestion de la mise en cluster)** pour activer le mode de gestion de la mise en cluster. Les nœuds du cluster partagent leurs informations de configuration et vous pouvez gérer l'ensemble des nœuds simultanément. Pour obtenir des informations complètes sur la mise en cluster, consultez la section *Clusters*, page 77. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Option	Description
Cluster : Interface	Définit l'interface par laquelle Content Gateway communique avec les autres nœuds du cluster. Par exemple, **eth0**. Il est recommandé d'utiliser une interface secondaire dédiée. Les informations de configuration des nœuds sont multidiffusées, en texte brut, vers les autres nœuds Content Gateway du même sous-réseau. C'est pourquoi Websense recommande de placer les clients dans un sous-réseau différent de celui des nœuds Content Gateway. En effet, les communications en multidiffusion ne sont pas acheminées pour le clustering. Pour les dispositifs V-Series, P1 (eth0) est l'interface conseillée. Vous pouvez cependant utiliser également P2 (eth1) si vous souhaitez isoler le trafic de gestion du cluster. Voir *Modification de la configuration du clustering*, page 80. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Cluster : Multicast Group Address (Adresse du groupe en multidiffusion)	Spécifie l'adresse du groupe en multidiffusion par laquelle Content Gateway communique avec ses pairs au sein du cluster. Voir *Modification de la configuration du clustering*, page 80.
Cluster : SSL Manager Configuration Server (Serveur de configuration de SSL Manager)	Définit l'adresse IP du serveur de configuration de SSL Manager. Lorsque Content Gateway redémarre, le serveur de configuration de SSL Manager (principal) est identifié pour tous les membres du cluster. Toutes les modifications de la configuration SSL doivent être effectuées dans le serveur principal. Voir *Mise en cluster de SSL Manager*, page 78.

Abonnement

Option	Description
	Gestion des abonnements
Clé de licence	Présente la clé d'abonnement que Websense vous a envoyée. Cette clé correspond aux produits auxquels vous vous êtes abonnés. Si Content Gateway est utilisé avec Web Security Gateway ou Web Security Gateway Anywhere, il s'agit de la clé l'abonnement que vous avez saisi dans TRITON – Web Security. Si Content Gateway est déployé uniquement avec Websense Data Security Suite, vous devez saisir votre clé d'abonnement Content Gateway dans ce champ.
	Analyse
Policy Server	
Adresse IP	Définit l'adresse IP du serveur de stratégies Websense Web Security Policy Server
Port	Définit le port utilisé par le serveur de stratégies Websense Web Security Policy Server

Option	Description
Service de filtrage	
Adresse IP	Définit l'adresse IP du service de filtrage de Websense Web Security
Port	Définit le port utilisé par le service de filtrage de Websense Web Security
Communication Timeout (Expiration de la communication)	Définit le délai, en millisecondes, au cours duquel Policy Server et Filtering Service doivent répondre avant que ne se produise une condition d'expiration de la communication et que le paramètre **Action for Communication Errors (Action pour erreurs de communication)** ne soit appliqué. La valeur par défaut est 5 000 (5 secondes).
Action for Communication Errors (Action pour erreurs de communication)	
Permit traffic (Autoriser le trafic)	Autorise toutes les pages en cas d'échec de la communication avec Policy Server ou Filtering Service
Block traffic (Bloquer le trafic)	Bloque toutes les pages en cas d'échec de la communication avec Policy Server ou Filtering Service

UI Setup (Configuration de l'interface utilisateur)

Option	Description
	Général
UI Port (Port de l'interface utilisateur)	Définit le port par lequel les navigateurs peuvent se connecter à Content Gateway Manager. Le port doit être situé dans le système Content Gateway et dédié à Content Gateway. Le port par défaut est le 8081. Si vous modifiez ce paramètre, vous devez redémarrer Content Gateway.
SSL UI Port (Port de l'interface utilisateur SSL)	Définit le port de l'interface utilisateur de SSL Manager. Cette interface vous permet de gérer le décryptage des données et les certificats. Le port par défaut est le 8071. Voir *Utilisation des données cryptées*, page 129. Les interfaces de Content Gateway Manager et de SSL Manager doivent être sur des ports différents. Si vous modifiez ce paramètre, vous devez redémarrer Content Gateway.
HTTPS : Activer/ Désactiver	Active ou désactive la prise en charge des connexions SSL à Content Gateway Manager. SSL protège la configuration et la surveillance administrative à distance. Pour utiliser SSL pour les connexions à Content Gateway Manager, vous devez installer un certificat SSL dans le serveur Content Gateway. Pour plus d'informations, consultez la section *Utilisation de SSL pour l'administration sécurisée*, page 166.

Option	Description
HTTPS : Certificate File (Fichier de certificat)	Définit le nom du fichier du certificat SSL utilisé pour authentifier les utilisateurs souhaitant accéder à Content Gateway Manager
Monitor Refresh Rate (Taux d'actualisation de la surveillance)	Définit la fréquence selon laquelle Content Gateway Manager actualise les statistiques affichées dans le volet **Monitor (Surveiller)**. La valeur par défaut est 30 secondes.
	Connexion
Basic Authentication (Authentification de base)	Active ou désactive l'authentification de base. Lorsque cette option est activée, Content Gateway vérifie le nom de connexion et le mot de passe de l'administrateur ou de l'utilisateur (si des comptes d'utilisateur ont été configurés) dès qu'un utilisateur tente d'accéder à Content Gateway Manager.
Administrateur : Connexion	Définit la connexion administrateur. La connexion administrateur est la connexion principale autorisée à accéder aux modes configuration et surveillance de Content Gateway Manager. Remarque : Si l'authentification de base est activée, Content Gateway vérifie uniquement l'ID de connexion administrateur.
Administrateur : Mot de passe	Permet de modifier le mot de passe d'administrateur qui contrôle l'accès à Content Gateway Manager. Pour le modifier, saisissez le mot de passe actuel dans le champ **Ancien mot de passe**, puis le nouveau dans le champ **Nouveau mot de passe**. Saisissez une nouvelle fois le nouveau mot de passe dans le champ **New Password (Retype) (Confirmer le nouveau mot de passe)**, puis cliquez sur **Appliquer**. Remarque : Si l'authentification de base est activée, Content Gateway vérifie uniquement l'ID administrateur et le mot de passe. Vous devez choisir le mot de passe de l'administrateur lors de l'installation. Le programme d'installation crypte automatiquement le mot de passe et le stocke dans le fichier **records.config**, de sorte que personne ne puisse le lire. Chaque fois que vous modifiez le mot de passe dans Content Gateway Manager, Content Gateway met à jour le fichier **records.config**. Si vous avez oublié le mot de passe de l'administrateur et que vous n'avez plus accès à Content Gateway Manager, consultez la section *Comment accéder à Content Gateway Manager si j'ai oublié le mot de passe de l'administrateur principal ?*, page 466.

Option	Description
Additional Users (Autres utilisateurs)	Répertorie les comptes d'utilisateur actuels et permet d'en ajouter de nouveaux. Les comptes d'utilisateur identifient les personnes autorisées à accéder à Content Gateway Manager et les activités que ces personnes peuvent y effectuer. Vous pouvez créer une liste de comptes d'utilisateur lorsqu'un seul ID/mot de passe d'administrateur ne répond pas à vos besoins en matière de sécurité. Pour créer un nouveau compte, saisissez un nom d'utilisateur dans le champ **New User (Nouvel utilisateur)**, puis un mot de passe dans le champ **Nouveau mot de passe**. Saisissez une nouvelle fois le mot de passe de l'utilisateur dans le champ **New Password (Retype) (Confirmer le nouveau mot de passe)**, puis cliquez sur **Appliquer**. Les informations du nouvel utilisateur s'affichent dans le tableau. Dans la liste déroulante **Access (Accès)** du tableau, sélectionnez les activités que ce nouvel utilisateur peut effectuer (surveillance, surveillance et affichage de la configuration et surveillance et modification de la configuration). Pour plus d'informations sur les comptes d'utilisateur, consultez la section *Création d'une liste de comptes d'utilisateur*, page 165. Remarque : Si l'authentification de base est activée, Content Gateway vérifie uniquement le nom de connexion et le mot de passe de l'utilisateur.
	Accès
Contrôle d'accès	Affiche un tableau répertoriant les règles présentes dans le *Fichier de configuration mgmt_allow.config* qui définissent les hôtes distants autorisés à accéder à Content Gateway Manager. Les entrées de ce fichier permettent d'être certain que seuls les utilisateurs authentifiés peuvent modifier les options de configuration et afficher les performances et les statistiques du trafic réseau. Remarque : par défaut, tous les hôtes distants sont autorisés à accéder à Content Gateway Manager.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **mgmt_allow.config**
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **mgmt_allow.config**
	Éditeur de fichier de configuration pour le fichier mgmt_allow.config
Champ d'affichage des règles	Répertorie les règles du fichier **mgmt_allow.config**. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste. Content Gateway applique les règles selon leur ordre d'apparition dans cette liste, en commençant à partir du haut.

Option	Description
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
IP Action (Action IP)	Répertorie le type de règles pouvant être ajoutées. Une règle **ip_allow** autorise les hôtes distants spécifiés dans le champ **Source IP** à accéder à Content Gateway Manager. Une règle **ip_deny** interdit aux hôtes distants spécifiés dans le champ **Source IP** d'accéder à Content Gateway Manager.
IP source	Définit les adresses IP pour lesquelles l'accès à Content Gateway Manager est autorisé ou refusé. Vous pouvez saisir une adresse IP individuelle (111.111.11.1) ou une plage d'adresses IP (0.0.0.0-255.255.255.255).
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

Instantanés

Option	Description
	Système de fichiers
Change Snapshot Directory (Modifier le répertoire des instantanés)	Définit le répertoire de stockage des instantanés dans ce nœud Content Gateway
Snapshots (Instantanés) : Save Snapshot (Enregistrer l'instantané)	Définit le nom de l'instantané de configuration que vous souhaitez créer. Cliquez sur **Appliquer** pour enregistrer cette configuration dans le nœud local. Content Gateway enregistre l'instantané de la configuration dans le répertoire défini dans le champ **Change Snapshot Directory (Modifier le répertoire des instantanés)**. Nous vous recommandons de créer un instantané de votre configuration avant d'effectuer la maintenance du système ou de tenter de régler ses performances. La création d'un instantané de configuration ne prend que quelques secondes et peut vous éviter de passer des heures à corriger les erreurs de configuration.

Option	Description
Snapshots (Instantanés) : Restore/Delete Snapshot (Restaurer/Supprimer un instantané)	Répertorie les instantanés stockés dans ce nœud. Sélectionnez l'instantané à restaurer ou à supprimer dans la liste déroulante.
Snapshots (Instantanés) : Restore Snapshot from "directory_name" Directory (Restaurer l'instantané à partir du répertoire nom_répertoire)	Restaure l'instantané sélectionné dans le champ déroulant **Restore/Delete Snapshot (Restaurer/ Supprimer un instantané)**. Dans une configuration en cluster, les instantanés sont restaurés dans tous les nœuds du cluster.
Snapshots (Instantanés) : Delete Snapshot from "directory_name" Directory (Supprimer l'instantané dans le répertoire nom_répertoire)	Supprime l'instantané sélectionné dans le champ déroulant **Restore/Delete Snapshot (Restaurer/ Supprimer un instantané)**
	Serveur FTP
Serveur FTP	Définit le nom du serveur FTP à partir duquel vous souhaitez restaurer un instantané de configuration ou dans lequel vous souhaitez enregistrer un instantané de votre configuration
Connexion	Définit l'ID de connexion nécessaire pour accéder au serveur FTP
Mot de passe	Définit le mot de passe nécessaire pour accéder au serveur FTP
Remote Directory (Supprimer le répertoire)	Définit le répertoire du serveur FTP à partir duquel vous souhaitez restaurer un instantané de configuration ou dans lequel vous souhaitez enregistrer un instantané de configuration
Restore Snapshot (Restaurer un instantané)	Répertorie les instantanés de configuration stockés dans le serveur FTP et que vous pouvez restaurer. Ce champ s'affiche lorsque vous avez réussi à vous connecter au serveur FTP.
Save Snapshot to FTP Server (Enregistrer l'instantané dans le serveur FTP)	Définit le nom de l'instantané de configuration que vous souhaitez créer et enregistrer dans le serveur FTP. Ce champ s'affiche lorsque vous avez réussi à vous connecter au serveur FTP.

Journaux

Option	Description
	Système
Fichier journal	Répertorie les fichiers journaux système que vous pouvez afficher, supprimer ou copier dans votre système local. Content Gateway répertorie les fichiers journaux système enregistrés via le mécanisme de journalisation à l'échelle du système **syslog** dans l'utilitaire du démon.
Action : Display the selected log file (Afficher le fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway affiche le premier Mo du fichier journal système sélectionné dans la liste déroulante **Fichier journal**. Pour afficher le fichier dans son intégralité, sélectionnez « Save the selected log file in local filesystem (Enregistrer le fichier journal sélectionné dans le système de fichiers local) » et affichez le fichier à l'aide d'une visionneuse locale.
Action : Display last lines of the selected file (Afficher les dernières lignes du fichier sélectionné)	Lorsque cette option est activée, Content Gateway affiche le nombre donné des dernières lignes du fichier journal système sélectionné.
Action : Display lines that match in the selected log file (Afficher les lignes correspondantes du fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway affiche toutes les lignes du fichier journal système sélectionné correspondant à la chaîne indiquée.
Action : Remove the selected log file (Supprimer le fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway supprime le fichier journal sélectionné.
Action : Save the selected log file in local filesystem (Enregistrer le fichier journal sélectionné dans le système de fichiers local)	Lorsque cette option est activée, Content Gateway enregistre le fichier journal sélectionné dans le système local, à l'emplacement que vous définissez.
	Accès
Fichier journal	Répertorie les fichiers journaux d'événements ou d'erreurs que vous pouvez afficher, supprimer ou copier dans votre système local. Content Gateway répertorie les fichiers journaux d'événements situés dans le répertoire défini dans le champ **Logging Directory (Répertoire de journalisation)** de l'onglet **Subsystems/Logging (Sous-systèmes/Journalisation)** et par la variable de configuration **proxy.config.log2.logfile_dir** du fichier **records.config**. Par défaut, il s'agit du répertoire **logs** situé dans le répertoire d'installation de Content Gateway.

Option	Description
Action : Display the selected log file (Afficher le fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway affiche le premier Mo du fichier journal d'événements ou d'erreurs sélectionné dans la liste déroulante **Fichier journal**. Pour afficher le fichier dans son intégralité, sélectionnez « Save the selected log file in local filesystem (Enregistrer le fichier journal sélectionné dans le système de fichiers local) » et affichez le fichier à l'aide d'une visionneuse locale.
Action : Display last lines of the selected file (Afficher les dernières lignes du fichier sélectionné)	Lorsque cette option est activée, Content Gateway affiche le nombre donné des dernières lignes du fichier journal d'événements ou d'erreurs sélectionné dans la liste déroulante **Fichier journal**.
Action : Display lines that match in the selected log file (Afficher les lignes correspondantes du fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway affiche toutes les lignes du fichier journal d'événements ou d'erreurs sélectionné correspondant à la chaîne indiquée.
Remove the selected log file (Supprimer le fichier journal sélectionné)	Lorsque cette option est activée, Content Gateway supprime le fichier journal sélectionné.
Action : Save the selected log file in local filesystem (Enregistrer le fichier journal sélectionné dans le système de fichiers local)	Lorsque cette option est activée, Content Gateway enregistre le fichier journal sélectionné dans le système local, à l'emplacement que vous définissez.

Protocoles

Les options de configuration des protocoles se répartissent dans les catégories suivantes :

HTTP, page 277

Réponses HTTP, page 285

HTTP Scheduled Update (HTTP - Mise à jour planifiée), page 286

HTTPS, page 288

FTP, page 288

HTTP

Option	Description
	Général
HTTP Proxy Server Port (Port du serveur proxy HTTP)	Définit le port utilisé par Content Gateway lorsqu'il joue le rôle de serveur proxy Web pour le trafic HTTP ou lorsqu'il dessert des requêtes HTTP en transparence. Le port par défaut est le 8080. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Secondary HTTP Proxy Server Ports (Ports des serveurs proxy HTTP secondaires)	**Pour les configurations avec proxy explicite** uniquement, définit les autres ports sur lesquels Content Gateway est à l'écoute du trafic HTTP. Les configurations avec proxy transparent envoient toujours la totalité du trafic HTTP sur le port 8080.
Unqualified Domain Name Expansion (Extension du nom de domaine non qualifié)	Active ou désactive l'extension du nom **.com**. Lorsque cette option est activée, Content Gateway tente de résoudre les noms d'hôte non qualifiés en les redirigeant vers l'adresse étendue, en ajoutant **www.** devant celle-ci et **.com** à la fin. Par exemple, lorsqu'un client demande `entreprise`, Content Gateway redirige la requête vers **www.entreprise.com**. Si l'extension de domaine local est activée (voir *Résolveur DNS*, page 330), Content Gateway essaie avec l'extension de domaine local située avant l'extension de domaine **.com**. Content Gateway essaie uniquement avec l'extension de domaine **.com** si l'extension de domaine local échoue.
Send HTTP 1.1 by Default (Envoyer HTTP 1.1 par défaut)	Active l'envoi de HTTP 1.1 en tant que première requête destinée au serveur d'origine (par défaut). Si le serveur d'origine répond par HTTP 1.0, Content Gateway bascule sur HTTP 1.0 (la plupart des serveurs d'origine utilisent HTTP 1.1). Lorsque cette option est désactivée, HTTP 1.0 est utilisée dans la première requête envoyée au serveur d'origine. Si le serveur d'origine répond par HTTP 1.1, Content Gateway bascule sur HTTP 1.1.
Reverse DNS (DNS inversé)	Active la recherche DNS inversée lorsque l'URL contient une adresse IP (à la place du nom d'hôte) et lorsque des règles existent dans les fichiers **filter.config**, **cache.config** ou **parent.config**. Cette option est nécessaire lorsque les règles sont basées sur le nom d'hôte de destination et le nom de domaine.
Tunnel Ports (Ports de tunnel)	Définit des ports sur lesquels Content Gateway autorise la mise en tunnel. Il s'agit d'une liste séparée par des espaces qui accepte également des plages de ports (ex. : 1-65535). Lorsque SSL n'est pas activé, tout le trafic destiné aux ports spécifiés peut-être mis en tunnel vers un serveur d'origine. Lorsque SSL est activé, le trafic passant par les ports également répertoriés dans le champ Ports HTTPS n'est pas mis en tunnel, mais décrypté avant de se voir appliquer la stratégie de filtrage.

Option	Description
Ports HTTPS	Définit les ports sur lesquels le trafic est décrypté et sur lesquels la stratégie est appliquée lorsque SSL est activé. Lorsque SSL est désactivé, le trafic passant par ces ports n'est pas décrypté et la stratégie de filtrage appliquée varie : • Dans un proxy explicite, selon le nom d'hôte du serveur indiqué dans la requête CONNECT • En mode transparent, selon le nom d'hôte du serveur indiqué dans le certificat du serveur
FTP sur HTTP : Anonymous Password (Mot de passe anonyme)	Définit le mot de passe anonyme que Content Gateway doit utiliser pour les connexions au serveur FTP exigeant un mot de passe. Cette option affecte les requêtes FTP provenant de clients HTTP.
FTP sur HTTP : Data Connection Mode (Mode Connexion de données)	Un transfert FTP requiert deux connexions : une connexion de contrôle pour signaler la demande de données au serveur FTP et une connexion de données pour l'envoi des données. Content Gateway initie toujours la connexion de contrôle. Le mode FTP détermine si Content Gateway ou le serveur FTP doit initier la connexion de données. Sélectionnez **PASV then PORT (PASV puis PORT)** pour que Content Gateway essaie d'abord le mode de connexion PASV. Si le mode PASV échoue, Content Gateway essaie le mode PORT et initie la connexion de données. Si le mode réussit, le serveur FTP accepte la connexion de données. Sélectionnez **PASV only (PASV uniquement)** pour que Content Gateway initie la connexion de données sur le serveur FTP. Ce mode supporte les pare-feu, mais pas certains serveurs FTP. Sélectionnez **PORT only (PORT uniquement)** pour que le serveur FTP initie la connexion de données et que Content Gateway accepte la connexion. La valeur par défaut est **PASV then PORT (PASV puis PORT)**.
	Capacités de mise en cache
Caching (Mise en cache) : HTTP Caching (Mise en cache HTTP)	Active ou désactive la mise en cache HTTP. Lorsque cette option est activée, Content Gateway dessert les requêtes HTTP à partir du cache. Lorsqu'elle est désactivée, Content Gateway joue le rôle de serveur proxy et transmet directement toutes les requêtes HTTP au serveur d'origine.
Caching (Mise en cache) : FTP over HTTP Caching (Mise en cache FTP sur HTTP)	Active ou désactive la mise en cache FTP sur HTTP. Lorsque cette option est activée, Content Gateway dessert les requêtes FTP issues de clients HTTP à partir du cache. Lorsqu'elle est désactivée, Content Gateway joue le rôle de serveur proxy et transmet directement toutes les requêtes FTP issues de clients HTTP au serveur FTP.

Option	Description
Behavior (Comportement) : Required Headers (En-têtes obligatoires)	Définit les informations d'en-tête minimales requises pour qu'un objet HTTP puisse être mis en cache. Sélectionnez **An Explicit Lifetime Header (Un en-tête de durée de vie explicite)** pour ne mettre en cache que les objets HTTP présentant des en-têtes **Expires ou max-age** Sélectionnez **A Last-Modified Header (Un en-tête de dernière modification)** pour ne mettre en cache que les objets HTTP présentant des en-têtes **lastmodified**. Sélectionnez **No Required Headers (Aucun en-tête obligatoire)** pour mettre en cache les objets HTTP qui ne présentent pas d'en-tête `Expires`, `max-age` ou `last-modified`. Il s'agit là de l'option par défaut. Attention : par défaut, Content Gateway met tous les objets en cache (y compris ceux sans en-tête). Nous vous recommandons de ne modifier cette configuration par défaut que dans les cas de proxy spéciaux. Si vous configurez Content Gateway pour qu'il ne mette en cache que les objets HTTP présentant des en-têtes **Expires** ou `max-age`, le taux d'accès fructueux au cache sera fortement réduit. En effet, très peu d'objets présentent des informations d'expiration explicites.
Behavior (Comportement) : When to Revalidate (Fréquence de revalidation)	Indique comment Content Gateway détermine le caractère récent d'un objet HTTP présent dans le cache : Sélectionnez **Never Revalidate (Ne jamais revalider)** pour ne jamais revalider les objets HTTP présents dans le cache via le serveur d'origine (Content Gateway considère que tous les objets HTTP du cache sont récents). Sélectionnez **Always Revalidate (Toujours revalider)** pour revalider systématiquement les objets HTTP présents dans le cache via le serveur d'origine (Content Gateway considère que tous les objets HTTP du cache sont périmés). Sélectionnez **Revalidate if Heuristic Expiration (Revalider en cas d'expiration heuristique)**pour vérifier le caractère récent d'un objet HTTP auprès du serveur d'origine lorsque cet objet ne contient pas d'en-tête `Expires` ou `Cache-Control`. Content Gateway considère tous les objets HTTP sans en-tête `Expires` ou `Cache-Control` comme périmés. Sélectionnez **Use Cache Directive or Heuristic (Utiliser les directives du cache ou les règles heuristiques)** pour vérifier le caractère récent d'un objet HTTP auprès du serveur d'origine lorsque Content Gateway considère l'objet présent dans le cache comme périmé en fonction de ses en-têtes, de sa limite d'actualité absolue et/ou des règles définies dans le fichier **cache.config**. Il s'agit là de l'option par défaut. Pour plus d'informations sur la revalidation, consultez la section *Revalidation des objets HTTP*, page 23.

Option	Description
Behavior (Comportement) : Add “no-cache” to MSIE Requests (Ajouter l’en-tête no-cache dans les requêtes MSIE)	Indique quand Content Gateway doit ajouter des en-têtes `no-cache` aux requêtes provenant de Microsoft Internet Explorer. Certaines versions de Microsoft Internet Explorer ne demandent pas un nouveau chargement du cache à partir des caches transparents lorsque l’utilisateur clique sur le bouton **Actualiser**. Il est ainsi possible que le contenu ne soit pas directement récupéré auprès des serveurs d’origine. Vous pouvez configurer Content Gateway pour qu’il traite les requêtes Microsoft Internet Explorer de façon plus prudente, en proposant un contenu plus récent, quitte à desservir moins de documents à partir du cache. Sélectionnez **To All MSIE Requests (Dans toutes les requêtes MSIE)** pour ajouter systématiquement des en-têtes `no-cache` à toutes les requêtes provenant de Microsoft Internet Explorer. Sélectionnez **To IMS MSIE Requests (Dans les requêtes MSIE IMS)** pour ajouter des en-têtes `no-cache` dans les requêtes Microsoft Internet Explorer IMS (If Modified Since, ou Si modifié depuis). Sélectionnez Not to Any MSIE Requests (Dans aucune requête MSIE) pour ne jamais ajouter d’en-tête `no-cache` aux requêtes provenant de Microsoft Internet Explorer.
Behavior (Comportement) : Ignore “no-cache” in Client Requests (Ignorer « no-cache » dans les requêtes des clients)	Lorsque cette option est activée, Content Gateway ignore les en-têtes `no-cache` présents dans les requêtes des clients et dessert les requêtes à partir du cache. Lorsqu’elle est désactivée, Content Gateway ne dessert pas les requêtes associées à des en-têtes `no-cache` à partir du cache, mais les transmet au serveur d’origine.
Freshness (Actualité) : Minimum Heuristic Lifetime (Durée de vie heuristique minimale)	Définit la durée minimale pendant laquelle un objet HTTP peut être considéré comme récent dans le cache
Freshness (Actualité) : Maximum Heuristic Lifetime (Durée de vie heuristique maximale)	Définit la durée maximale pendant laquelle un objet HTTP peut être considéré comme récent dans le cache
Freshness (Actualité) : FTP Document Lifetime (Durée de vie des documents FTP)	Définit la durée maximale pendant laquelle un fichier FTP pour rester dans le cache. Cette option affecte uniquement les requêtes FTP provenant de clients HTTP.
Maximum Alternates (Nombre maximal d’alternatives)	Définit le nombre maximal de versions alternatives d’un objet HTTP que Content Gateway peut mettre en cache. Attention : si vous saisissez 0 (zéro), le nombre d’alternatives pouvant être mises en cache n’est pas limité. Lorsqu’une URL populaire est associée à des milliers d’alternatives, les retards d’accès au cache peuvent se multiplier (délais de transaction), car Content Gateway recherche parmi les milliers d’alternatives pour chaque requête. Certaines URL peuvent notamment présenter un grand nombre d’alternatives du fait des cookies. Si Content Gateway est configuré pour varier en fonction des cookies, vous pouvez rencontrer ce problème.

Option	Description
Vary Based on Content Type (Varie en fonction du type de contenu) : Activer/Désactiver	Active ou désactive la mise en cache des versions alternatives des documents HTTP qui ne contiennent pas l'en-tête **Vary**. En l'absence de l'en-tête **Vary**, Content Gateway varie en fonction des en-têtes définis ci-dessous, selon le type de contenu du document.
Vary by Default on Text (Varie par défaut pour le texte)	Définit le champ d'en-tête en fonction duquel Content Gateway varie pour les documents de type texte
Vary by Default on Images (Varie par défaut pour les images)	Définit le champ d'en-tête en fonction duquel Content Gateway varie pour les images
Vary by Default on Other Document Types (Varie par défaut pour les autres types de documents)	Définit le champ d'en-tête en fonction duquel Content Gateway varie pour les éléments qui ne correspondent ni à du texte ni à des images
Dynamic Caching (Mise en cache du contenu dynamique) : Caching Documents with Dynamic URLs (Mise en cache des documents présentant des URL dynamiques)	Lorsque cette option est activée, Content Gateway tente de mettre en cache le contenu dynamique. Le contenu est considéré comme dynamique lorsqu'il contient un point d'interrogation (?), un point-virgule (;), **cgi**, ou lorsqu'il se termine par **.asp**. Attention : il est recommandé de ne configurer Content Gateway pour qu'il mette en cache le contenu dynamique que dans des cas de proxy particuliers.
Dynamic Caching (Mise en cache du contenu dynamique) : Caching Response to Cookies (Mise en cache des réponses dans des cookies)	Définit le mode de mise en cache des réponses aux requêtes contenant des cookies : Sélectionnez **Cache All but Text (Tout mettre en cache sauf le texte)** pour mettre en cache les cookies qui contiennent tout type de contenu à l'exception du texte. Il s'agit là du paramètre par défaut. Sélectionnez **Cache Only Image Types (Mettre en cache les types Image uniquement)** pour ne mettre en cache que les cookies contenant des images. Sélectionnez **Cache Any Content-Type (Mettre en cache tous les types de contenu)** pour mettre en cache les cookies, quel que soit leur contenu. Sélectionnez **No Cache on Cookies (Aucun cache pour les cookies)** pour ne pas mettre en cache les cookies du tout.
Caching Policy/Forcing Document Caching (Stratégie de mise en cache/Mise en cache obligatoire des documents)	Présente un tableau répertoriant les règles définies dans le fichier **cache.config** pour définir le mode de mise en cache d'un groupe d'URL particulier. Ce fichier vous permet également d'imposer la mise en cache de certaines URL pendant une période définie.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **cache.config**. Après avoir ajouté ou modifié des règles dans l'éditeur de fichiers de configuration, cliquez sur **Actualiser**.
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **cache.config**.

Option	Description
	Éditeur de fichiers de configuration pour le fichier cache.config
Champ d'affichage des règles	Répertorie les règles du fichier **cache.config**. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Rule Type (Type de règle)	Répertorie le type de règles que vous pouvez ajouter dans le fichier **cache.config** : Une règle de non mise en cache (**never-cache**) indique à Content Gateway de ne jamais mettre en cache les objets spécifiés. Une règle **ignore-no-cache** indique à Content Gateway d'ignorer tous les en-têtes **Cache-Control: no-cache**. Une règle **ignore-client-no-cache** indique à Content Gateway d'ignorer tous les en-têtes **Cache-Control: no-cache** des requêtes des clients. Une règle **ignore-server-no-cache** indique à Content Gateway d'ignorer tous les en-têtes **Cache-Control: no-cache** des réponses des serveurs d'origine. Une règle **pin-in-cache** indique à Content Gateway de conserver les objets dans le cache pendant un temps défini. Une règle de revalidation (**revalidate**) indique à Content Gateway de considérer les objets présents dans le cache comme récents pendant un temps défini. Une règle **ttl-in-cache** indique à Content Gateway de desservir certains objets HTTP à partir du cache pendant la période définie dans le champ **Time Period (Période)**, quelles que soient les directives de mise en cache indiquées dans les en-têtes des requêtes HTTP et des réponses.
Primary Destination Type (Type de destination principale)	Répertorie les différents types de destinations principales : **dest_domain** : nom du domaine demandé **dest_host** : nom d'hôte demandé **dest_ip** : adresse IP demandée **url_regex** : expression régulière que l'on retrouve dans une URL
Primary Destination Value (Valeur de la destination principale)	Définit la valeur du type de destination principale. Par exemple, si le type de destination principale est **dest_ip**, la valeur de ce champ peut être 123.456.78.9.
Additional Specifier (Autre spécificateur) : Time Period (Période)	Définit la durée d'application des types de règles **revalidate**, **pin-in-cache** et **ttl-in-cache**. Les formats disponibles sont les suivants : **d** pour jours (days) (par exemple, 2d) **h** pour heures (par exemple, 10h) **m** pour minutes (par exemple, 5m) **s** pour secondes (par exemple, 20s) Combinaison des unités (par exemple, 1h15m20s)

Option	Description
Secondary Specifiers (Spécificateurs secondaires) : Heure	Définit une plage horaire, par exemple 08:00 à 14:00
Secondary Specifiers (Spécificateurs secondaires) : Préfixe	Définit un préfixe situé dans le chemin d'une URL
Secondary Specifiers (Spécificateurs secondaires) : Suffixe	Définit un suffixe de fichier dans l'URL
Secondary Specifiers (Spécificateurs secondaires) : IP source	Définit l'adresse IP du client
Secondary Specifiers (Spécificateurs secondaires) : Port	Définit le port dans une URL demandée
Secondary Specifiers (Spécificateurs secondaires) : Méthode	Définit une méthode d'URL de requête
Secondary Specifiers (Spécificateurs secondaires) : Scheme (Schéma)	Définit le protocole d'une URL demandée
Secondary Specifiers (Spécificateurs secondaires) : User-Agent	Définit la valeur User-Agent de l'en-tête de la requête
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
	Confidentialité
Insert Headers (Insérer des en-têtes) : Client-IP	Lorsque cette option est activée, Content Gateway insère l'en-tête **Client-IP** dans les requêtes sortantes pour conserver l'adresse IP du client.
Insert Headers (Insérer des en-têtes) : Via	Lorsque cette option est activée, Content Gateway insère un en-tête **Via** dans la requête sortante.
Insert Headers (Insérer des en-têtes) : X-Forwarded-For	Lorsque cette option est activée, Content Gateway insère un en-tête **X-Forwarded-For** dans la requête sortante.
Remove Headers (Supprimer des en-têtes) : Client-IP	Lorsque cette option est activée, Content Gateway supprime l'en-tête **Client-IP** dans les requêtes sortantes pour préserver la confidentialité de vos utilisateurs.
Remove Headers (Supprimer des en-têtes) : Cookie	Lorsque cette option est activée, Content Gateway supprime l'en-tête **Cookie** dans les requêtes sortantes pour préserver la confidentialité de vos utilisateurs. L'en-tête **Cookie** permet généralement d'identifier l'utilisateur à l'origine de la requête.
Remove Headers (Supprimer des en-têtes) : From	Lorsque cette option est activée, Content Gateway supprime l'en-tête **From** dans les requêtes sortantes pour préserver la confidentialité de vos utilisateurs. L'en-tête **From** identifie l'adresse électronique du client.

Option	Description
Remove Headers (Supprimer des en-têtes) : Referer	Lorsque cette option est activée, Content Gateway supprime l'en-tête **Referer** dans les requêtes sortantes pour préserver la confidentialité de vos utilisateurs. L'en-tête **Referer** identifie le lien Web sélectionné par le client.
Remove Headers (Supprimer des en-têtes) : User-Agent	Lorsque cette option est activée, Content Gateway supprime l'en-tête **User-Agent** dans les requêtes sortantes pour préserver la confidentialité de vos utilisateurs. L'en-tête **User-Agent** identifie l'agent à l'origine de la demande, en général un navigateur.
Remove Headers (Supprimer des en-têtes) : Remove Others (Autres retraits)	Définit les en-têtes, autres que **From**, **Referer**, **User-Agent** et **Cookie**, que vous souhaitez retirer des requêtes sortantes afin de préserver la confidentialité de vos utilisateurs.
	Délais d'expiration
Keep-Alive Timeouts (Expirations Maintenir la connexion) : Client	Définit (en secondes) la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux clients en vue de la requête suivante après la fin d'une transaction. Chaque fois que Content Gateway ouvre une connexion pour accepter la requête d'un client, il traite la requête, puis maintient la connexion pendant la durée spécifiée. Si le client n'envoie pas d'autres requêtes avant la fin du délai d'expiration, Content Gateway ferme la connexion. Si le client envoie une autre requête, le délai d'expiration reprend au début. Le client peut fermer la connexion à tout moment.
Keep-Alive Timeouts (Expirations Maintenir la connexion) : Serveur d'origine	Définit (en secondes) la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux serveurs d'origine en vue du prochain transfert de données après la fin d'une transaction. Chaque fois que Content Gateway ouvre une connexion pour télécharger des données à partir d'un serveur d'origine, il télécharge les données, puis maintient la connexion pendant la durée spécifiée. Si Content Gateway n'a pas besoin d'envoyer d'autres demandes de données avant la fin du délai d'expiration, il ferme la connexion. Dans le cas contraire, le délai d'expiration reprend au début. Le serveur d'origine peut fermer la connexion à tout moment.
Inactivity Timeouts (Délais d'inactivité) : Client	Définit la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux clients lorsqu'une transaction est périmée. Si Content Gateway ne reçoit plus de données du client ou si le client cesse de lire les données, Content Gateway ferme la connexion à la fin de ce délai. Le client peut fermer la connexion à tout moment.
Inactivity Timeouts (Délais d'inactivité) : Serveur d'origine	Définit la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux serveurs d'origine lorsqu'une transaction est périmée. Si Content Gateway ne reçoit plus de données du serveur d'origine, il ne ferme pas la connexion avant l'expiration de ce délai. Le serveur d'origine peut fermer la connexion à tout moment.
Active Timeouts (Délais d'activité) : Client	Spécifie la durée pendant laquelle Content Gateway doit rester connecté à un client. Si le client ne termine pas une requête (lecture et écriture des données) avant l'expiration de ce délai, Content Gateway ferme la connexion. La valeur par défaut, 0 (zéro), indique qu'il n'y a pas de délai d'expiration. Le client peut fermer la connexion à tout moment.

Option	Description
Active Timeouts (Délais d'activité) : Origin Server Request (Requête du serveur d'origine)	Spécifie la durée pendant laquelle Content Gateway doit attendre que la demande de connexion à un serveur d'origine soit satisfaite. Si Content Gateway n'établit pas la connexion au serveur d'origine avant l'expiration de ce délai, il met fin à la demande de connexion. La valeur par défaut, 0 (zéro), indique qu'il n'y a pas de délai d'expiration. Le serveur d'origine peut fermer la connexion à tout moment.
Active Timeouts (Délais d'activité) : Origin Server Response (Réponse du serveur d'origine)	Définit la durée pendant laquelle Content Gateway doit attendre une réponse du serveur d'origine
FTP Control Connection Timeout (Expiration de la connexion de contrôle FTP)	Définit la durée pendant laquelle Content Gateway doit attendre une réponse d'un serveur FTP. Si le serveur FTP ne répond pas pendant le délai spécifié, Content Gateway abandonne la requête de données du client. Cette option affecte uniquement les requêtes FTP provenant de clients HTTP. La valeur par défaut est 300.

Réponses HTTP

Option	Description
	Général
Response Suppression Mode (Mode Suppression de réponse)	Lorsque Content Gateway détecte un problème HTTP pour une transaction de client (par exemple des serveurs d'origine non disponibles, des exigences d'authentification et des erreurs de protocole), il envoie une réponse HTML au navigateur client. Content Gateway dispose d'un jeu de pages de réponse par défaut codées en dur détaillant chaque erreur HTTP au client. Sélectionnez **Always Suppressed (Toujours supprimer)** si vous ne voulez pas envoyer de réponse HTTP aux clients. Sélectionnez **Intercepted Traffic Only (Trafic intercepté uniquement)** pour envoyer des réponses HTTP au trafic non transparent uniquement. (Cette option est utile lorsque Content Gateway s'exécute en transparence et que vous ne voulez pas signaler la présence d'un cache.) Sélectionnez **Never Suppressed (Ne jamais supprimer)** si vous voulez envoyer des réponses HTTP à tous les clients. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Option	Description
	Personnalisé
Custom Responses (Réponses personnalisées)	Vous pouvez personnaliser les réponses que Content Gateway envoie aux clients. Par défaut, les réponses personnalisables sont situées dans le répertoire **config/body_factory/default** de Content Gateway. Sélectionnez **Enabled Language-Targeted Response (Réponse dans la langue cible)** pour envoyer aux clients des réponses personnalisées dans la langue définie dans l'en-tête `Accept-Language`. Sélectionnez **Enabled in "default" Directory Only (Réponses du répertoire par défaut uniquement)** pour envoyer aux clients les réponses personnalisées stockées dans le répertoire par défaut. Sélectionnez **Disabled (Désactivé)** pour désactiver les réponses personnalisées. Lorsque l'option **Never Suppressed (Ne jamais supprimer)** ou **Intercepted Traffic Only (Trafic intercepté uniquement)** est sélectionnée pour l'option **Response Suppression Mode (Mode Suppression de réponse)**, Content Gateway envoie les réponses par défaut codées en dur. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Custom Response Logging (Journalisation des réponses personnalisées)	Lorsque cette option est activée, Content Gateway envoie systématiquement un message au journal d'erreurs lorsque des réponses personnalisées sont utilisées ou modifiées. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Custom Response Template Directory (Répertoire des modèles de réponses personnalisées)	Définit le répertoire de stockage des réponses personnalisées. L'emplacement par défaut est le répertoire **config/body_factory** de Content Gateway. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

HTTP Scheduled Update (HTTP - Mise à jour planifiée)

Option	Description
	Général
Scheduled Update (Mise à jour planifiée)	Active ou désactive l'option de mise à jour planifiée. Lorsque cette option est activée, Content Gateway peut actualiser automatiquement certains objets du cache local au moment indiqué.
Maximum Concurrent Updates (Mises à jour simultanées maximales)	Définit le nombre maximal de demandes de mise à jours simultanées autorisées à tout moment. Cette option vous permet d'éviter que le processus de mise à jour planifiée ne surcharge l'hôte. La valeur par défaut est 100.
Retry on Update Error (Nouvelle tentative en cas d'erreur de mise à jour) : Count (Nombre)	Définit le nombre de nouvelles tentatives de mises à jour d'une URL que Content Gateway peut effectuer en cas d'échec. La valeur par défaut est 10.

Option	Description
Retry on Update Error (Nouvelle tentative en cas d'erreur de mise à jour) : Intervalle	Définit le délai (en secondes) devant s'écouler entre chaque nouvelle tentative de mise à jour d'une URL en cas d'échec. La valeur par défaut est 2 secondes.
	Mise à jour des URL
Force Immediate Update (Imposer une mise à jour immédiate)	Lorsque cette option est activée, Content Gateway ignore le délai d'expiration de planification pour toutes les entrées de mise à jour planifiées et déclenche des mises à jour toutes les 25 secondes.
Scheduled Object Update (Mise à jour planifiée des objets)	Présente un tableau répertoriant les règles du *Fichier de configuration update.config* qui indiquent à Content Gateway comment effectuer la mise à jour planifiée du contenu d'un cache local spécifique
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **update.config**
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **update.config**
	Éditeur de fichiers de configuration pour le fichier update.config
Champ d'affichage des règles	Répertorie les règles du fichier **update.config**. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
URL	Définit l'URL à mettre à jour
Request Headers (En-têtes des requêtes) (facultatif)	Définit la liste des en-têtes (séparés par des points-virgules) transmis dans chaque requête `GET`. Vous pouvez définir tout en-tête de requête respectant les spécifications du protocole HTTP. Le paramètre par défaut consiste à ne pas utiliser d'en-tête de requête.
Offset Hour (Heure de décalage)	Définit l'heure de base à partir de laquelle découlent les périodes de mise à jour. La plage est 00-23 heures.
Intervalle	Intervalle, en secondes, selon lequel les mises à jour doivent être effectuées, à partir de l'heure de décalage
Recursion Depth (Profondeur de récursion)	Profondeur à laquelle les URL référencées sont mises à jour de façon récursive, à partir de l'URL donnée. Par exemple, une profondeur récursive de 1 met à jour l'URL donnée, ainsi que toutes les URL immédiatement référencées par les liens de l'URL d'origine.

HTTPS

Option	Description
	Général
HTTPS Proxy Server Port (Port du serveur proxy HTTPS)	Définit le port utilisé par Content Gateway lorsqu'il joue le rôle de serveur proxy Web pour le trafic HTTPS. Ce paramètre est également appelé SSL Inbound Port (Port entrant SSL).
SSL Outbound Port (Port sortant SSL)	Définit le port HTTPS par lequel passe le trafic afin d'être recrypté avant d'être envoyé à destination. La valeur par défaut est 8090.
Tunnel Skype	Active/désactive la mise en tunnel du trafic Skype lorsque HTTPS (SSL Manager) est activé et que Content Gateway est un proxy explicite. **Pour terminer la configuration**, vous devez vous assurer que tous les utilisateurs autorisés à se servir de Skype disposent d'une stratégie de filtrage autorisant la **téléphonie Internet**. Cette option est obligatoire pour l'utilisation de Skype, que SSL Manager soit activé ou non. Par ailleurs, s'il n'en est pas empêché, Skype acheminera le trafic vers un port non HTTP après la négociation. Pour obliger le trafic Skype à passer par Content Gateway, un Objet de stratégie de groupe (GPO) doit être utilisé conformément à la description donnée dans le Guide de l'administrateur Skype. **Remarque :** cette option n'est pas nécessaire lorsque SSL n'est pas activé. **Remarque :** cette option n'est pas valide lorsque Content Gateway est un proxy transparent.

FTP

> **Remarque**
> Les options de configuration FTP ne s'affichent dans le volet de configuration que si vous avez activé le traitement FTP dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Option	Description
	Général
FTP Proxy Server Port (Port du serveur proxy FTP)	Définit le port utilisé par Content Gateway pour accepter les requêtes FTP. Le port par défaut est le 2121.

Option	Description
Listening Port Configuration (Configuration du port d'écoute)	Indique comment FTP ouvre un port d'écoute pour le transfert de données. Sélectionnez **Default Settings (Paramètres par défaut)** pour laisser le système d'exploitation choisir un port disponible. Content Gateway envoie 0 et récupère le nouveau numéro de port si l'écoute réussit. Sélectionnez **Specify Range (Spécifier une plage)** si vous souhaitez que le port d'écoute soit déterminé en fonction de la plage de ports spécifiée dans les champs **Listening Port (Port d'écoute) (Maxi)** et **Listening Port (Port d'écoute) (Mini)**.
Default Data Connection Method (Méthode de connexion de données par défaut)	Définit la méthode utilisée par défaut pour configurer les connexions de données au serveur FTP. Sélectionnez **Proxy Sends PASV (Le proxy envoie PASV)** pour envoyer un PASV au serveur FTP et laisser ce dernier ouvrir un port d'écoute. Sélectionnez **Proxy Sends PORT (Le proxy envoie PORT)** pour configurer un port d'écoute sur le côté Content Gateway de la connexion d'abord.
Shared Server Connections (Connexions de serveurs partagées)	Lorsque cette option est activée, les connexions de contrôle des serveurs peuvent être partagées entre plusieurs clients FTP anonymes.
	Délais d'expiration
Keep-Alive Timeouts (Expirations Maintenir la connexion) : Server Control (Contrôle des serveurs)	Définit la valeur d'expiration lorsque la connexion de contrôle des serveurs FTP n'est utilisée par aucun client FTP. La valeur par défaut est 90 secondes.
Inactivity Timeouts (Délais d'inactivité) : Client Control (Contrôle des clients)	Définit le délai pendant lequel les connexions de contrôle des clients FTP peuvent rester inactives. La valeur par défaut est 900 secondes.
Inactivity Timeouts (Délais d'inactivité) : Server Control (Contrôle des serveurs)	Définit le délai pendant lequel la connexion de contrôle des serveurs FTP peut rester inactive. La valeur par défaut est 120 secondes.
Active Timeouts (Délais d'activité) : Client Control (Contrôle des clients)	Définit le délai pendant lequel les connexions de contrôle des clients FTP peuvent rester ouvertes. La valeur par défaut est 14 400 secondes.
Active Timeouts (Délais d'activité) : Server Control (Contrôle des serveurs)	Définit le délai pendant lequel la connexion de contrôle des serveurs FTP peut rester ouverte. La valeur par défaut est 14 400 secondes.

Routage du contenu

Les options de configuration du routage du contenu se répartissent dans les catégories suivantes :

Hiérarchies, page 290

Mappage et redirection, page 293

Auto-configuration du navigateur, page 295

Hiérarchies

Option	Description
	Parenting (Parentalité)
Parent Proxy (Proxy parent)	Active ou désactive l'option de mise en cache des parents HTTP. Lorsque cette option est activée, Content Gateway peut participer à une hiérarchie de caches HTTP. Vous pouvez configurer votre serveur Content Gateway pour qu'il pointe vers un cache réseau parent (soit un autre serveur Content Gateway, soit un autre produit de mise en cache) pour établir une hiérarchie de caches au sein de laquelle un cache enfant compte sur un cache parent pour satisfaire les demandes des clients. Voir *Hiérarchies de caches HTTP*, page 85.
No DNS and Just Forward to Parent (Pas de recherche DNS et transmission au parent seulement)	Lorsque cette option est activée, de même que la mise en cache des parents HTTP, Content Gateway n'effectue pas de recherches DNS sur les noms d'hôte demandés. Si des règles du fichier **parent.config** indiquent que seules les requêtes sélectionnées doivent être envoyées à un proxy parent, Content Gateway ignore uniquement la résolution de nom pour les requêtes destinées au proxy parent. Pour les requêtes non destinées à un proxy parent, la résolution de nom s'effectue de la manière habituelle. Si le proxy parent est inactif et que le proxy enfant peut accéder directement aux serveurs d'origine, l'enfant effectue la résolution DNS.
Uncacheable Requests Bypass Parent (Les requêtes ne pouvant pas être mises en cache ignorent le proxy parent)	Si cette option est activée, de même que la mise en cache du parent, Content Gateway ignore le proxy parent pour les requêtes qui ne peuvent pas être mises en cache.
HTTPS Requests Bypass Parent (Les requêtes HTTPS ignorent le proxy parent)	Lorsque cette option est activée, Content Gateway ignore le proxy parent pour les requêtes HTTPS.
Tunnel Requests Bypass Parent (Les requêtes mises en tunnel ignorent le proxy parent)	Lorsque cette option est activée, Content Gateway ignore le proxy parent pour les requêtes non HTTPS mises en tunnel.

Option	Description
Parent Proxy Cache Rules (Règles des caches de proxy parents)	Présente un tableau répertoriant les règles du *Fichier de configuration parent.config* qui identifient les proxy HTTP parents utilisés dans une hiérarchie de caches HTTP et configurent les requêtes d'URL sélectionnées pour qu'elles ignorent les proxy parents. Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas. La première correspondance étant appliquée en premier.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **parent.config**.
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **parent.config**
	Éditeur de fichiers de configuration pour le fichier parent.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration parent.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Primary Destination Type (Type de destination principale)	Répertorie les différents types de destinations principales : **dest_domain** : nom du domaine demandé **dest_host** : nom d'hôte demandé **dest_ip** : adresse IP demandée **url_regex** : expression régulière que l'on retrouve dans une URL
Primary Destination Value (Valeur de la destination principale)	Définit la valeur du type de destination principale. Par exemple : Si la destination principale est **dest_domain**, la valeur de ce champ peut être yahoo.com. Si le type de destination principale est **dest_ip**, la valeur de ce champ peut être 123.456.78.9. Si la destination principale est **url_regex**, la valeur de ce champ peut être une stratégie.
Parent Proxies (Proxy parents)	Définit les adresses IP ou les noms d'hôte des proxy parents et les numéros de port utilisés pour leurs communications. Les proxy parents sont interrogés selon leur ordre d'apparition dans la liste. Lorsque la requête ne peut pas être traitée par le dernier serveur parent de la liste, elle est acheminée vers le serveur d'origine. Séparez chaque entrée par un point-virgule. Par exemple : **parent1:8080**; **parent2:8080**
Round Robin (Recherche circulaire)	Sélectionnez **true** pour que le proxy effectue une recherche circulaire basée sur l'adresse IP du client dans la liste des caches parents. Sélectionnez **strict** pour que le proxy desserve strictement les requêtes dans leur ordre d'arrivée. Par exemple, l'ordinateur proxy1 dessert la première requête, proxy2 dessert la seconde, etc. Sélectionnez **false** lorsque vous ne voulez effectuer aucune recherche circulaire.

Option	Description
Go direct (Envoi direct)	Sélectionnez **true** pour que les requêtes ignorent les hiérarchies parentes et soient envoyées directement au serveur d'origine. Sélectionnez **false** pour que les requêtes n'ignorent pas les hiérarchies parentes.
Secondary Specifiers (Spécificateurs secondaires) : Heure	Définit une plage horaire (sur 24 heures), telle que 08:00-14:00. Si la plage va au-delà de minuit, saisissez-la sous forme de deux plages séparées par une virgule. Par exemple, lorsqu'une plage va de 18:00 à 8:00 le lendemain matin, saisissez les plages suivants : `18:00 - 23:59, 0:00 - 8:00`
Secondary Specifiers (Spécificateurs secondaires) : Préfixe	Définit un préfixe situé dans le chemin d'une URL
Secondary Specifiers (Spécificateurs secondaires) : Suffixe	Définit un suffixe de fichier dans l'URL, par exemple .htm ou .gif
Secondary Specifiers (Spécificateurs secondaires) : IP source	Définit l'adresse IP ou la plage d'adresses IP des clients
Secondary Specifiers (Spécificateurs secondaires) : Port	Définit le port dans une URL demandée
Secondary Specifiers (Spécificateurs secondaires) : Méthode	Définit une méthode d'URL de requête. Par exemple : • `get` • `post` • `put` • `trace`
Secondary Specifiers (Spécificateurs secondaires) : Scheme (Schéma)	Définit le protocole d'une URL demandée. Ce doit être HTTP ou FTP.
Secondary Specifiers (Spécificateurs secondaires) : User-Agent	Définit la valeur User-Agent de l'en-tête de la requête

Mappage et redirection

Option	Description
Serve Mapped Hosts Only (Desservir les hôtes mappés uniquement)	Sélectionnez **Required (Obligatoire)** pour que le proxy n'envoie les requêtes qu'aux serveurs d'origine répertoriés dans les règles de mappage du *Fichier de configuration remap.config*. Lorsque la requête ne correspond à aucune règle du fichier **remap.config**, le navigateur reçoit une erreur. Cette option renforce la sécurité de votre système Content Gateway.
Retain Client Host Header (Conserver l'en-tête de l'hôte du client)	Lorsque cette option est activée, Content Gateway conserve l'en-tête de l'hôte du client indiqué dans la requête (sans l'inclure dans la traduction du mappage).
Redirect No-Host Header to URL (Rediriger les requêtes sans en-tête d'hôte)	Définit l'URL alternative vers laquelle les requêtes entrantes provenant d'anciens clients qui ne fournissent pas d'en-tête `Host:` doivent être acheminées. Nous vous conseillons de définir cette option sur une page qui explique la situation à l'utilisateur et qui l'invite à mettre son navigateur à niveau ou qui propose un lien conduisant directement au serveur d'origine, en ignorant le proxy. Vous pouvez également spécifier une règle de mappage associant les requêtes qui ne présentent pas d'en-tête `Host:` à un serveur particulier.
URL Remapping Rules (Règles de remappage des URL)	Présente un tableau répertoriant les règles de mappage définies dans le fichier **remap.config** qui vous permet de rediriger définitivement ou temporairement les requêtes HTTP, sans que le proxy n'ait besoin de contacter les serveurs d'origine. **Remarque :** le mappage d'une URL vers une autre URL du même domaine implique que le caractère « / » soit spécifié dans le champ **From Path Prefix (Préfixe DE du chemin)**. Reportez-vous à l'exemple qui suit ce tableau.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **remap.config**
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **remap.config**
	Éditeur de fichier de configuration pour le fichier remap.config
Champ d'affichage des règles	Répertorie les règles du fichier **remap.config**. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration

Option	Description
Rule Type (Type de règle)	Répertorie le type de règles que vous pouvez ajouter dans le fichier `remap.config` : **redirect** dirige définitivement les requêtes HTTP sans que le serveur d'origine n'ait besoin d'être contacté. Les redirections permanentes signalent la modification d'URL au navigateur (en renvoyant l'état HTTP de code 301) pour que celui-ci puisse mettre à jour les signets. **redirect_temporary** redirige temporairement les requêtes HTTP sans que le serveur d'origine n'ait besoin d'être contacté. Les redirections temporaires signalent la modification d'URL au navigateur pour la requête en cours uniquement (en renvoyant l'état HTTP de code 307).
From Scheme (Schéma From)	Définit le protocole de la règle de mappage. Les protocoles « rtsp » et « mms » ne sont **pas** pris en charge. **Remarque :** le mappage d'une URL d'un protocole (schéma) avec un autre protocole (schéma) n'est pas pris en charge.
From Host (Hôte From)	Définit le nom d'hôte de l'URL à partir duquel le mappage doit être effectué
From Port (Port From) (facultatif)	Définit le numéro de port de l'URL à partir duquel le mappage doit être effectué
From Path Prefix (Préfixe From du chemin) (facultatif)	Définit le préfixe du chemin de l'URL à partir duquel le mappage doit être effectué
To Host (Hôte To)	Définit le nom d'hôte de l'URL avec lequel le mappage doit être effectué
To Port (Port To) (facultatif)	Définit le numéro de port de l'URL avec lequel le mappage doit être effectué
From Path Prefix (Préfixe To du chemin) (facultatif)	Définit le préfixe du chemin de l'URL vers lequel le mappage doit être effectué
{undefined} ({non défini})	Définit le type de protocole de média de la règle de mappage. Non pris en charge.

Il est parfois préférable de rediriger une URL vers une sous-page du même domaine. Par exemple, « www.cnn.com » peut être redirigé vers « www.cnn.com/tech ». Pour que cette règle fonctionne, vous devez spécifier le caractère « / » dans le champ **From Path Prefix (Préfixe From du chemin)**. Si ce caractère n'est pas spécifié, la redirection résulte en une URL qui ajoute récursivement le spécificateur de la page dans l'URL. Par exemple, « www.cnn.com/tech » devient dans ce cas « www.cnn.com/tech/tech/tech/tech/tech/tech/tech/tech/... ».

Auto-configuration du navigateur

Option	Description
	PAC
Auto-Configuration Port (Port d'auto-configuration)	Définit le port utilisé par Content Gateway pour télécharger le fichier d'auto-configuration vers les navigateurs. Ce port ne peut pas être affecté à un autre processus. Le port par défaut est le 8083. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
PAC Settings (Paramètres PAC)	Permet de modifier le fichier PAC (**proxy.pac**). Voir *Utilisation d'un fichier PAC*, page 40.
	WPAD
WPAD Settings (Paramètres WPAD)	Permet de modifier le fichier **wpad.dat**. Voir *Utilisation du protocole WPAD*, page 42.

Sécurité

Les options de configuration de la sécurité se répartissent dans les catégories suivantes :

Contrôle des connexions

Option	Description
	Accès au proxy
Contrôle d'accès	Affiche les règles du *Fichier de configuration ip_allow.config* qui identifient les clients pouvant accéder à Content Gateway Par défaut, tous les hôtes distants sont autorisés à accéder au proxy.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **ip_allow.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **ip_allow.config** dans l'éditeur de fichiers de configuration

Option	Description
	Éditeur de fichiers de configuration pour le fichier ip_allow.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration ip_allow.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
IP Action (Action IP)	Répertorie le type de règles pouvant être ajoutées. Une règle **ip_allow** permet aux clients répertoriés dans le champ IP source d'accéder au proxy. Une règle **ip_deny** interdit aux clients répertoriés dans le champ IP source d'accéder au proxy.
IP source	Définit l'adresse IP ou la plage d'adresses IP des clients
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

Sécurité FIPS

Cette option concerne le trafic HTTPS et la norme cryptographique FIPS 140-2.

Par défaut, lorsqu'il gère le trafic HTTPS, Content Gateway accepte les connexions provenant de sites qui utilisent des protocoles tels que SSLv2 et SSLv3.

Activez l'option FIPS pour que Content Gateway accepte uniquement les connexions HTTPS qui utilisent TLSv1 et les algorithmes FIP 140-2 approuvés.

Avertissement

Une fois activé, le mode FIPS 140-2 ne peut plus être désactivé sans que Content Gateway ne soit réinstallé. Si Content Gateway est installé sur un dispositif, ce dernier doit être réimagé.

Pour plus d'informations, consultez la section *Mode FIPS 140-2*, page 167.

Option	Description
Boutons radios FIPS Enable/Disable (Activer/ Désactiver FIPS)	Par défaut, Content Gateway n'est pas installé en mode FIPS 140-2. Pour passer en mode FIPS 140-2, activez le bouton radio **Enabled (Activé)**, cliquez sur **Appliquer**, puis redémarrez Content Gateway. **Remarque :** une fois activé, le mode FIPS 140-2 ne peut plus être désactivé sans que Content Gateway ne soit réinstallé. Dans le cas des installations sur dispositif Websense, la réinstallation implique que le système soit réimagé.

Data Security

Remarque

Les options de configuration de Data Security s'affichent dans le volet Configurer dans les cas suivants uniquement :

- Vous disposez d'un abonnement Web Security Gateway Anywhere et la clé a été saisie dans TRITON – Web Security.
- Data Security est activé dans l'onglet **Configurer > Mon proxy > De base > Général** et l'option **Integrated on-box (Intégration prête à l'emploi)** est activée dans le tableau **Features (Fonctions)**.

Option	Description
Data Security IP address (Adresse IP de Data Security)	Définit l'adresse IP du serveur de gestion de Data Security. C'est là que s'effectue la gestion et la configuration des stratégies de Websense Data Security.
Analyze HTTPS Content (Analyser le contenu HTTPS)	Indiquez si le trafic décrypté doit être envoyé à Websense Data Security Suite pour analyse ou envoyé directement à destination.
Analyze FTP Uploads (Analyser les chargements FTP)	Indiquez si les requêtes de chargement FTP doivent être envoyées à Websense Data Security pour analyse. La fonction de proxy FTP doit être activée. Voir *FTP*, page 288.

Champs de l'écran d'enregistrement :

Option	Description
Data Security IP address (Adresse IP de Data Security)	Définit l'adresse IP du serveur de gestion de Data Security. C'est là que s'effectue la gestion et la configuration des stratégies de sécurité des données.
Data Security Manager user name (Nom d'utilisateur Data Security Manager)	Définit le nom du compte d'un administrateur Websense Data Security. L'administrateur doit être autorisé à déployer des paramètres.
Data Security Manager user name (Nom d'utilisateur Data Security Manager)	Définit le mot de passe de l'administrateur Websense Data Security
Bouton Register (Enregistrement)	Lance l'opération d'enregistrement. Ce bouton s'active uniquement lorsque tous les champs ont été renseignés.

Contrôle d'accès

Servez-vous des onglets du contrôle d'accès pour :

- Créer des règles de filtrage personnalisées
- Configurer l'authentification des utilisateurs du proxy

L'onglet *Filtrage* est toujours disponible dans la page **Access Control (Contrôle d'accès)**.

L'onglet *Authentification du proxy transparent* n'est pas toujours présent, mais ne s'active que si Content Gateway est déployé en tant que proxy transparent.

Les autres onglets sont dynamiques et dépendent de la méthode d'authentification sélectionnée dans la section **Authentification** de la page **Configurer > Mon proxy**.

Lorsque l'*Authentification Windows intégrée* est sélectionnée, les onglets suivants s'affichent :

- **Authentification Windows intégrée**
- **Global Authentication Options (Options d'authentification globales)** (s'appliquent à l'authentification NTLM)

Lorsque l'authentification *LDAP* est sélectionnée, l'onglet suivant s'affiche :

- **LDAP**

Lorsque l'authentification *Radius* est sélectionnée, l'onglet suivant s'affiche :

- **Radius**

Lorsque l'*Authentification NTLM héritée* est sélectionnée, l'onglet suivant s'affiche :

- **NTLM**

Lorsque l'*Authentification dans plusieurs domaines Kerberos* est sélectionnée, les onglets suivants s'affichent :

- **Domaines**
- **Authentication Realms (Authentification des domaines Kerberos)**
- **Global Authentication Options (Options d'authentification globales)**

Le tableau suivant décrit l'objectif des champs de chaque onglet. Vous pouvez utiliser la fonction de recherche de votre navigateur pour localiser le champ recherché.

Vous trouverez la description complète des fonctions d'authentification des utilisateurs de Content Gateway à la section *Authentification des utilisateurs du proxy*, page 175.

Option	Description
	Filtrage
Filtering (Filtrage)	Affiche un tableau répertoriant les règles définies dans le *Fichier de configuration filter.config* Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas, la première correspondance étant appliquée en premier. Lorsque aucune règle ne correspond, la requête poursuit sa route. L'objectif des règles de filtrage est présenté en détail à la section *Règles de filtrage*, page 167. **Remarque :** lorsque vous ajoutez, supprimez ou modifiez une règle, redémarrez Content Gateway. **Remarque :** les règles d'authentification NTLM et LDAP sont définies dans l'onglet **Authentication Realms (Authentification des domaines Kerberos)** et stockées dans le *Fichier de configuration auth.config* (reportez-vous à l'entrée correspondante dans la suite de ce tableau).
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **filter.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **filter.config** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier filter.config
Champ d'affichage des règles	Répertorie les règles actuellement stockées dans le *Fichier de configuration filter.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration. Après la sélection ou la saisie des valeurs de la règle, cliquez sur Ajouter.
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration

Option	Description
Rule Type (Type de règle)	Définit le type de règles : Sélectionnez **allow (autoriser)** pour que certaines requêtes d'URL soient autorisées à ignorer l'authentification. Le proxy met en cache, puis envoie le contenu demandé. Sélectionnez **deny (refuser)** pour refuser les requêtes d'objets associées à des destinations spécifiques. Lorsqu'une requête est refusée, le client reçoit un message d'accès refusé. Sélectionnez **keep_hdr** pour définir les informations d'en-tête des requêtes de clients que vous souhaitez conserver. Sélectionnez **strip_hdr** pour définir les informations d'en-tête des requêtes de clients que vous souhaitez supprimer. Sélectionnez **add_hdr** pour qu'un en-tête personnalisé soit ajouté à la requête. Ce type de règles implique que les valeurs des options **Custom Header (En-tête personnalisé)** et **Header Value (Valeur de l'en-tête)** soient définies. L'ajout d'en-têtes personnalisés vous permet de répondre aux exigences spécifiques d'un domaine de destination. Voir *Règles de filtrage*, page 167. **Remarque :** le type de règle « radius » n'est pas pris en charge.
Primary Destination Type (Type de destination principale)	Répertorie les différents types de destinations principales : **dest_domain** : nom du domaine demandé **dest_host** : nom d'hôte demandé **dest_ip** : adresse IP demandée **url_regex** : expression régulière que l'on retrouve dans une URL
Primary Destination Value (Valeur de la destination principale)	Définit la valeur du type de destination principale. Par exemple, si le type de destination principale est **dest_ip**, la valeur de ce champ peut être 123.456.78.9.
Additional Specifiers (Autres spécificateurs) : Header Type (Type d'en-tête)	Définit les informations d'en-tête des requêtes de clients à conserver ou supprimer. Cette option ne concerne que les types de règles **keep_hdr** et **strip_hdr**.
Additional Specifiers (Autres spécificateurs) : Realm (Domaine Kerberos) (facultatif)	Non pris en charge
Additional Specifiers (Autres spécificateurs) : Proxy Port (Port du proxy) (facultatif)	Définit le port du proxy concerné par cette règle
Additional Specifiers (Autres spécificateurs) : Custom Header (En-tête personnalisé) (facultatif)	À utiliser avec le type de règle **add_hdr**. Définit le nom de l'en-tête personnalisé attendu par le domaine de destination dans la requête.
Additional Specifiers (Autres spécificateurs) : Header Value (Valeur de l'en-tête) (facultatif)	À utiliser avec le type de règle **add_hdr**. Définit la valeur de l'en-tête personnalisé qui, selon le domaine de destination, doit être associée à l'en-tête personnalisé.
Secondary Specifiers (Spécificateurs secondaires) : Heure	Définit une plage horaire, par exemple 08:00 à 14:00

Option	Description
Secondary Specifiers (Spécificateurs secondaires) : Préfixe	Définit un préfixe situé dans le chemin d'une URL
Secondary Specifiers (Spécificateurs secondaires) : Suffixe	Définit un suffixe de fichier dans l'URL
Secondary Specifiers (Spécificateurs secondaires) : IP source	Définit l'adresse IP du client
Secondary Specifiers (Spécificateurs secondaires) : Port	Définit le port dans une URL demandée
Secondary Specifiers (Spécificateurs secondaires) : Méthode	Définit une méthode d'URL de requête : – **get** – **post** – **put** – **trace**
Secondary Specifiers (Spécificateurs secondaires) : Scheme (Schéma)	Définit le protocole d'une URL demandée. Les options disponibles sont : – **HTTP** – **HTTPS** – **FTP** (pour FTP sur HTTP uniquement) **Remarque : rtsp** et **mms** ne sont **pas** pris en charge.
Secondary Specifiers (Spécificateurs secondaires) : User-Agent	Définit la valeur User-Agent de l'en-tête de la requête Servez-vous de ce champ pour créer des règles de filtrage des applications permettant : • D'autoriser les applications qui ne gèrent pas correctement les demandes d'authentification à contourner l'authentification • D'empêcher certaines applications de type client à accéder à Internet
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
	Authentification Windows intégrée
La page Authentification Windows intégrée ne s'affiche que si vous avez activé IWA dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**. Servez-vous de cette page pour effectuer ou annuler la jonction du domaine Windows. Lorsque la jonction d'un domaine a été effectuée, la page présente un résumé des attributs du domaine et un bouton Unjoin (Annuler la jonction). Voir *Authentification Windows intégrée*, page 179.	
Nom de domaine	Définit le nom de domaine Windows complet
Administrator Name (Nom d'administrateur)	Définit le nom d'utilisateur de l'administrateur Windows
Administrator Password (Mot de passe de l'administrateur)	Définit le mot de passe de l'administrateur Windows **Remarque :** ce nom et ce mot de passe ne sont utilisés que pendant la jonction et ne sont pas stockés.

Option	Description
Contrôleur de domaine	Indique comment localiser le contrôleur de domaine : • Auto-detect using DNS (Auto-détection via DNS) • DC name or IP address (Nom ou adresse IP du contrôleur de domaine) Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules.
Content Gateway Hostname (Nom d'hôte Content Gateway)	Définit le nom d'hôte de Content Gateway L'authentification IWA utilisant le nom d'hôte en tant que nom NetBIOS lors de l'enregistrement auprès de Kerberos, ce nom d'hôte ne doit pas dépasser 15 caractères (restrictions NetBIOS), ou 11 caractères dans les dispositifs V-Series (V-Series ajoute 4 caractères au nom d'hôte pour garantir le caractère unique du nom d'hôte dans tous les modules (Doms)). **IMPORTANT :** après la jonction du domaine, le nom d'hôte n'est plus modifiable. Lorsque ce nom est modifié, IWA cesse immédiatement de fonctionner et ne fonctionnera plus tant que la jonction au domaine n'aura pas été annulée, puis réeffectuée avec le nouveau nom d'hôte.
Join Domain (Joindre le domaine)	Cliquez sur cette option pour joindre le domaine.
	Global Authentication Options (Options d'authentification globales) Cette page vous permet de définir les options à appliquer lorsque l'authentification Windows intégrée effectue une authentification NTLM.
Fail Open (Échec ouvert)	Activée (par défaut), cette option autorise le traitement des requêtes lorsque l'authentification échoue dans les cas suivants : • Aucune réponse du contrôleur de domaine • Messages malformés provenant du client • Réponses SMB non valides **Remarque :** les échecs d'authentification du mot de passe sont toujours des échecs.
NTLM Credential Caching (Mise en cache des informations d'identification NTLM)	Active ou désactive la mise en cache des informations d'identification des utilisateurs lorsqu'ils ont été authentifiés par NTLM. Cette option s'applique uniquement lorsque Content Gateway est un proxy explicite.
Caching TTL (Durée de vie de la mise en cache)	Définit la durée de vie des entrées stockées dans le cache. La valeur par défaut est 900 secondes (15 minutes).
Multi-user IP Exclusions (Exclusion des adresses IP d'utilisateurs)	Définit la liste des adresses IP et des plages d'adresses IP (séparées par des virgules) des systèmes réseau hébergeant plusieurs hôtes, par exemple des serveurs Terminal Server

Option	Description
	Authentification du proxy transparent Servez-vous de cette page lorsque Content Gateway est un proxy transparent. Pour plus d'informations, consultez la section *Paramètres de l'authentification transparente du proxy*, page 178.
Redirect Hostname (Rediriger le nom d'hôte) (facultatif)	Définit un autre nom d'hôte du proxy pouvant être résolu via DNS pour tous les clients du réseau **Remarque** : cette option n'est pas nécessaire et ne concerne pas l'Authentification Windows intégrée (IWA).
Authentication Mode (Mode d'authentification)	Lorsque l'authentification du proxy transparent est configurée, Content Gateway doit être défini sur un mode d'authentification : • En **mode IP** (par défaut), l'adresse IP du client est associée à un nom d'utilisateur lors de l'authentification de la session. Les requêtes provenant de cette adresse IP ne sont plus authentifiées jusqu'à expiration du paramètre **Session TTL (Durée de vie de la session)**. La valeur par défaut est 15 minutes. • Le **mode Cookie** sert exclusivement à identifier les utilisateurs qui partagent une même adresse IP, par exemple dans les environnements utilisant des chaînes de proxy ou lorsqu'une traduction d'adresses réseau (NAT) est effectuée.
Session TTL (Durée de vie de la session)	Définit le délai devant s'écouler (en minutes) avant que le client ne soit à nouveau authentifié. Cette option est obligatoire pour les modes IP et Cookie. La valeur par défaut est 15 minutes. La plage des valeurs prises en charge va de 5 à 65 535 minutes.
	LDAP
Les options de configuration LDAP ne s'affichent dans le volet de configuration que si vous avez activé LDAP dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**. Pour plus d'informations sur la configuration de LDAP, consultez la section *Authentification LDAP*, page 188.	
Purge Cache on Authentication Failure (Purger le cache en cas d'échec d'authentification)	Lorsque cette option est activée, Content Gateway supprime l'entrée de l'autorisation du client dans le cache LDAP en cas d'échec de l'authentification.
Serveur LDAP : Nom d'hôte	Définit le nom d'hôte du serveur LDAP Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Serveur LDAP : Port	Définit le port utilisé pour la communication LDAP. Le numéro de port par défaut est le 389. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Serveur LDAP : Secure LDAP (LDAP sécurisé)	Indique si Content Gateway doit établir une communication sécurisée avec le serveur LDAP. Lorsque cette option est activée, définissez le champ Port LDAP (ci-dessus) sur 636 ou 3269 (ports LDAP sécurisés).
Serveur LDAP : Server Type (Type de serveur)	Définit le filtre de recherche. Sélectionnez Active Directory ou d'autres services d'annuaire.

Option	Description
Serveur LDAP : Bind Distinguished Name (Nom distinctif de liaison)	Spécifie le Nom distinctif complet (FDN) d'un utilisateur dans le service d'annuaire de type LDAP. Par exemple : `CN=John Smith,CN=USERS,DC=MASOCIETE, DC=COM` Entrez un maximum de 128 caractères dans ce champ. Si vous ne renseignez pas la valeur de ce champ, le proxy tente une liaison anonyme.
Serveur LDAP : Mot de passe	Définit le mot de passe de l'utilisateur identifié dans le champ **Bind_DN**
Serveur LDAP : Base Distinguished Name (Nom unique de la base de recherche LDAP)	Définit le Nom unique de la base de recherche LDAP (DN). Vous pouvez demander cette valeur à votre administrateur LDAP. Vous devez spécifier un nom de base de recherche LDAP correct, sinon l'authentification LDAP ne fonctionnera pas. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
	Radius
Les options de configuration Radius ne s'affichent dans le volet de configuration que si vous avez activé Radius dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**. Pour plus d'informations sur la configuration de Radius, consultez la section *Authentification RADIUS*, page 190.	
Primary Radius Server (Serveur Radius principal) : Nom d'hôte	Définit le nom d'hôte ou l'adresse IP du serveur d'authentification RADIUS principal. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Primary Radius Server (Serveur Radius principal) : Port	Définit le port utilisé par Content Gateway pour communiquer avec le serveur d'authentification RADIUS principal. Le port par défaut est le 1812. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Primary Radius Server (Serveur Radius principal) : Shared Key (Clé partagée)	Définit la clé d'encodage à utiliser Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Secondary Radius Server (Serveur Radius secondaire) (facultatif) : Nom d'hôte	Spécifie le nom d'hôte ou l'adresse IP du serveur d'authentification RADIUS secondaire Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Secondary Radius Server (Serveur Radius secondaire) (facultatif) : Port	Définit le port utilisé par Content Gateway pour communiquer avec le serveur d'authentification RADIUS secondaire. Le port par défaut est le 1812. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Secondary Radius Server (Serveur Radius secondaire) (facultatif) : Shared Key (Clé partagée)	Définit la clé d'encodage à utiliser Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Option	Description
	Authentification NTLM héritée
Les options de configuration NTLM ne s'affichent dans le volet de configuration que si vous avez activé NTLM dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**. Pour plus d'informations sur la configuration de l'authentification NTLM, consultez la section *Authentification NTLM héritée*, page 185.	

Domain Controller Hostnames (Noms d'hôte des contrôleurs de domaine)	Définit les noms d'hôte des contrôleurs de domaine dans une liste séparée par des virgules. Le format est le suivant :
	`nom_hôte[:port][%nom_netbios]`
	ou
	`adresse_IP[:port][%nom_netbios]`
	Si vous utilisez Active Directory 2008, vous devez inclure le `nom_netbios` ou utiliser le port SMB 445.
	Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Load Balancing (Équilibrage de la charge)	Active ou désactive l'équilibrage de la charge. Lorsque cette option est activée, Content Gateway équilibre la charge lorsqu'il envoie des requêtes d'authentification aux contrôleurs de domaine. **Remarque :** lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Fail Open (Échec ouvert)	Activée (par défaut), cette option autorise le traitement des requêtes lorsque l'authentification échoue dans les cas suivants : • Aucune réponse du contrôleur de domaine • Messages malformés provenant du client • Réponses SMB non valides **Remarque :** les échecs d'authentification du mot de passe sont toujours des échecs.
IP Credentials (Informations d'identification des adresses IP) : Credential caching (Mise en cache des informations d'identification)	Active ou désactive la mise en cache des informations d'identification NTLM. Cette option s'applique uniquement lorsque Content Gateway est un proxy explicite.
IP Credentials (Informations d'identification des adresses IP) : Caching TTL (Durée de vie de la mise en cache)	Définit la durée de vie, en secondes, des informations d'identification NTLM mises en cache. La valeur par défaut est 900 secondes (15 minutes). La plage des valeurs prises en charge va de 300 à 86 400 secondes.

Option	Description
IP Credentials (Informations d'identification des adresses IP) : Multi-user IP Exclusions (Exclusion des adresses IP multi-utilisateurs)	Définit la liste des adresses IP et des plages d'adresses IP multi-utilisateurs (séparées par des virgules) des serveurs Terminal Server, des pare-feu NAT, etc. Les informations d'identification de ces utilisateurs ne sont pas mises en cache.
	Domaines
La page Domaines ne s'affiche dans la liste Access Control (Contrôle d'accès) que si vous avez activé l'option **Multiple Realm Authentication (Authentification dans plusieurs domaines Kerberos)** dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**. Servez-vous de cet onglet pour joindre les domaines pour lesquels vous allez créé des règles d'authentification. La description détaillée de l'authentification dans plusieurs domaines Kerberos est disponible à la section *Authentification dans plusieurs domaines Kerberos*, page 194.	
Nom de domaine	Définit le nom de domaine Windows complet
Administrator Name (Nom d'administrateur)	Définit le nom d'utilisateur de l'administrateur Windows
Administrator Password (Mot de passe de l'administrateur)	Définit le mot de passe de l'administrateur Windows **Remarque :** ce nom et ce mot de passe ne sont utilisés que pendant la jonction et ne sont pas stockés.
Contrôleur de domaine	Indique comment localiser le contrôleur de domaine : • Auto-detect using DNS (Auto-détection via DNS) • DC name or IP address (Nom ou adresse IP du contrôleur de domaine) Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules.
Content Gateway Hostname (Nom d'hôte Content Gateway)	Définit le nom d'hôte de Content Gateway L'authentification IWA utilisant le nom d'hôte en tant que nom NetBIOS lors de l'enregistrement auprès de Kerberos, ce nom d'hôte ne doit pas dépasser 15 caractères (restrictions NetBIOS), ou 11 caractères dans les dispositifs V-Series (V-Series ajoute 4 caractères au nom d'hôte pour garantir le caractère unique du nom d'hôte dans tous les modules (Doms)). **IMPORTANT :** après la jonction du domaine, le nom d'hôte n'est plus modifiable. Lorsque ce nom est modifié, IWA cesse immédiatement de fonctionner et ne fonctionnera plus tant que la jonction au domaine n'aura pas été annulée, puis réeffectuée avec le nouveau nom d'hôte.
Join Domain (Joindre le domaine)	Cliquez sur cette option pour joindre le domaine.
Liste Joined Domains (Domaines joints)	Présente la liste des domaines dont la jonction a été effectuée
Bouton Unjoin Domain (Annuler la jonction du domaine)	Pour annuler la jonction d'un domaine, sélectionnez un domaine, puis cliquez sur ce bouton.
Realm Name (Nom du domaine Kerberos)	Affiche le nom du domaine sélectionné dans la liste Joined Domains (Domaines joints)

Option	Description
Fully Qualified Domain Name (Nom de domaine complet)	Affiche le nom de domaine complet du domaine sélectionné dans la liste Joined Domains (Domaines joints)
Content Gateway Hostname (Nom d'hôte Content Gateway)	Affiche le nom d'hôte que les navigateurs clients doivent utiliser dans la section des paramètres de proxy du navigateur lorsque l'Authentification Windows intégrée (Kerberos) est configurée
Contrôleur de domaine	Indique comment localiser le contrôleur de domaine sélectionné : • Auto-detect using DNS (Auto-détection via DNS) • DC name or IP address (Nom ou adresse IP du contrôleur de domaine) Lorsque le contrôleur de domaine est défini par son nom ou son adresse IP, vous pouvez également spécifier des contrôleurs de domaine de sauvegarde dans une liste séparée par des virgules.
	Authentification dans plusieurs domaines Kerberos
Dans les réseaux avec plusieurs domaines Kerberos (domaines qui ne partagent pas de relations de confiance mutuelles), des règles peuvent être définies pour diriger les jeux d'adresse IP vers des contrôleurs de domaine spécifiques. Pour plus d'informations, consultez la section *Authentification dans plusieurs domaines Kerberos*, page 194.	
Authentification	Présente un tableau répertoriant les règles du *Fichier de configuration auth.config* qui dirigent les adresses IP spécifiées vers des contrôleurs de domaine spécifiques pour l'authentification. Dans les environnements de proxy explicite, il est possible de définir des règles pour le trafic entrant sur des ports spécifiques. Des règles IWA, LDAP et NTLM peuvent être configurées.
Actualiser	Met à jour le tableau pour afficher les règles actuelles du fichier **auth.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **auth.config** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier auth.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration auth.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Rule Type (Type de règle)	Définit le type de règles : Sélectionnez **Authentification Windows intégrée** pour les règles devant appliquer Kerberos. Sélectionnez **Legacy NTLM (Authentification NTLM héritée)** pour définir les règles devant appliquer la méthode NTLMSSP. Sélectionnez **LDAP** pour définir les règles devant utiliser LDAP.
Statut (État)	Indique si la règle est activée ou désactivée après son enregistrement et le redémarrage de Content Gateway

Option	Description
Rule Name (Nom de la règle)	Spécifie le nom descriptif de la règle (ce nom doit être unique)
IP source	Définit les adresses IP ou les plages d'adresses IP de cette règle (elles doivent être saisies sans espace) Exemple : 10.1.1.1 ou 0.0.0.0-255.255.255.255 ou 10.1.1.1,20.2.2.2,3.0.0.0-3.255.255.255
Proxy Port (Port du proxy)	Définit le port entrant du trafic lorsque Content Gateway est déployé en tant que proxy explicite
Paramètres avancés : Aliasing (Alias)	Définit l'alias à envoyer au service de filtrage pour tous les utilisateurs auxquels cette règle s'applique. L'alias doit être statique et peut être vide (non renseigné). L'alias doit exister dans le contrôleur de domaine principal (celui qui est visible pour le service de filtrage).
IWA Specifiers (Spécificateurs IWA) : Domain/Realm (Domaine/Domaine Kerberos)	Définit le domaine (Kerberos) auquel la règle s'applique
NTLM Specifiers (Spécificateurs NTLM) : DC List (Liste des contrôleurs de domaine)	Définit l'adresse IP le numéro de port du contrôleur de domaine principal (lorsqu'aucun port n'est défini, Content Gateway utilise le port 139), suivis de la liste des contrôleurs de domaine secondaires, séparés par des virgules, à utiliser pour l'équilibrage de la charge et le basculement
NTLM Specifiers (Spécificateurs NTLM) : DC Load Balance (Équilibrage de la charge des contrôleurs de domaine)	Définit le mode d'utilisation de l'équilibrage de la charge : • `0` = désactivé • `1` = activé **Remarque :** lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé.
LDAP Specifiers (Spécificateurs LDAP) : LDAP Server Name (Nom du serveur LDAP)	Spécifie le nom du serveur LDAP Cette option ne concerne que les types de règles `ldap`.
LDAP Specifiers (Spécificateurs LDAP) : LDAP Server Port (Port du serveur LDAP)	Définit le port du serveur LDAP (facultatif ; par défaut 389)
LDAP Specifiers (Spécificateurs LDAP) : Base Distinguished Name LDAP (Nom unique de la base de recherche LDAP)	Définit le nom unique de la base de recherche LDAP Cette option ne concerne que les types de règles `ldap`.
LDAP Specifiers (Spécificateurs LDAP) : Server Type (Type de serveur)	Définit le filtre de recherche sur « sAMAccountName » pour Active Directory ou sur « uid » pour les autres services d'annuaire

Option	Description
LDAP Specifiers (Spécificateurs LDAP) : Bind DN (Nom distinctif de liaison)	Définit le nom distinctif du compte de liaison LDAP
LDAP Specifiers (Spécificateurs LDAP) : Bind Password (Mot de passe de liaison)	Définit le mot de passe du compte de liaison LDAP
LDAP Specifiers (Spécificateurs LDAP) : Secure LDAP (LDAP sécurisé)	Indique si Content Gateway doit établir une communication sécurisée avec le serveur LDAP Si cette option est activée, vous devez définir le port LDAP sur l'un des ports sécurisés : 636 ou 3269.
LDAP Specifiers (Spécificateurs LDAP) : LDAP Attribute Name (Nom d'attribut LDAP) (facultatif)	Définit le nom de l'attribut LDAP
LDAP Specifiers (Spécificateurs LDAP) : LDAP Attribute Value (Valeur de l'attribut LDAP) (facultatif)	Définit la paire d'attributs LDAP
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

SOCKS

Pour plus d'information sur la prise en charge de SOCKS par Content Gateway, consultez la section *Configuration de l'intégration du pare-feu SOCKS*, page 171.

> **Remarque**
> Les options de configuration SOCKS ne s'affichent dans le volet de configuration que si vous avez activé SOCKS dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Option	Description
	Général
SOCKS Version (Version SOCKS)	Spécifie la version SOCKS utilisée dans votre serveur SOCKS. Content Gateway prend en charge les versions SOCKS 4 et 5. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
	Proxy
SOCKS Proxy (Proxy SOCKS)	Active ou désactive l'option Proxy SOCKS. En tant que proxy SOCKS, Content Gateway peut recevoir les paquets SOCKS (en général sur le port 1080) provenant des clients et transmettre les requêtes directement au serveur SOCKS. Pour plus d'informations sur l'option de proxy SOCKS, consultez la section *Configuration de l'intégration du pare-feu SOCKS*, page 171. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
SOCKS Proxy Port (Port du proxy SOCKS)	Définit le port sur lequel Content Gateway accepte le trafic SOCKS. Il s'agit généralement du port 1080. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
	Serveur
On-Appliance SOCKS server (Serveur SOCKS sur dispositif)	S'affiche uniquement lorsque Content Gateway est installé dans un dispositif V-Series. Active ou désactive le serveur SOCKS installé dans le dispositif L'option de proxy SOCKS doit être activée pour acheminer les requêtes des clients via le serveur SOCKS. Pour configurer Content Gateway pour qu'il utilise d'autres serveurs SOCKS de votre réseau, vous pouvez modifier le fichier **socks_server.config**. Reportez-vous à l'entrée suivante, ci-dessous.
Tableau des serveurs Socks	Présente le tableau des serveurs SOCKS configurés. Pour plus d'informations sur l'ajout et la configuration des serveurs SOCKS, consultez la section *Configuration des serveurs SOCKS*, page 172.
Actualiser	Met à jour le tableau pour afficher les entrées actuelles du fichier **socks_server.config**
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration pour le fichier **socks_server.config**

Option	Description
	Éditeur de fichiers de configuration pour le fichier socks_server.config
Champ d'affichage des entrées	Répertorie les serveurs SOCKS configurés pour une utilisation avec Content Gateway. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer l'entrée sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une entrée dans la liste des serveurs
Set (Définir)	Met à jour l'entrée sélectionnée. Sélectionnez un serveur dans la liste, modifiez les paramètres, puis cliquez sur **Set (Définir)** pour actualiser cette entrée.
Clear Fields (Effacer les champs)	Efface tous les champs du serveur sélectionné
SOCKS Server Name (Nom du serveur SOCKS)	Définit un nom qui différencie ce serveur SOCKS des autres serveurs SOCKS
SOCKS Server Host (Hôte du serveur SOCKS)	Définit l'adresse IP du serveur SOCKS ou un nom d'hôte que votre service DNS interne peut résoudre
SOCKS Port (Port SOCKS)	Définit le port sur lequel le serveur SOCKS est à l'écoute
Default SOCKS Server (Serveur SOCKS par défaut)	Activez cette option pour que ce serveur SOCKS devienne le serveur SOCKS par défaut.
SOCKS User Name (Nom d'utilisateur SOCKS)	Lorsque l'authentification SOCKS est utilisée, définissez le nom d'utilisateur SOCKS à utiliser pour l'authentification.
SOCKS Password (Mot de passe SOCKS)	Lorsque l'authentification SOCKS est utilisée, définissez le mot de passe associé à l'utilisateur spécifié.
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
Socks Server Rules (Règles des serveurs Socks)	Présente un tableau répertoriant les règles du fichier **socks.config** qui identifient les serveurs SOCKS par lesquels Content Gateway doit passer pour accéder à des serveurs d'origine spécifiques et l'ordre dans lequel Content Gateway doit parcourir la liste des serveurs SOCKS Vous pouvez également spécifier les serveurs d'origine auxquels le proxy peut accéder directement, sans passer par un serveur SOCKS.
Actualiser	Met à jour le tableau pour afficher les règles actuelles du fichier **socks.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **socks.config** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier socks.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration socks.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.

Option	Description
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Rule Type (Type de règle)	Sélectionnez **Route through SOCKS server (Acheminer via le serveur SOCKS)** pour définir les serveurs d'origine que le proxy doit acheminer par l'intermédiaire d'un serveur SOCKS. Sélectionnez **Do not route through SOCKS server (Ne pas acheminer via le serveur SOCKS)** pour spécifier les serveurs d'origine auxquels le proxy doit accéder directement, en ignorant le(s) serveur(s) SOCKS.
IP de destination	Pour l'option **Route through SOCKS server (Acheminer via le serveur SOCKS)**, définissez l'adresse IP individuelle *ou* la plage d'adresses IP de serveurs d'origine pour lesquelles Content Gateway doit utiliser les serveurs SOCKS définis dans le champ **SOCKS Servers (Serveurs SOCKS)** ci-dessous. Pour l'option **Do not route through SOCKS server (Ne pas acheminer via le serveur SOCKS)**, définissez les adresses IP des serveurs d'origine auxquels le proxy doit accéder directement (sans passer par le serveur SOCKS). Vous pouvez saisir une adresse IP individuelle, une plage d'adresses IP ou une liste d'adresses IP. Séparez chaque entrée de la liste par une virgule. Ne spécifiez pas l'adresse de diffusion de tous les réseaux : 255.255.255.255.
Serveur SOCKS	Pour la règle **Route through SOCKS server (Acheminer via le serveur SOCKS)**, sélectionnez le(s) serveur(s) SOCKS par le(s)quel(s) les requêtes doivent être acheminées.
Round Robin (Recherche circulaire)	Définit le mode de recherche circulaire que Content Gateway doit respecter. Vous pouvez sélectionner **strict** ou **false**.
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
	Options
Server Connection Timeout (Expiration des connexions aux serveurs)	Cette option définit le nombre de secondes pendant lesquelles Content Gateway doit tenter de se connecter à un serveur SOCKS avant expiration.
Connection Attempts Per Server (Tentatives de connexion par serveur)	Cette option définit le nombre de fois où Content Gateway doit tenter de se connecter à un certain serveur SOCKS avant de le désigner comme indisponible.
Server Pool Connection Attempts (Tentatives de connexion au pool de serveurs)	Cette option définit le nombre de fois où Content Gateway doit tenter de se connecter à un certain serveur SOCKS du pool avant d'abandonner.

Sous-systèmes

Les options de configuration des sous-systèmes se répartissent dans les catégories suivantes :

Cache, page 313

Journalisation, page 315

Référentiel d'analyses, page 319

Cache

Option	Description
	Général
Allow Pinning (Autoriser l'épinglage)	Active ou désactive l'option d'épinglage du cache, qui vous permet de conserver des objets dans le cache pour une durée spécifiée. Définissez les règles d'épinglage du cache dans le *Fichier de configuration cache.config*.
Ram Cache Size (Taille du cache de mémoire RAM)	Définit la taille du cache de mémoire RAM, en octets. La taille par défaut est de 104 857 600 (100 Mo). La valeur « -1 » indique à Content Gateway de dimensionner automatiquement le cache de mémoire RAM sur environ 1 Mo par Go de cache disque. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Maximum Object Size (Taille maximale des objets)	Définit la taille maximale autorisée pour les objets du cache. La valeur 0 (zéro) indique que la taille n'est pas limitée.
	Partition
Cache Partition (Partition du cache)	Présente un tableau répertoriant les règles du *Fichier de configuration partition.config* qui contrôlent le partitionnement du cache
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **partition.config**. Cliquez sur ce bouton après avoir ajouté ou modifié des règles dans l'éditeur de fichiers de configuration.
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **partition.config**
	Éditeur de fichier de configuration pour le fichier partition.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration partition.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.

Option	Description
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration. Renseignez les champs fournis avant de cliquer sur ce bouton.
Set (Définir)	Actualise le champ d'affichage des règles situé en haut de la page. Avant de cliquer sur ce bouton, sélectionnez une règle et modifiez ses propriétés.
Partition Number (Numéro de partition)	Définit un numéro de partition entre 1 et 255
Scheme (Schéma)	Définit le type de contenu stocké dans la partition. Seul HTTP est pris en charge.
Partition Size (Taille de la partition)	Définit le volume d'espace du cache alloué à la partition. Cette taille peut être un pourcentage de l'espace total du cache ou une valeur absolue en Mo.
Partition Size Format (Format de taille de la partition)	Définit le format de la taille de la partition : en pourcentage ou absolue
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
	Hébergement
Cache Hosting (Hébergement du cache)	Présente un tableau répertoriant les règles du fichier **hosting.config** qui contrôlent les partitions du cache attribuées à des serveurs d'origine et des domaines spécifiques.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **hosting.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **hosting.config** dans l'éditeur de fichiers de configuration. La page de l'éditeur de fichiers de configuration est décrite ci-dessous.
	Éditeur de fichiers de configuration pour le fichier hosting.config
Champ d'affichage des règles	Répertorie les règles du fichier **hosting.config**. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Primary Destination Type (Type de destination principale)	Définit le type de règle de destination principale : Sélectionnez **domain (domaine)** si vous souhaitez partitionner le cache en fonction du domaine. Sélectionnez **hostname (nom d'hôte)** si vous souhaitez partitionner le cache en fonction du nom d'hôte.

Option	Description
Primary Destination Value (Valeur de la destination principale)	Définit le nom d'hôte du domaine ou du serveur d'origine dont le contenu doit être stocké dans une partition spécifique
Partitions	Définit les partitions dans lesquelles vous souhaitez stocker le contenu appartenant au serveur d'origine ou au domaine spécifié. Séparez chaque partition par une virgule. Remarque : Les partitions doivent déjà avoir été créées dans le fichier **partition.config**. Pour plus d'informations sur la création de partitions, consultez la section *Partitionnement du cache*, page 91.
Partitions	Définit la liste des partitions (séparées par des virgules) dans lesquelles vous souhaitez stocker le contenu appartenant au serveur d'origine ou au domaine spécifié
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

Journalisation

Option	Description
	Général
Journalisation	Active ou désactive la journalisation des événements pour que les transactions soient enregistrées dans des fichiers journaux d'événements et/ou des fichiers journaux d'erreurs. Sélectionnez **Log Transactions and Errors (Enregistrer les transactions et les erreurs)** pour consigner les transactions dans vos fichiers journaux d'événements sélectionnés et les erreurs dans les fichiers journaux d'erreurs. Sélectionnez **Log Transactions Only (Enregistrer les transactions uniquement)** pour enregistrer les transactions dans vos fichiers journaux d'événements sélectionnés uniquement. Dans ce cas, Content Gateway n'enregistre pas les erreurs dans les fichiers journaux d'erreurs. Sélectionnez **Log Errors Only (Enregistrer les erreurs uniquement)** pour enregistrer les erreurs dans les fichiers journaux d'erreurs uniquement. Dans ce cas, Content Gateway n'enregistre pas les transactions dans vos fichiers journaux d'événements sélectionnés. Sélectionnez **Disabled (Désactivé)** pour désactiver la journalisation.
Log Directory (Répertoire des journaux)	Définit le chemin du répertoire dans lequel Content Gateway stocke les journaux d'événements. Le chemin de ce répertoire doit être le même dans chaque nœud du groupe de basculement du cluster Content Gateway. L'emplacement par défaut est : /opt/WCG/logs.

Option	Description
Log Space (Espace des journaux) : Limite	Définit la quantité maximale d'espace (en méga-octets) allouée au répertoire de journalisation pour les fichiers journaux. Lorsque Content Gateway est installé dans un dispositif V-series, la taille est définie sur 5 120 (5 Go) et n'est pas modifiable. Lorsque Content Gateway est installé dans un serveur autonome, la taille par défaut est de 20 480 (20 Go) et peut être configurée. **Remarque :** les journaux des transactions occupent énormément d'espace. Assurez-vous que cette limite soit inférieure à l'espace réellement disponible dans la partition contenant le répertoire de journalisation.
Log Space (Espace des journaux) : Headroom (Marge)	Définit la tolérance vis-à-vis de la limite d'espace occupé par les journaux. Lorsque l'option **Auto-Delete Rolled Files (Supprimer automatiquement les fichiers après leur rotation)** est activée, la suppression automatique intervient lorsque le volume d'espace disponible dans le répertoire de journalisation est inférieur à la marge définie.
Log Rolling (Rotation des journaux) : Activer/ Désactiver	Active ou désactive la rotation des fichiers journaux. Pour que les fichiers journaux ne dépassent pas une certaine taille, vous pouvez effectuer une rotation à intervalles réguliers. Voir *Rotation des fichiers journaux d'événements*, page 221.
Log Rolling (Rotation des journaux) : Offset Hour (Heure de décalage)	Définit l'heure à laquelle la rotation des journaux intervient. Vous pouvez définir une heure du jour dans la plage 0 à 23. Par exemple, si l'heure de décalage est définie sur 0 (minuit) et l'intervalle de rotation sur 6, la rotation des fichiers journaux intervient à 00:00, 06:00, midi et 18:00.
Log Rolling (Rotation des journaux) : Intervalle	Définit le nombre de fois où Content Gateway saisit des données dans les fichiers journaux avant d'effectuer leur rotation et de définir leur extension sur **.old**. La valeur minimale est 300 secondes (cinq minutes). La valeur par défaut est 21 600 secondes (6 heures). La valeur maximale est 86 400 (1 jour).
Log Rolling (Rotation des journaux) : Auto-Delete Rolled Files (Supprimer automatiquement les fichiers après leur rotation)	Active la suppression automatique des fichiers journaux ayant subi une rotation lorsque l'espace disponible commence à manquer dans le répertoire des journaux. La suppression automatique commence lorsque la quantité d'espace disponible dans le répertoire de journalisation est inférieure à la marge définie.
	Formats
Format Squid : Activer/ Désactiver	Active ou désactive le format de journaux Squid
Format Squid : ASCII/ Binaire	Sélectionnez **ASCII** ou **Binaire** en tant que type des fichiers journaux à créer.
Format Squid : Nom de fichier	Définit le nom utilisé pour les fichiers journaux Squid. Le nom par défaut est **squid.log**.
Format Squid : En-tête	Définit l'en-tête de texte à insérer dans les fichiers journaux Squid

Option	Description
Format Netscape Common : Activer/ Désactiver	Active ou désactive le format de journal Netscape Common
Format Netscape Common : ASCII/ Binaire	Sélectionnez **ASCII** ou **Binary** en tant que type de fichiers journaux à créer.
Format Netscape Common : Nom de fichier	Définit le nom utilisé par les fichiers journaux Netscape Common. Le nom de fichier par défaut est **common.log**.
Format Netscape Common : En-tête	Définit l'en-tête de texte à insérer dans les fichiers journaux Netscape Common
Format Netscape Extended : Activer/ Désactiver	Active ou désactive le format de journaux Netscape Extended
Format Netscape Extended : ASCII/ Binaire	Sélectionnez **ASCII** ou **Binary** en tant que type de fichiers journaux à créer.
Format Netscape Extended : Nom de fichier	Définit le nom utilisé pour les fichiers journaux Netscape Extended. Le nom de fichier par défaut est **extended.log**.
Format Netscape Extended : En-tête	Définit l'en-tête de texte à insérer dans les fichiers journaux Netscape Extended
Format Netscape Extended-2 : Activer/ Désactiver	Active ou désactive le format de journaux Netscape Extended-2
Format Netscape Extended-2 : ASCII/ Binaire	Sélectionnez **ASCII** ou **Binary** en tant que type de fichiers journaux à créer.
Format Netscape Extended-2 : Nom de fichier	Définit le nom utilisé pour les fichiers journaux Netscape Extended-2. Le nom de fichier par défaut est **extended2.log**.
Format Netscape Extended-2 : En-tête	Définit l'en-tête de texte à insérer dans les fichiers journaux Netscape Extended-2

Option	Description
	Collecte
Collation Mode (Mode de collecte)	Définit le mode de collecte des journaux pour ce nœud Content Gateway. Vous pouvez utiliser la fonction de collecte des fichiers journaux pour stocker toutes les informations enregistrées en un même emplacement. Pour plus d'informations sur la collecte des fichiers journaux, consultez la section *Collecte des fichiers journaux d'événements*, page 226. Sélectionnez **Collation Disabled (Collecte désactivée)** pour désactiver la collecte des journaux dans ce nœud Content Gateway. Sélectionnez **Be a Collation Server (CG en tant que serveur de collecte)** pour configurer ce nœud Content Gateway en tant que serveur de collecte. Sélectionnez **Be a Collation Client (CG en tant que client de collecte)** pour configurer ce serveur Content Gateway en tant que client de collecte. Un serveur Content Gateway configuré en tant que client de collecte envoie uniquement les fichiers journaux standard actifs, tels que Squid, Netscape Common, etc., au serveur de collecte. Si vous activez cette option, saisissez le nom d'hôte du serveur de collecte de votre cluster dans le champ **Log Collation Server (Serveur de collecte des journaux)**. Remarque : Lors de la collecte des journaux, la source de l'entrée du journal (son nœud d'origine) est perdue, sauf si vous activez l'option **Log collation host tagged (Collecte des journaux des hôtes balisés)** (décrite ci-dessous). Lorsque toutes les entrées de journal sont envoyées à un même nœud, la collecte des journaux monopolise la bande passante du cluster. Les performances du cluster peuvent donc être affectées. Pour que Content Gateway, configuré en tant que client de collecte, envoie des fichiers journaux personnalisés (de type XML), vous devez spécifier un objet `LogObject` dans le fichier **logs_xml.config**.
Log Collation Server (Serveur de collecte des journaux)	Définit le nom d'hôte du serveur de collecte des journaux auquel vous souhaitez envoyer les fichiers journaux
Log Collation Port (Port de collecte des journaux)	Définit le port utilisé pour la communication entre le serveur et le client de collecte. Vous devez dans tous les cas définir un numéro de port, sauf lorsque la collecte des journaux est inactive. Le numéro de port par défaut est le 8085. Remarque : ne modifiez pas ce numéro de port, sauf en cas de conflit avec un autre service passant déjà par ce port.
Log Collation Secret (Mot de passe de collecte des journaux)	Définit le mot de passe du serveur de collecte des journaux et des autres nœuds du cluster. Ce mot de passe sert à valider les données de la journalisation et à empêcher tout échange d'informations aléatoires.
Log Collation Host Tagged (Collecte des journaux des hôtes balisés)	Lorsque cette option est activée, Content Gateway ajoute le nom d'hôte du nœud à l'origine de l'entrée du journal à la fin de l'entrée du fichier journal collecté.

Option	Description
Log Collation Orphan Space (Espace de stockage des fichiers journaux orphelins)	Définit la quantité maximale d'espace (en méga-octets) allouée au répertoire de journalisation pour le stockage des fichiers journaux orphelins dans le nœud Content Gateway. Content Gateway crée des entrées de journaux orphelins lorsqu'il ne peut pas contacter le serveur de collecte des journaux.
	Personnaliser
Custom Logging (Journalisation personnalisée)	Active ou désactive la journalisation personnalisée
Custom Log File Definitions (Définitions du fichier journal personnalisé)	Affiche le *Fichier de configuration logs_xml.config* pour que vous puissiez configurer les options de la journalisation personnalisée (de type XML)

Référentiel d'analyses

Option	Description
Registration status (État de l'enregistrement)	Indique l'État actuel de l'enregistrement Content Gateway auprès du référentiel d'analyses (Forensics Repository)
Forensics Repository IP address (Adresse IP du référentiel d'analyses)	Présente l'emplacement (adresse IP) du référentiel d'analyses
Bouton Unregister (Annuler l'enregistrement)	Servez-vous de ce bouton pour annuler l'enregistrement auprès du référentiel d'analyses. Remarque : Content Gateway vérifie l'état d'enregistrement du référentiel d'analyses dès qu'il démarre et tente éventuellement de s'auto-enregistrer.

Mise en réseau

Les options de configuration de la mise en réseau se répartissent dans les catégories suivantes :

Gestion des connexions, page 320

ARM, page 321

WCCP, page 326

Proxy DNS, page 330

Résolveur DNS, page 330

ICAP, page 332

IP virtuel, page 333

Gestion des connexions

Option	Description
	Limitation
Throttling Net Connections (Limitation de connexions nette)	Définit le nombre maximal de connexions réseau que Content Gateway peut accepter. Définir la limite de Content Gateway permet d'éviter la surcharge du système en cas d'engorgement du trafic. Lorsque le nombre de connexions réseau atteint cette limite, Content Gateway place les nouvelles connexions en file d'attente jusqu'à la fermeture des connexions en cours. Ne définissez pas cette variable sur une valeur inférieure à la valeur minimale de 100.
	Délestage de la charge
Maximum Connections (Nombre maximal de connexions)	Définit le nombre maximal de connexions de clients autorisées avant que le module ARM ne commence à transmettre directement les requêtes entrantes au serveur d'origine. La valeur par défaut est 1 million de connexions. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
	Contrôle des connexions de clients Indique : • Les limites de connexions de clients simultanées • Les limites de taux de connexions de clients • La réponse du proxy lorsqu'une limite est dépassée • La liste des clients autorisés à ne pas respecter les limites
Concurrent Connection Limit (Limite de connexions simultanées) : Maximum concurrent connections (Nombre maximal de connexions simultanées)	Définit le nombre maximal de connexions HTTP/HTTPS simultanées autorisées pour un client. La valeur par défaut est 1000. la plage prise en charge de 1 à 45 000.
Concurrent Connection Limit (Limite de connexions simultanées) : Alert when limit exceeded (Alerte de dépassement de limite)	Lorsque cette option est activée, Content Gateway doit générer une alerte lorsqu'un client dépasse la limite maximale de connexions simultanées. En plus de s'afficher dans Content Gateway Manager, l'alerte est également journalisée dans les fichiers /var/log/messages et content_gateway.out.
Concurrent Connection Limit (Limite de connexions simultanées) : Close excessive connections when limit exceeded (Fermer les connexions en excès lorsque la limite est dépassée)	Lorsque cette option est activée, Content Gateway ferme les connexions en excès dès que la limite définie est dépassée.

Option	Description
Connection Rate Limit (Limite de taux de connexions) : Maximum connection rate (Taux maximal de connexions)	Définit le nombre maximal de connexions par seconde autorisées pour un client, calculé en moyenne sur une minute. La valeur par défaut est 1000. la plage prise en charge de 1 à 45000.
Connection Rate Limit (Limite de taux de connexions) : Alert when limit exceeded (Alerte de dépassement de limite)	Lorsque cette option est activée, Content Gateway doit générer une alerte lorsqu'un client dépasse la limite maximale du taux de connexions. En plus de s'afficher dans Content Gateway Manager, l'alerte est également journalisée dans les fichiers /var/log/messages et content_gateway.out.
Connection Rate Limit (Limite de taux de connexions) : Close excessive connections when limit exceeded (Fermer les connexions en excès lorsque la limite est dépassée)	Lorsque cette option est activée, Content Gateway ferme les connexions en excès dès que la limite définie est dépassée.
Exceptions	Définit les adresses IP et/ou les plages d'adresses IP auxquelles les limites de connexion ne s'appliquent **pas**. Il peut s'agir d'adresses IPv4 ou IPv6 (la prise en charge des adresses IPv6 doit être activée). Il est possible de spécifier plusieurs adresses ou plages dans une liste séparée par des virgules.
	Low Memory Mode (Mode Mémoire faible) Indique si Content Gateway doit interrompre l'analyse du trafic Web lorsque le système hôte vient à manquer de mémoire **Remarque :** dans cet état, le filtrage des URL s'applique comme d'habitude.
Low Memory Mode (Mode Mémoire faible) : Enabled/ Disabled (Activé/Désactivé)	Sélectionnez **Enabled (Activé)** pour suspendre l'analyse en présence d'une condition de mémoire faible.
Low Memory Mode Duration (Durée du mode Mémoire faible)	Définit la durée de l'interruption de l'analyse, en minutes Lorsque la condition de mémoire faible se résout d'elle-même avant expiration de ce délai, l'analyse reprend et le déclencheur du mode de mémoire faible est réinitialisé. Si le délai arrive à expiration, l'analyse reprend et le déclencheur du mode de mémoire faible n'est **pas** réinitialisé.

ARM

Le module ARM (Adaptive Redirection Module) exécute plusieurs fonctions essentielles, dont l'envoi aux périphériques des notifications de basculement de l'interface de communication du cluster et l'examen des paquets entrants avant que la couche IP ne puisse les voir, en les envoyant ensuite à Content Gateway en vue de leur traitement.

Le module ARM est toujours actif. Pour plus d'informations, consultez la section *Module ARM*, page 48.

Option	Description
	Général
IP spoofing (Usurpation d'adresse IP)	Active ou désactive l'option d'usurpation d'adresse IP, qui demande à Content Gateway d'établir des connexions au serveur d'origine avec l'adresse IP du client et non pas avec l'adresse IP de Content Gateway. Pour plus d'informations, consultez la section *Usurpation d'adresse IP*, page 72. **AVERTISSEMENT :** l'usurpation d'adresse IP requiert un contrôle précis des chemins de routage sur votre réseau, car il remplace le processus de routage habituel du trafic s'exécutant sur les ports TCP 80 et 443.
Network Address Translation (Traduction d'adresses réseau) (NAT)	Présente les règles de redirection du *Fichier de configuration ipnat.conf* qui définissent le mode de réadressage des paquets entrants lorsque le proxy dessert le trafic en transparence. Content Gateway crée ces règles de redirection pendant l'installation. Vous pouvez modifier ces règles.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **ipnat.conf**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **ipnat.conf** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier ipnat.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration ipnat.conf*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Interface Ethernet	Définit l'interface Ethernet que le trafic doit utiliser pour accéder à l'ordinateur Content Gateway : par exemple, `eth0` sous Linux.
Type de connexions	Définit le type de connexions auquel la règle s'applique : TCP ou UDP
Original Destination IP (Adresse IP d'origine)	Définit l'adresse IP d'où provient le trafic. 0.0.0.0 correspond à toutes les adresses IP.
Original Destination CIDR (CIDR de destination originale)	Définit l'adresse IP au format CIDR (Classless Inter-Domain Routing), par exemple 1.1.1.0/24. La saisie d'une valeur dans ce champ est facultative.
Original Destination Port (Port de destination originale)	Définit le port de destination du trafic : par exemple, 80 pour le trafic HTTP.

Option	Description
Local Client IP (Adresse IP locale du client)	Définit l'adresse IP de votre serveur Content Gateway
Local Port (Port local)	Définit le port du proxy : par exemple, 8080 pour le trafic HTTP.
User Protocol (Protocole utilisateur) (facultatif)	Lorsque **dns** est sélectionné, le module ARM redirige le trafic DNS vers Content Gateway. Sinon, le trafic DNS est ignoré.
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont annulées.
	Contournement statique
Static Bypass (Contournement statique)	Présente un tableau répertoriant les règles du *Fichier de configuration bypass.config* qui définissent le comportement du contournement statique transparent. Lorsque la transparence est activée, le proxy utilise ces règles pour déterminer s'il doit ignorer les requêtes de clients entrantes ou tenter de les desservir en transparence.
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **bypass.config**
Edit File (Modifier le fichier)	Permet d'ouvrir le fichier **bypass.config** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier bypass.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration bypass.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Rule Type (Type de règle)	Définit le type de règles : Une règle **bypass** permet d'ignorer les requêtes entrantes spécifiées. Une règle **deny_dyn_bypass** interdit au proxy d'ignorer les requêtes entrantes de clients spécifiées dynamiquement (une règle de refus de contournement peut empêcher Content Gateway de s'ignorer lui-même).

Option	Description
IP source	Définit l'adresse IP source des requêtes entrantes que le proxy doit ignorer ou à laquelle il doit refuser le contournement. L'adresse IP peut être : Une simple adresse IP, telle que 123.45.67.8 Une adresse au format CIDR (Classless Inter-Domain Routing), tel que 1.1.1.0/24 Une plage d'adresses séparées par un tiret, telle que 1.1.1.1-2.2.2.2 Toute combinaison des éléments ci-dessus, séparés par des virgules, telle que 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123
IP de destination	Définit l'adresse IP de destination des requêtes entrantes que le proxy doit ignorer ou à laquelle il doit refuser le contournement. L'adresse IP peut être : Une simple adresse IP, telle que 123.45.67.8 Une adresse au format CIDR (Classless Inter-Domain Routing), tel que 1.1.1.0/24 Une plage d'adresses séparées par un tiret, telle que 1.1.1.1-2.2.2.2 Toute combinaison des éléments ci-dessus, séparés par des virgules, telle que 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.
	Contournement dynamique
Dynamic Bypass (Contournement dynamique)	Active ou désactive l'option de contournement dynamique de manière à ignorer le proxy et à accéder directement au serveur d'origine en cas de problème avec des clients ou des serveurs. Les règles de contournement dynamique sont supprimées lorsque vous arrêtez Content Gateway.
Behavior (Comportement) : Non HTTP, Port 80	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsque Content Gateway rencontre du trafic non HTTP sur le port 80. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsque Content Gateway rencontre du trafic non HTTP sur le port 80. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsque Content Gateway rencontre du trafic non HTTP sur le port 80. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsque Content Gateway rencontre du trafic non HTTP sur le port 80.

Option	Description
Behavior (Comportement) : HTTP 400	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 400. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 400. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 400. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 400.
Behavior (Comportement) : HTTP 401	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 401. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 401. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 401. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 401.
Behavior (Comportement) : HTTP 403	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 403. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 403. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 403. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 403.
Behavior (Comportement) : HTTP 405	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 405. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 405. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 405. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 405.

Option	Description
Behavior (Comportement) : HTTP 406	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 406. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 406. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 406. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 406.
Behavior (Comportement) : HTTP 408	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 408. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 408. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 408. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 408.
Behavior (Comportement) : HTTP 500	Sélectionnez **Enabled (Activé)** pour activer le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 500. Sélectionnez **Disabled (Désactivé)** pour désactiver le contournement dynamique lorsqu'un serveur d'origine renvoie une erreur 500. Sélectionnez **Source-Destination** pour activer le contournement dynamique source/destination lorsqu'un serveur d'origine renvoie une erreur 500. Sélectionnez **Destination Only (Destination uniquement)** pour activer le contournement dynamique de la destination lorsqu'un serveur d'origine renvoie une erreur 500.

WCCP

> **Remarque**
> Les options de configuration WCCP ne s'affichent dans le volet de configuration que si vous avez activé WCCP dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Les options définies dans le fichier de configuration **wccp.config** contrôlent l'utilisation de WCCP avec Content Gateway. Pour définir et gérer les entrées, vous devez utiliser l'éditeur fourni via **Configurer > Networking (Mise en réseau) > WCCP**.

Il est sous-entendu que les administrateurs connaissent déjà bien WCCP.

Seul WCCP v2 est pris en charge.

Nous vous conseillons de consulter la documentation et le site de support du fabricant afin d'obtenir des informations sur la configuration et les performances optimales de votre dispositif WCCP v2. La plupart des périphériques doivent être configurés pour tirer pleinement parti de la redirection matérielle. Avec les dispositifs Cisco, la version la plus récente d'IOS est généralement la meilleure.

Pour chaque groupe de services WCCP actif, une règle de traduction d'adresses réseau ARM correspondante doit exister. Voir *ARM*, page 321.

Lorsque plusieurs serveurs proxy sont configurés dans un cluster, tous les paramètres **sauf** le paramètre d'activation/désactivation du groupe de services, l'interface réseau et le poids se propagent au niveau du cluster.

La description complète de la prise en charge des dispositifs WCCP v2 par Content Gateway est disponible à la section *Interception transparente avec dispositifs WCCP v2*, page 50.

Option	Description
WCCP Service Groups (Groupes de services WCCP)	Présente le tableau des groupes de services définis dans le fichier **wccp.config**. La configuration des groupes de services WCCP définit le comportement WCCP. Les champs des colonnes sont détaillés dans les entrées de l'éditeur de configuration ci-dessous.
Actualiser	Actualise le tableau pour afficher les définitions actuelles du fichier **wccp.config**
Edit File (Modifier le fichier)	Ouvre le fichier **wccp.config** dans l'éditeur de fichiers de configuration
	Éditeur de fichiers de configuration pour le fichier wccp.config
Champ d'affichage des groupes de services	Présente la liste des définitions de groupes de services WCCP Sélectionnez une entrée dans la liste pour la modifier. Servez-vous du bouton « X » pour supprimer la sélection. L'ordre de la liste n'ayant pas d'importance, les flèches haut et bas peuvent être ignorées.
Ajouter	Ajoute une nouvelle définition de groupe de services. Lorsque vous cliquez sur Ajouter, la nouvelle définition s'affiche dans le champ situé en haut de la page.
Set (Définir)	Accepte les modifications apportées à la définition du groupe de services sélectionné, en affichant les nouvelles valeurs dans le champ situé en haut de la page
	Informations du groupe de services
Service Group Status (État du groupe de services)	Active ou désactive ce groupe de services Ce paramètre ne se propage pas au niveau du cluster, un groupe de services pouvant être seulement actif dans les membres sélectionnés. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Option	Description
Service Group Name (Nom du groupe de services)	Définit le nom unique du groupe de services. Ce nom simplifie l'administration.
Service Group ID (ID du groupe de services)	Définit l'ID du groupe de services entre 0 et 255. Cet ID doit également être configuré dans le(s) routeur(s). Si le numéro indiqué est déjà utilisé, une erreur s'affiche lorsque vous cliquez sur Ajouter ou Set (Définir).
Protocole	Définit le protocole, TCP ou UDP, s'appliquant à ce groupe de services
Ports	Définit jusqu'à 8 ports dans une liste séparée par des virgules
Network Interface (Interface réseau)	Définit l'interface Ethernet à utiliser avec ce groupe de services dans ce système hôte Content Gateway
	Négociation du mode
Packet Forward Method (Méthode de transmission des paquets)	Définit la méthode d'encapsulation favorite utilisée par le routeur WCCP pour transmettre le trafic intercepté au proxy. Si le routeur prend en charge les méthodes GRE et L2, la méthode définie ici est utilisée. **Important :** les méthodes GRE et Multicast (Multidiffusion) sont incompatibles.
Packet Return Method (Méthode de renvoi des paquets)	Définit la méthode favorite d'encapsulation des paquets utilisée pour renvoyer le trafic intercepté au routeur WCCP **Remarque** : si Content Gateway est configuré avec une méthode de transmission/retour non prise en charge par le routeur, le proxy tente d'utiliser une méthode que ce routeur prend en charge. **Remarque** : la sélection de L2 implique que le routeur ou le commutateur soit adjacent au Niveau 2 (dans le même sous-réseau que Content Gateway).
	Paramètres avancés
Assignment Method (Méthode d'attribution)	Définit la méthode que le routeur doit utiliser pour distribuer le trafic intercepté vers plusieurs serveurs proxy. Les choix disponibles sont HASH et MASK. La valeur de MASK s'applique au maximum à 6 bits significatifs (dans un cluster, 64 compartiments sont créés au total). Pour plus d'informations sur la méthode d'attribution, consultez votre documentation WCCP. Pour votre dispositif, utilisez la valeur recommandée dans la documentation du fabricant.
Distribution attribute(s) (Attribut(s) de distribution)	Définit l'attribut que la méthode d'attribution doit utiliser pour identifier les requêtes devant être distribuées à tel ou tel serveur proxy. Si la méthode d'attribution est HASH, sélectionnez un ou plusieurs attributs de distribution. Si la méthode d'attribution est MASK, sélectionnez un seul attribut de distribution.

Option	Description
Weight (Poids)	Définit la distribution proportionnelle des requêtes aux serveurs d'un cluster. Définissez le poids sur une valeur correspondant à la proportion souhaitée du flux total de trafic. Si tous les membres du cluster présentent la valeur 0 (par défaut), la distribution est uniforme. Lorsque l'un des membres est défini sur une valeur autre que zéro, la distribution est proportionnelle aux valeurs de poids des autres membres. Les membres dont la valeur est toujours zéro ne reçoivent aucun trafic.
Reverse Service Group ID (ID du groupe de services inverse)	Cette option ne doit être utilisée que si l'usurpation d'adresse IP est activée. Lorsque l'usurpation d'adresse IP est activée, le proxy annonce un groupe de services inverse pour chaque groupe de services de transmission WCCP activé. **Le groupe de services inverse doit être appliqué tout au long du chemin de renvoi des réponses du serveur d'origine au proxy.**
	Informations sur le routeur
Sécurité (facultatif)	Active ou désactive la sécurité, de sorte que le routeur et Content Gateway puissent s'authentifier mutuellement Si vous activez la sécurité dans Content Gateway, vous devez également l'activer au niveau du routeur. Reportez-vous à la documentation de votre routeur. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Sécurité : Mot de passe	Définit le mot de passe utilisé pour l'authentification. Ce mot de passe doit être le même que celui configuré dans le routeur et ne doit pas dépasser huit caractères. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Multicast (Multidiffusion) (facultatif)	Active ou désactive le mode de multidiffusion WCCP **Important :** cette option ne peut pas être utilisée avec la méthode de transmission/renvoi des paquets GRE. Si vous modifiez cette option, vous devez redémarrer Content Gateway.
Multicast (Multidiffusion) : Adresse IP	Définit l'adresse IP de multidiffusion Si vous modifiez cette option, vous devez redémarrer Content Gateway.
WCCP Routers (Routeurs WCCP)	Définit les adresses IP de jusqu'à 10 routeurs de type WCCP v2 Si la méthode de transmission ou de retour des paquets GRE est sélectionnée, spécifiez également l'adresse IP virtuelle de chaque routeur et l'adresse IP d'une passerelle. Les adresses IP virtuelles doivent être uniques. Lorsque la multidiffusion n'est pas activée, les routeurs de votre réseau ne sont pas détectés automatiquement. Si vous modifiez cette option, vous devez redémarrer Content Gateway.

Proxy DNS

> **Remarque**
> Les options de configuration de proxy DNS ne s'affichent dans le volet de configuration que si vous avez activé l'option Proxy DNS dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Option	Description
DNS Proxy Port (Port du proxy DNS)	Définit le port utilisé par Content Gateway pour le trafic DNS. Le port par défaut est le 5353.

Résolveur DNS

Option	Description
	Résolveur
Local Domain Expansion (Extension du domaine local)	Active ou désactive l'extension du domaine local de sorte que Content Gateway puisse tenter de résoudre les noms d'hôte non qualifiés en étendant le domaine local. Par exemple, lorsqu'un client demande un nom d'hôte non qualifié nommé `hostx` et que le domaine local WCG est **y.com**, Content Gateway étend le nom d'hôte en **hostx.y.com**.
	Base de données des hôtes
DNS Lookup Timeout (Expiration des recherches DNS)	Définit le nombre maximal de secondes pendant lesquelles le proxy doit attendre la réponse de la recherche du Serveur de noms de domaine
Foreground Timeout (Expiration de premier plan)	Définit le délai pendant lequel les entrées DNS peuvent rester dans la base de données avant d'être désignées comme périmées Par exemple, si ce délai d'expiration est de 24 heures et que le client demande une entrée présente dans la base de données depuis 24 heures ou davantage, le proxy actualise l'entrée avant de l'envoyer. Attention : définir l'expiration de premier plan sur une valeur trop faible peut ralentir les réponses. Le définir sur une valeur trop élevée peut entraîner une accumulation d'informations incorrectes.
Failed DNS Timeout (Expiration des échecs DNS)	Définit le délai, en secondes, pendant lequel un nom d'hôte doit rester dans le cache des échecs de recherche DNS. Lorsque ce délai expire, le nom d'hôte est supprimé du cache et la demande suivante de ce nom d'hôte est envoyée au serveur DNS.
	Division DNS

Option	Description
Split DNS (Division DNS)	Active ou désactive l'option de division DNS. Lorsque cette option est activée, Content Gateway peut utiliser plusieurs serveurs DNS, selon vos propres conditions de sécurité. Par exemple, vous pouvez configurer le proxy pour qu'il utilise un lot de serveurs DNS pour résoudre les noms d'hôte de votre réseau interne, tout en autorisant les serveurs DNS situés à l'extérieur du pare-feu à résoudre les hôtes situés sur Internet. Pour plus d'informations sur l'utilisation de la division DNS, consultez la section *Utilisation de l'option de division DNS*, page 175.
Default Domain (Domaine par défaut)	Définit le domaine par défaut utilisé pour diviser les requêtes DNS. Lorsque le nom d'hôte n'inclut pas de domaine, Content Gateway lui ajoute le nom de domaine par défaut avant de choisir le serveur DNS à utiliser.
DNS Servers Specification (Spécification des serveurs DNS)	Présente un tableau répertoriant les règles du *Fichier de configuration splitdns.config* qui identifient les serveurs DNS utilisés par le proxy pour résoudre les noms d'hôte dans des conditions spécifiques
Actualiser	Met à jour le tableau pour afficher les règles les plus récentes du fichier **splitdns.config**. Cliquez sur ce bouton après avoir ajouté ou modifié des règles dans l'éditeur de fichiers de configuration.
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des règles dans le fichier **splitdns.config** La page de l'éditeur de fichiers de configuration est décrite ci-dessous.
	Éditeur de fichiers de configuration pour le fichier splitdns.config
Champ d'affichage des règles	Répertorie les règles du *Fichier de configuration splitdns.config*. Sélectionnez une règle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer la règle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle règle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration. Renseignez les champs fournis avant de cliquer sur ce bouton.
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration. Avant de cliquer sur ce bouton, sélectionnez une règle et modifiez ses propriétés.
Primary Destination Type (Type de destination principale)	Indique que la sélection du serveur DNS est basée sur le domaine de destination (`dest_domain`), l'hôte de destination (`dest_host`) ou une expression régulière (`url_regex`)
Primary Destination Value (Valeur de la destination principale)	Définit la valeur de la destination principale. Placez le symbole « ! » au début de cette valeur pour spécifier l'opérateur logique NOT.
DNS Server IP (Adresse IP du serveur DNS)	Définit le serveur DNS à utiliser avec le spécificateur de destination principale. Vous pouvez spécifier un port en utilisant le caractère deux points (`:`). Si vous ne spécifiez pas de port, le port 53 est utilisé. Vous pouvez spécifier plusieurs serveurs DNS séparés par des espaces ou des point-virgules (`;`).

Option	Description
Default Domain Name (Nom du domaine par défaut) (facultatif)	Définit le nom de domaine par défaut à utiliser pour la résolution des hôtes. Une seule entrée est autorisée. Si vous ne fournissez pas de domaine par défaut, le système détermine sa valeur via le fichier **/etc/resolv.conf**.
Domain Search List (Liste des domaines de recherche) (facultatif)	Définit l'ordre de recherche des domaines. Vous pouvez spécifier plusieurs domaines séparés par des espaces ou des point-virgules (`;`). Si vous ne fournissez pas de liste de recherches, le système détermine sa valeur via le fichier **/etc/resolv.conf**.
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

ICAP

> **Remarque**
> L'option de configuration ICAP ne s'affiche dans le volet Configurer que si vous avez activé l'option **ICAP** dans le tableau **Features (Fonctions)** de l'onglet **Configurer > Mon proxy > De base > Général**.

ICAP est une interface alternative à Websense Data Security et aux autres services de sécurité des données qui reconnaissent ICAP. Il est possible de spécifier un URI principal et de sauvegarde et de configurer le basculement et l'équilibrage de la charge. Voir *Configuration du client ICAP*, page 125 et la sous-section suivante *Basculement ICAP et équilibrage de la charge*, page 126.

Option	Description
ICAP Service URI (URI du service ICAP)	Définit l'URI (Uniform Resource Identifier) du service ICAP. Le format est le suivant : `icap://`*nomdhôte*`:`*port*`/`*chemin* Par exemple : `icap://ICAP_machine:1344/REQMOD` Le port ICAP par défaut est le 1344. Il n'est pas nécessaire de spécifier ce port dans l'URI si vous utilisez le port ICAP par défaut. Un service URI secondaire facultatif peut être spécifié immédiatement après le premier en ajoutant une virgule et l'URI du second service, sans espace.
Analyze HTTPS Content (Analyser le contenu HTTPS)	Indiquez si le trafic décrypté doit être envoyé à Data Security Suite pour analyse ou envoyé directement à destination.

Option	Description
Analyze FTP Uploads (Analyser les chargements FTP)	Indiquez si les requêtes de chargement FTP doivent être envoyées à Websense Data Security Suite pour analyse. La fonction de proxy FTP doit être activée. Voir *FTP*, page 288.
Action for Communication Errors (Action pour erreurs de communication)	Indiquez si le trafic doit être autorisé ou si une page de blocage doit être envoyée lorsque Content Gateway reçoit une erreur lors de la communication avec Websense Data Security Suite.
Action for Large files (Action pour les fichiers volumineux)	Choisissez d'autoriser le trafic ou d'envoyer une page de blocage lorsque la taille du fichier envoyé dépasse la limite définie dans DSS. Dans DSS, la limite de taille par défaut est de 12 Mo.

IP virtuel

Remarque

Les options de configuration IP virtuel ne s'affichent dans le volet de configuration que si vous avez activé l'option IP virtuel dans le tableau des fonctions de l'onglet **Configurer > Mon proxy > De base > Général**.

Option	Description
Adresses IP virtuelles	Présente un tableau répertoriant les adresses IP virtuelles gérées par Content Gateway
Actualiser	Met à jour le tableau pour afficher la liste d'adresses IP virtuelles la plus récente. Cliquez sur ce bouton après avoir ajouté ou modifié la liste des adresses IP virtuelles dans l'éditeur de fichiers de configuration.
Edit File (Modifier le fichier)	Ouvre l'éditeur de fichiers de configuration qui vous permet de modifier et d'ajouter des adresses dans la liste des adresses IP virtuelles
	Éditeur de fichiers de configuration pour le fichier vaddrs.config
Champ d'affichage des règles	Présente la liste des adresses IP virtuelles. Sélectionnez une adresse IP virtuelle pour la modifier. Les boutons de gauche vous permettent de supprimer ou de déplacer l'adresse IP virtuelle sélectionnée vers le haut ou le bas de la liste.
Ajouter	Ajoute une nouvelle adresse IP virtuelle dans le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration
Set (Définir)	Actualise le champ d'affichage des règles en haut de la page de l'éditeur de fichiers de configuration.
Adresse IP virtuelle	Définit l'adresse IP virtuelle gérée par Content Gateway
Interface Ethernet	Définit l'interface réseau attribuée à cette adresse IP virtuelle
Sub-Interface (Sous-interface)	Définit l'ID de sous-interface. Cet identifiant est un nombre compris entre 1 et 255 utilisé par l'interface pour cette adresse.

Option	Description
Appliquer	Applique les modifications de la configuration
Fermer	Ferme l'éditeur de fichiers de configuration. Cliquez sur **Appliquer** avant de cliquer sur **Fermer**, sinon toutes les modifications apportées à la configuration sont perdues.

SSL

Les options de configuration SSL se répartissent dans les catégories suivantes :

- Certificats (voir *Gestion des certificats*, page 141)
- Décryptage/Cryptage (voir *Configuration de SSL Manager pour le trafic entrant*, page 144, et *Configuration de SSL Manager pour le trafic entrant*, page 145)
- Validation (voir *Validation des certificats*, page 146)
- Incidents (voir *Gestion des accès aux sites Web HTTPS*, page 152)
- Certificats des clients (voir *Certificats des clients*, page 156)
- Journalisation (voir *Configuration de la journalisation de SSL Manager*, page 158)
- Personnalisation (voir *Personnalisation des messages d'échec des connexions SSL*, page 161)
- Autorité de certification racine interne (voir *Autorité de certification racine interne*, page 134)

D Formats de journalisation des événements

Champs de journalisation personnalisés

Rubrique connexe :

- *Référence croisée pour le format de journalisation*, page 341

%<symbole du champ>	Description
{*nom du champ d'en-tête HTTP*}cqh	Journalise les informations dans le champ demandé de l'en-tête HTTP de la requête du client ; par exemple, %<{Accept-Language}cqh> journalise le contenu du champ **Accept-Language:** dans les en-têtes de la requête des clients. Ce champ ne peut pas être utilisé dans les filtres de journaux personnalisés.
{*nom du champ d'en-tête HTTP*}cqhua	Journalise les informations dans le champ demandé de l'en-tête HTTP de la requête du client ; par exemple, %<{User-Agent}cqhua> journalise le contenu du champ **User-Agent:** dans les en-têtes de la requête des clients.
{*nom du champ d'en-tête HTTP*}pqh	Journalise les informations dans le champ demandé de l'en-tête HTTP de la requête du proxy ; par exemple, %<{Authorization}pqh> journalise le contenu du champ **Authorization:** dans les en-têtes de la requête du proxy. Ce champ ne peut pas être utilisé dans les filtres de journaux personnalisés.
{*nom du champ d'en-tête HTTP*}psh	Journalise les informations dans le champ demandé de l'en-tête HTTP de la réponse du proxy ; par exemple, %<{Retry-After}psh> journalise le contenu du champ **Retry-After:** dans les en-têtes de la réponse du proxy. Ce champ ne peut pas être utilisé dans les filtres de journaux personnalisés.

%<symbole du champ>	Description
{*nom du champ d'en-tête HTTP*}ssh	Journalise les informations dans le champ demandé de l'en-tête HTTP de la réponse du serveur ; par exemple, %<{Age}ssh> journalise le contenu du champ **Age:** dans les en-têtes de la réponse du serveur. Ce champ ne peut pas être utilisé dans les filtres de journaux personnalisés.
caun	Nom d'utilisateur authentifié du client ; résultat de la recherche RFC931/ident du nom d'utilisateur du client
cfsc	Code de fin de l'état du client ; spécifie si la demande du client envoyée au proxy a été satisfaite (FIN) ou interrompue (INTR)
chi	Adresse IP de l'hôte du client ; adresse IP de l'ordinateur hôte du client
cqbl	Longueur du transfert de la requête du client ; taille du corps de la requête envoyée à Content Gateway en octets
cqhl	Longueur de l'en-tête de la requête du client; taille de l'en-tête de la requête envoyée à Content Gateway
cqhm	Méthode HTTP de la requête du client envoyée à Content Gateway : GET, POST, etc. (sous-ensemble de cqtx)
cqhv	Version HTTP de la requête du client
cqtd	Horodatage de la requête du client ; spécifie la date de la requête du client au format *aaaa-mm-jj*, où *aaaa* correspond à l'année en 4-chiffres, *mm* au mois en 2 chiffres et *jj* au jour en 2 chiffres
cqtn	Horodatage de la requête du client ; date et heure de la requête du client (au format Netscape)
cqtq	Horodatage de la requête du client avec résolution en millisecondes
cqts	Horodatage de la requête du client au format Squid ; heure de la requête du client en secondes à compter du 1er janvier 1970
cqtt	Horodatage de la requête du client ; heure de la requête du client au format *hh:mm:ss*, où *hh* correspond à l'heure sur 2 chiffres au format 24 heures, *mm* aux minutes sur 2 chiffres et *ss* aux secondes sur 2 chiffres Par exemple, 16:01:19.
cqtx	Texte intégral de la requête HTTP du client, moins les en-têtes. Par exemple : GET http://www.entreprise.com HTTP/1.0
cqu	URI de la requête du client ; URI (Uniform Resource Identifier) de la requête du client envoyée à Content Gateway (sous-ensemble de cqtx)

%<symbole du champ>	Description
cquc	URL canonique (CNAME) de la requête du client ; diffère de la commande cqu car les espaces (et les autres caractères susceptibles de ne pas être analysés par les outils des journaux) sont remplacés par des séquences d'échappement. La séquence d'échappement est un symbole de pourcentage suivi par le code ASCII en hexadécimal.
cqup	Chemin de l'URL de la requête du client ; spécifie la partie argument de l'URL (tout ce qui suit l'hôte). Par exemple, si l'URL est **http://www.entreprise.com/images/x.gif**, ce champ affiche **/images/x.gif**.
cqus	Schéma de l'URL de la requête du client (HTTP, FTP, etc.)
crc	Code de résultat du cache ; spécifie la manière dont le cache a répondu à la requête (accès fructueux (HIT), accès infructueux (MISS), etc.)
pfsc	Code de fin de l'état du proxy ; spécifie si la demande de Content Gateway envoyée au serveur d'origine a été satisfaite (FIN) ou interrompue (INTR)
phn	Nom d'hôte du serveur Content Gateway qui a généré cette entrée dans les fichiers journaux assemblés
phr	Itinéraire hiérarchique du proxy ; itinéraire suivi par Content Gateway pour récupérer l'objet
pqbl	Longueur du transfert de la requête du proxy ; taille du corps de la requête de Content Gateway envoyée au serveur d'origine
pqhl	Longueur de l'en-tête de la requête du proxy; taille de l'en-tête de la requête de Content Gateway envoyée au serveur d'origine
pqsi	Adresse IP du serveur de la requête envoyée au proxy (0 pour les accès au cache et parent-ip pour les requêtes envoyées aux proxy parents)
pqsn	Nom du serveur de la requête envoyée au proxy ; nom du serveur qui a satisfait la requête
pscl	Longueur du transfert de la réponse envoyée au proxy ; longueur de la réponse de Content Gateway envoyée au client, en octets
psct	Type de contenu de la réponse envoyée au proxy ; type de contenu du document (par exemple, img/gif) indiqué dans l'en-tête de la réponse du serveur
pshl	Longueur de l'en-tête de la réponse envoyée au proxy; longueur de l'en-tête de la réponse de Content Gateway envoyée au client
psql	Longueur de l'en-tête de la réponse envoyée au proxy au format Squid (inclut la longueur de l'en-tête et du contenu)
pssc	Code d'état de la réponse du proxy ; code d'état de la réponse HTTP envoyée par Content Gateway au client

%<symbole du champ>	Description
shi	Adresse IP résolue par la recherche du nom DNS de l'hôte dans la requête. Pour les hôtes ayant plusieurs adresses IP, ce champ enregistre les adresses IP résolues par cette recherche DNS. Ceci peut conduire par erreur vers des documents mis en cache. Par exemple, si la première requête était un accès infructueux au cache et provenait de l'adresse IP1 pour le serveur S et que la seconde requête du serveur S a conduit à l'adresse IP2 mais provenait du cache, l'entrée du journal affichera l'adresse IP2 pour la seconde requête.
shn	Nom d'hôte du serveur d'origine
sscl	Longueur du transfert de la réponse du serveur ; longueur de la réponse, en octets, entre le serveur d'origine et Content Gateway
sshl	Longueur de l'en-tête de la réponse du serveur ; longueur de l'en-tête de la réponse du serveur d'origine envoyée à Content Gateway, en octets
sshv	Version HTTP de la réponse du serveur (1.0, 1.1, etc.)
sssc	Code d'état de la réponse du serveur ; code d'état de la réponse HTTP du serveur d'origine à Content Gateway
ttms	Temps consacré par Content Gateway au traitement de la requête du client ; nombre de millisecondes écoulé entre le moment où le client établit la connexion à Content Gateway et le moment où Content Gateway lui renvoie le dernier octet de la réponse
ttmsf	Temps consacré par Content Gateway au traitement de la requête du client sous forme d'un nombre de secondes fractionné ; spécifie la durée de la résolution en millisecondes mais, au lieu de formater le résultat sous forme d'entier (comme pour *ttms*), le résultat est un nombre en virgule flottante représentant un nombre de secondes fractionné. Par exemple, si la durée est 1 500 millisecondes, ce champ affiche 1,5 alors que le champ **ttms** affiche 1500 et le champ **tts** affiche uniquement 1.
tts	Temps consacré par Content Gateway au traitement de la requête du client; nombre de secondes écoulé entre le moment où le client établit la connexion au proxy et le moment où ce dernier lui renvoie le dernier octet de la réponse
wc	Catégorie prédéfinie ou personnalisée de l'URL des données analysées. Par exemple, « Actualités et médias ».
wct	Type de contenu de la page Web. Par exemple, « text/ html; charset=UTF-8 ».
wsds	Chaîne de disposition de l'analyse, telle que CATEGORY_BLOCKED, PERMIT_ALL, FILTERED_AND_PASSED, etc.

%<symbole du champ>	Description
wsr	Bit d'analyse recommandé (« true » ou « false »). La base de données des URL identifie et recommande quelles données doivent être davantage analysées. Selon la stratégie utilisée, les données seront ou non analysées davantage.
wstms	Durée de l'analyse en millisecondes d'une page ou d'un fichier téléchargé(e)
wui	ID de l'utilisateur authentifié qui sert à sélectionner la stratégie à appliquer pour l'analyse des données de la requête du client

Référence croisée pour le format de journalisation

Les sections suivantes illustrent la correspondance entre les champs de journalisation de Content Gateway et les champs de journalisation standard des formats Squid et Netscape.

Formats de journalisation Squid

Squid	Symbole du champ Content Gateway
time	cqts
elapsed	ttms
client	chi
action/code	crc/pssc
size	psql
method	cqhm
url	cquc
ident	caun
hierarchy/from	phr/pqsn
contenu	psct

Par exemple, si vous souhaitez créer un format personnalisé appelé `short_sq` basé sur les trois premiers champs Squid, entrez une ligne dans le fichier **logs.config** comme suit :

```
format:enabled:1:short_sq:%<cqts> %<ttms>
%<chi>:short_sq:ASCII:none
```

Pour plus d'informations sur la définition des fichiers journaux personnalisés, consultez la section *Format personnalisé*, page 216.

Formats de journalisation Netscape Common

Netscape Common	Symbole du champ Content Gateway
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtx”
s1	pssc
c1	pscl

Formats de journalisation Netscape Extended

Netscape Extended	Symbole du champ Content Gateway
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtx”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts

Formats de journalisation Netscape Extended-2

Netscape Extended-2	Symbole du champ Content Gateway
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtx”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts
route	phr
pfs	cfsc
ss	pfsc
crc	crc

E Fichiers de configuration

Websense Content Gateway comprend les fichiers de configuration suivants, que vous pouvez modifier pour personnaliser le proxy.

Définition des expressions régulières d'URL (url_regex)

Dans les fichiers de configuration, les entrées de type `url_regex` établissent des correspondances à l'aide d'expressions régulières.

Les exemples donnés dans le tableau suivant illustrent la création d'une entrée `url_regex` valide.

Valeur	Description
x	Correspond au caractère x
.	Correspond à n'importe quel caractère
^	Définit le début d'une ligne
$	Définit la fin d'une ligne
[xyz]	*Classe de caractères*. Dans ce cas, le modèle correspond aux caractères x, y ou z.
[abj-oZ]	*Classe de caractères* au sein d'une plage. Ce modèle correspond aux caractères a et b, à n'importe quelle lettre de la plage j à o ou au caractère Z.
[^A-Z]	*Classe de caractères niés*. Ce modèle correspond par exemple à n'importe quel caractère, sauf ceux de la classe.
r*	Zéro ou plusieurs r, où r est une expression régulière quelconque
r+	Un ou plusieurs r, où r est une expression régulière quelconque
r?	Zéro ou un r, où r est une expression régulière quelconque
r{2,5}	De deux à cinq r, où r est une expression régulière quelconque
r{2,}	Deux ou plusieurs r, où r est une expression régulière quelconque
r{4}	4 r exactement, où r est une expression régulière quelconque
"[xyz]\"images"	Chaîne littérale [xyz]"images"
\X	Si X correspond à un caractère a, b, f, n, r, t ou v, interprétation ANSI-C de \x. Sinon, un X littéral. Permet d'éviter les opérateurs tels que *.
\0	Caractère NULL
\123	Caractère de valeur octale 123
\x2a	Caractère de valeur hexadécimale 2a
(r)	Correspond à un r, où r est une expression régulière quelconque. Vous pouvez utiliser des parenthèses pour ignorer la priorité.
rs	Expression régulière r, suivie de l'expression régulière s
r|s	Expression régulière r ou s
#<n>#	Insère un nœud de *end* entraînant l'arrêt de l'expression régulière correspondante lorsque ce nœud est atteint. La valeur n est renvoyée.

Exemples

Vous pouvez spécifier `dest_domain=mondomaine.com` pour établir une correspondance avec n'importe quel hôte de *mondomaine.com*. De la même façon, vous pouvez spécifier `dest_domain=.` pour établir une correspondance avec n'importe quelle requête.

Fichier de configuration auth.config

Le fichier **auth.config** stocke les règles qui dirigent les adresses IP et les plages d'adresses IP spécifiées, et/ou le trafic passant par les ports entrants spécifiés (proxy explicite uniquement) vers des contrôleurs de domaine distincts. Cette fonction est appelée *Authentification dans plusieurs domaines Kerberos*, page 194. Les règles d'authentification dans plusieurs domaines Kerberos sont définies dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)**.

- L'Authentification dans plusieurs domaines Kerberos est prise en charge pour l'Authentification Windows intégrée (IWA), l'authentification NTLM héritée et l'authentification LDAP uniquement.
- Chaque règle d'authentification définit les adresses IP sources et/ou le port entrant (proxy explicite uniquement), la méthode d'authentification, le domaine et les autres options associées.
- Plusieurs règles peuvent être actives en même temps. Il est donc possible d'utiliser plusieurs méthodes d'authentification simultanément.
- Les spécificateurs utilisés dans les règles IWA, LDAP et NTLM diffèrent.
- Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas. Seule la première correspondance s'applique. Lorsque l'adresse IP ne correspond à aucune règle, aucune authentification n'est tentée.

> **Remarque**
> Si tous les clients de votre réseau sont authentifiés par des serveurs d'authentification partageant des relations de confiance, vous n'avez pas besoin de créer des règles pour l'authentification dans plusieurs domaines Kerberos.

Format

Chaque ligne du fichier **auth.config** contient une règle d'authentification composée d'un jeu de balises, suivies de leur valeur. Le format des règles d'authentification est le suivant :

type=<type_auth> name=<nom_profil> src_ip=<adresses IP> <balises supplémentaires>

Le tableau suivant répertorie les balises communes à l'ensemble des règles.

Balises universelles	Valeur autorisée
type	Chaîne identifiant le type de règle : winauth, ntlm, ldap
enabled (activé)	Indique si la règle doit être active : • `0` = désactivé • `1` = activé
name	Non simple et unique utilisé dans la journalisation
src_ip	Accepte une liste d'adresses IP ou de plages d'adresses IP séparées par des virgules
proxy_port (facultatif)	Accepte un numéro de port
use_alias	Définit le nom d'utilisateur envoyé au service de filtrage lorsque l'authentification réussit • `0` = envoie le nom réel de l'utilisateur authentifié (par défaut) • `1` = envoie un nom d'utilisateur vide • `2` = envoie la chaîne définie dans auth_name_string
auth_name_string	Active uniquement si la balise use_alias=2. Définit la chaîne statique à envoyer comme nom d'utilisateur pour toutes les authentifications réussies qui utilisent cette règle.

Le tableau suivant répertorie les autres balises utilisées dans les règles d'Authentification Windows intégrée.

Balises IWA	Valeur autorisée
winauth_realm	Définit le domaine Windows joint à utiliser avec la règle. Content Gateway doit être joint et actif dans ce domaine.

Le tableau suivant répertorie les autres balises utilisées dans une règle NTLM.

Balises universelles	Valeur autorisée
dc_list	Accepte l'adresse IP et le numéro de port du contrôleur de domaine principal (lorsqu'aucun port n'est défini, Content Gateway utilise le port 139), suivis de la liste des contrôleurs de domaine secondaires, séparés par des virgules, à utiliser pour l'équilibrage de la charge et le basculement
dc_load_balance (facultatif)	Définit le mode d'utilisation de l'équilibrage de la charge : • `0` = désactivé • `1` = activé **Remarque :** lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé.

Le tableau suivant répertorie les autres balises utilisées dans une règle LDAP.

Balise LDAP	Valeur autorisée
server_name	Définit le nom de domaine complet du serveur LDAP
server_port (facultatif)	Définit le port du serveur LDAP. La valeur par défaut est 389. Si l'option Secure LDAP (LDAP sécurisé) est activée, définissez le port sur 636 ou 3269 (ports LDAP sécurisés).
base_dn (facultatif)	Définit le nom unique de la base de recherche LDAP
uid_filter (facultatif)	Définit le type de service lorsque celui-ci diffère de celui configuré dans l'onglet LDAP. Entrez **sAMAccountName** pour Active Directory ou **uid** pour les autres services.
bind_dn (facultatif)	Définit le nom distinctif de liaison. Il doit s'agir du nom distinctif complet d'un utilisateur du service d'annuaire LDAP. Par exemple : CN=John Smith,CN=USERS,DC=MASOCIETE, DC=COM
bind_pwd (facultatif)	Définit le mot de passe du nom distinctif de liaison
sec_bind	Indique si Content Gateway doit établir une communication sécurisée avec le serveur LDAP • 0 = désactivé • 1 = activé Lorsque cette option est activée, définissez le port sur 636 ou 3269 (ports LDAP sécurisés).
attr	Définit le nom d'un attribut LDAP
attr_value	Définit la valeur d'un attribut LDAP

Exemples

Authentification Windows intégrée :

```
type=winauth name=CorpHQ src_ip=10.1.1.1,10.10.0.0-
10.100.254.254 proxy_port=0 status=1 domain=BigCorp.com
```

NTLM :

```
type=ntlm name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128
dc_list=HQdc1.BigCorp.com,HQdc2.BigCorp.com
```

LDAP :

```
type=ldap name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128
server_name=HQldap1.BigCorp.com server_port=389
```

> **Remarque**
> Les règles s'appliquent selon leur ordre d'apparition dans la liste, la première correspondance étant appliquée.

Fichier de configuration bypass.config

Le fichier **bypass.config** contient les règles de contournement *statique* utilisées par Content Gateway en mode proxy transparent. Ces règles de contournement statique demandent à Content Gateway d'ignorer certaines requêtes entrantes de clients pour qu'elles soient desservies par le serveur d'origine.

Le fichier **bypass.config** accepte également des règles de refus de contournement *dynamique*. Voir *Règles de refus de contournement dynamique*, page 351.

Vous pouvez configurer trois types de règles de contournement statique :

- Les règles de *contournement de la source* configurent le proxy pour qu'il ignore une adresse IP source ou une plage d'adresses IP sources spécifique. Par exemple, vous pouvez ignorer les clients qui ne veulent pas utiliser la mise en cache.
- Les règles de *contournement de la destination* configurent le proxy pour qu'il ignore une adresse IP de destination ou une plage d'adresses IP de destination spécifique. Vous pouvez par exemple ignorer les serveurs d'origine qui utilisent l'authentification IP en se basant sur l'adresse IP réelle du client.

Important

Les règles de contournement de la destination empêchent le proxy de mettre en cache la totalité d'un site. Si le site contourné est populaire, l'impact sera important en termes de taux d'accès.

- Les règles de contournement de *paires source/destination* configurent le proxy de sorte qu'il ignore les requêtes provenant de la source spécifiée et destinées à la cible spécifiée. Par exemple, vous pouvez détourner les paires client/serveur qui rencontrent des problèmes d'authentification IP rompue ou de trafic HTTP hors plage lors de la mise en cache. Les règles de contournement de source/destination sont parfois préférables aux règles de destination, car elles ne bloquent un serveur de destination que pour les utilisateurs qui rencontrent des problèmes.

Format

Le format des règles de contournement est le suivant :

```
bypass src adresseIP | dst adresseIP | src adresseIP AND dst
adresseIP
```

Option	Description
src *adresseIP*	Définit l'adresse IP source (client) des requêtes entrantes que le proxy doit ignorer L'*adresseIP* peut être : Une simple adresse IP, telle que `123.45.67.8` • Une adresse au format CIDR (Classless Inter-Domain Routing), tel que `1.1.1.0/24` • Une plage séparée par un tiret, telle que `1.1.1.1-2.2.2.2` • Toute combinaison des éléments ci-dessus, séparés par des virgules, telle que `1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123`
dst *adresseIP*	Définit l'adresse IP de destination (serveur d'origine) des requêtes entrantes que le proxy doit ignorer L'*adresseIP* peut être : Une simple adresse IP, telle que `123.45.67.8` • Une adresse au format CIDR (Classless Inter-Domain Routing), tel que `1.1.1.0/24` • Une plage séparée par un tiret, telle que `1.1.1.1-2.2.2.2` • Toute combinaison des éléments ci-dessus, séparés par des virgules, telle que `1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123`
src *adresseIP* AND dst *adresseIP*	Définit la paire d'adresses IP source et de destination que le proxy doit ignorer *adresseIP* doit être une adresse IP unique, telle que `123.45.67.8`.

Règles de refus de contournement dynamique

Outre les règles de contournement statique, le fichier **bypass.config** accepte également des règles de *refus de contournement dynamique*.

Les règles de refus de contournement interdisent au proxy d'ignorer certaines requêtes entrantes de clients dynamiquement (une règle de refus de contournement peut empêcher le proxy de s'ignorer lui-même). Les règles de refus de contournement dynamique peuvent correspondre à une source, à une destination ou à une paire source/destination et présentent le format suivant :

```
deny_dyn_bypass src adresseIP | dst adresseIP | src
adresseIP AND dst adresseIP
```

La description de ces options est disponible dans le tableau de la section *Format*, page 351.

> **Remarque**
> Pour que les règles de refus de contournement dynamique fonctionnent, vous devez activer l'option **Dynamic Bypass (Contournement dynamique)** dans Content Gateway Manager ou définir la variable *proxy.config.arm.bypass_dynamic_enabled* sur `1` dans le fichier **records.config**.

> **Important**
> Les règles de contournement statique sont prioritaires sur les règles de refus de contournement dynamique. Par conséquent, lorsque la règle de contournement statique et la règle de contournement dynamique contiennent la même adresse IP, la règle de refus de contournement dynamique est ignorée.

Exemples

L'exemple suivant illustre des règles de *contournement* de source, destination et source/destination :

```
bypass src 1.1.1.0/24, 25.25.25.25, 128.252.11.11-
128.252.11.255
bypass dst 24.24.24.0/24
bypass src 25.25.25.25 AND dst 24.24.24.0
```

L'exemple suivant illustre des règles de *refus de contournement dynamique* de source, destination et source/destination :

```
deny_dyn_bypass src 128.252.11.11-128.252.11.255
deny_dyn_bypass dst 111.111.11.1
deny_dyn_bypass src 111.11.11.1 AND dst 111.11.1.1
```

Fichier de configuration cache.config

Le fichier **cache.config** définit le mode de mise en cache des objets Web par le proxy. Vous pouvez ajouter des règles de mise en cache pour spécifier la configuration suivante :

- Ne pas mettre en cache les objets provenant d'adresses IP spécifiques
- Délai d'épinglage de certains objets dans le cache
- Délai pendant lequel les objets mis en cache sont considérés comme récents

- Ignorer ou non les directives de non mise en cache du serveur (no-cache)

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Chaque ligne du fichier **cache.config** contient une règle de mise en cache. Content Gateway reconnaît trois balises délimitées par un espace :

```
primary_destination=valeur secondary_specifier=valeur
action=valeur
```

Le tableau suivant répertorie les destinations principales possibles et leurs valeurs autorisées.

Destination principale	Valeur autorisée
dest_domain	Nom du domaine demandé
dest_host	Nom de l'hôte demandé
dest_ip	Adresse IP demandée
url_regex	Expression régulière que l'on retrouve dans une URL

Dans le fichier **cache.config**, les spécificateurs secondaires sont facultatifs. Le tableau suivant répertorie les spécificateurs secondaires possibles et leurs valeurs autorisées.

Remarque

Plusieurs spécificateurs secondaires peuvent être utilisés dans une même règle. Vous ne pouvez cependant pas répéter un même spécificateur secondaire.

Spécificateur secondaire	Valeur autorisée
port	Port d'URL demandé
scheme	Protocole d'URL demandé, l'un des deux suivants : • `HTTP` • `FTP`
prefix	Préfixe du chemin d'une URL
suffix	Suffixe de fichier dans l'URL

Spécificateur secondaire	Valeur autorisée
method	Méthode d'URL demandée, l'une des deux suivantes : • `get` • `put` • `trace`
time	Plage horaire, par exemple 08:00-14:00
src_ip	Adresse IP du client
user_agent	Valeur User-Agent de l'en-tête de la requête

Le tableau suivant répertorie les actions possibles et leurs valeurs autorisées.

Action	Valeur
action	L'une des valeurs suivantes : • `never-cache` configure le proxy de sorte qu'il ne mette jamais en cache les objets spécifiés. • `ignore-no-cache` configure le proxy de sorte qu'il ignore tous les en-têtes `Cache-Control: no-cache`. • `ignore-client-no-cache` configure le proxy de sorte qu'il ignore les en-têtes `Cache-Control: no-cache` des requêtes de clients. • `ignore-server-no-cache` configure le proxy de sorte qu'il ignore les en-têtes `Cache-Control: no-cache` des réponses du serveur d'origine.
pin-in-cache	Délai de conservation du ou des objets dans le cache. Les formats disponibles sont les suivants : • *d* pour jours (days) (par exemple, `2d`) • *h* pour heures (par exemple, `10h`) • *m* pour minutes (par exemple, `5m`) • *s* pour secondes (par exemple, `20s`) • Combinaison des unités (par exemple, `1h15m20s`)
revalidate	Délai pendant lequel le ou les objets doivent être considérés comme récents. Les formats horaires sont les mêmes que pour l'action `pin-in-cache`.
ttl-in-cache	Délai pendant lequel les objets doivent rester dans le cache, quels que soient les en-têtes de réponse Cache-Control. Les formats horaires sont les mêmes que pour les actions `pin-in-cache` et `revalidate`.

Exemples

L'exemple suivant configure le proxy de sorte qu'il ne mette jamais en cache les documents FTP demandés à partir de l'adresse IP 112.12.12.12 :

```
dest_ip=112.12.12.12 scheme=ftp action=never-cache
```

L'exemple suivant configure le proxy pour qu'il conserve les documents présentant des URL contenant l'expression régulière `politique` et le chemin **prefix/viewpoint** dans le cache pendant 12 heures :

```
url_regex=politique prefix=/viewpoint pin-in-cache=12h
```

L'exemple suivant demande au proxy de revalider les objets `gif` et `jpeg` du domaine `mondomaine.com` toutes les 6 heures et tous les autres objets de `mondomaine.com` toutes les heures :

```
dest_domain=mondomaine.com suffix=gif revalidate=6h
dest_domain=mondomaine.com suffix=jpeg revalidate=6h
dest_domain=mondomaine.com revalidate=1h
```

> **Remarque**
> Les règles s'appliquent selon leur ordre d'apparition dans la liste.

Fichier de configuration filter.config

Les règles de filtrage définies dans le fichier **filter.config** vous permettent d'effectuer les opérations suivantes :

- Refuser ou autoriser des requêtes d'URL
- Conserver ou supprimer les informations d'en-tête dans les requêtes des clients
- Insérer des en-têtes personnalisés
- Autoriser certaines applications ou requêtes de sites Web à contourner l'authentification
- Empêcher les applications spécifiées de passer par le proxy

Les règles de filtrages doivent être définies dans l'onglet **Configurer > Sécurité > Access Control (Contrôle d'accès) > Filtering (Filtrage)** de Content Gateway Manager. Voir *Création de règles de filtrage*, page 168.

> **Remarque**
> Les règles de filtrage NTLM et LDAP sont définies dans l'onglet **Access Control (Contrôle d'accès) > Authentication Realms (Authentification des domaines Kerberos)** et stockées dans le *Fichier de configuration auth.config*.

Important

Après avoir modifié le fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Chaque ligne du fichier **filter.config** correspond à une règle de filtrage. Content Gateway applique les règles selon leur ordre d'apparition dans la liste, en commençant à partir du haut. Lorsque aucune règle ne correspond, la requête poursuit sa route.

Content Gateway reconnaît trois balises délimitées par un espace :

```
primary_destination=valeur secondary_specifier=valeur
action=valeur
```

Le tableau suivant répertorie les différents types de destination principale possibles.

Type de destination principale	Valeur autorisée
dest_domain	Nom du domaine demandé
dest_host	Nom de l'hôte demandé
dest_ip	Adresse IP demandée
url_regex	Expression régulière que l'on retrouve dans une URL

Les spécificateurs secondaires sont facultatifs. Le tableau suivant répertorie les spécificateurs secondaires possibles et leur objectif.

Remarque

Plusieurs spécificateurs secondaires peuvent être utilisés dans une même règle. Vous ne pouvez cependant pas répéter un même spécificateur secondaire.

Spécificateur secondaire	Valeur autorisée
time	Plage horaire, par exemple 08:00-14:00
prefix	Préfixe du chemin d'une URL
suffix	Suffixe de fichier dans l'URL
src_ip	Adresse IP unique d'un client ou plage d'adresses IP de clients

Spécificateur secondaire	Valeur autorisée
port	Port d'URL demandé
method	Méthode d'URL demandée, l'une des deux suivantes : • `get` • `post` • `put` • `trace`
scheme	Protocole d'URL demandé. Vous pouvez spécifier l'un des protocoles suivants : • `HTTP` • `HTTPS` • `FTP` (pour FTP sur HTTP uniquement)
user_agent	Valeur User-Agent de l'en-tête de la requête

Le tableau suivant répertorie les actions possibles et leurs valeurs autorisées.

Action	Valeur autorisée
action	Spécifiez l'un des éléments suivants : • **allow** : pour autoriser certaines requêtes d'URL à contourner l'authentification. Le proxy met en cache, puis dessert le contenu demandé. • **deny** : pour refuser les demandes d'objets HTTP ou FTP de certaines destinations. Lorsqu'une requête est refusée, le client reçoit un message d'accès refusé. • **radius** : non pris en charge
keep_hdr	Informations d'en-tête de requête de client que vous souhaitez conserver. Vous pouvez spécifier les options suivantes : • date • host • cookie • client_ip
strip_hdr	Informations d'en-tête de requête de client que vous souhaitez supprimer. Les options sont les mêmes que pour **keep_hdr**.
add_hdr	Valeur de l'en-tête personnalisé que vous souhaitez ajouter. Implique que l'en-tête personnalisé et sa valeur soient spécifiés. Par exemple : `add_hdr="nom_entête:valeur_entête"`

Exemples

L'exemple suivant demande à Content Gateway de refuser toutes les requêtes de documents FTP provenant de l'adresse IP 112.12.12.12 :

```
dest_ip=112.12.12.12 scheme=ftp action=deny
```

L'exemple suivant demande à Content Gateway de conserver l'en-tête d'adresse IP du client des requêtes d'URL qui contiennent l'expression régulière `politique` et dont le préfixe du chemin est **/viewpoint** :

```
url_regex=politique prefix=/viewpoint keep_hdr=ip_client
```

L'exemple suivant demande à Content Gateway de supprimer tous les cookies des requêtes de clients destinées au serveur d'origine **www.serveur1.com** :

```
dest_host=www.serveur1.com strip_hdr=cookie
```

L'exemple suivant demande à Content Gateway d'interdire les méthodes **put** pour le serveur d'origine **www.serveur2.com** :

```
dest_host=www.serveur2.com method=put action=deny
```

Content Gateway applique les règles selon leur ordre d'apparition dans la liste. L'exemple de fichier **filter.config** suivant configure par exemple Content Gateway pour qu'il effectue les opérations suivantes :

- Autoriser tous les utilisateurs (sauf ceux qui tentent d'accéder à interne.com) à accéder à serveur1.com
- Refuser l'accès à pascesite.com pour tous les utilisateurs

```
dest_host=serveur1.com action=allow
dest_host=pascesite.com action=deny
```

Fichier de configuration hosting.config

Le fichier **hosting.config** vous permet d'affecter des partitions du cache à certains serveurs d'origine et domaines pour gérer plus efficacement l'espace du cache et réduire l'utilisation des disques.

Pour obtenir des instructions détaillées sur le partitionnement du cache en fonction des domaines et des serveurs d'origine, consultez la section *Partitionnement du cache en fonction du serveur d'origine ou du domaine*, page 92.

> **Remarque**
> Avant d'affecter des partitions du cache à certains serveurs d'origine et domaines, vous devez partitionner votre cache en fonction de la taille et du protocole dans le fichier **partition.config**. Pour plus d'informations sur le partitionnement du cache, consultez la section *Partitionnement du cache*, page 91. Pour obtenir la description du fichier **partition.config**, consultez la section *Fichier de configuration partition.config*, page 376.

Après avoir modifié le fichier **hosting.config**, vous devez exécuter la commande **content_line -x** dans le répertoire **bin** de Content Gateway pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique automatiquement les modifications à tous les nœuds de ce cluster.

> **Important**
> La configuration du partitionnement doit être identique dans tous les nœuds d'un cluster.

Format

Le format de chaque ligne du fichier **hosting.config** doit être l'un des suivants :

```
hostname=nomhôte partition=numéros_partition
domain=nom_domaine partition=numéros_partition
```

où :

nomhôte correspond au nom d'hôte complet du serveur d'origine dont vous souhaitez stocker le contenu dans une partition spécifique (par exemple, www.monhote.com).

nom_domaine correspond au domaine dont vous souhaitez stocker le contenu dans une partition spécifique (par exemple, mondomaine.com).

numéros_partition correspond à la liste des partitions (séparées par des virgules) dans lesquelles vous souhaitez stocker le contenu appartenant aux serveurs d'origine ou aux domaines répertoriés. Les numéros de partition doivent être des

numéros valides répertoriés dans le fichier **partition.config** (voir *Fichier de configuration partition.config*, page 376).

> **Remarque**
> Si vous souhaitez allouer plusieurs partitions à un serveur d'origine ou à un domaine, saisissez ces partitions sur une même ligne dans une liste séparée par des virgules. Le fichier **hosting.config** ne peut pas contenir plusieurs entrées pour le même serveur d'origine ou domaine.

Partition générique

Lorsque vous configurez le fichier **hosting.config**, vous devez définir la partition générique à utiliser pour le contenu qui n'appartient à aucun des serveurs d'origine et domaines répertoriés. Lorsque toutes les partitions d'un serveur d'origine spécifique sont endommagées, Content Gateway utilise alors la partition générique pour stocker le contenu de ce serveur.

Le format de la partition générique doit être le suivant :

```
hostname=* partition=numéros_partition
```

où **numéros_partition** correspond à la liste des partitions génériques séparées par des virgules.

Exemples

L'exemple suivant configure le proxy pour qu'il stocke le contenu du domaine **mondomaine.com** dans la partition 1 et le contenu de **www.monhote.com** dans la partition 2. Le proxy stocke le contenu de tous les serveurs d'origine dans les partitions 3 et 4.

```
domain=mondomaine.com partition=1
hostname=www.monhote.com partition=2
hostname=* partition=3,4
```

Fichier de configuration ip_allow.config

Le fichier **ip_allow.config** contrôle l'accès des clients au proxy. Vous pouvez spécifier les plages d'adresses IP autorisées à utiliser Content Gateway.

> **Important**
> Après avoir modifié le fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Le format de chaque ligne du fichier **ip_allow.config** doit être le suivant :

```
src_ip=adresseIP action=ip_allow | ip_deny
```

où *adresseIP* correspond à l'adresse IP ou à la plage d'adresses IP des clients autorisés à accéder au proxy.

L'action `ip_allow` autorise les clients spécifiés à accéder au proxy.

L'action `ip_deny` refuse l'accès au proxy aux clients spécifiés.

Par défaut, le fichier **ip_allow.config** contient la ligne suivante, qui autorise tous les clients à accéder au proxy. Avant d'ajouter d'autres lignes pour limiter l'accès, supprimez cette ligne ou placez-la dans des commentaires.

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

Exemples

L'exemple suivant autorise tous les clients à accéder au proxy :

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

L'exemple suivant autorise tous les clients d'un certain sous-réseau à accéder au proxy :

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

L'exemple suivant interdit à tous les clients d'un certain sous-réseau à accéder au proxy :

```
src_ip=123.45.6.0-123.45.6.123 action=ip_deny
```

Fichier de configuration ipnat.conf

Le fichier **ipnat.conf** contient les règles de redirection qui définissent le mode de réadressage des paquets entrants lorsque le proxy dessert le trafic en transparence. Content Gateway crée ces règles de redirection pendant l'installation. Vous pouvez modifier ces règles.

Important
Après avoir modifié ce fichier, vous devez redémarrer le proxy.

Format

Le format de chaque ligne du fichier **ipnat.config** doit être le suivant :

```
rdr interface 0.0.0.0/0 port dest -> adresseIP port proxy
tcp|udp
```

où :

interface correspond à l'interface Ethernet que le trafic doit utiliser pour accéder à l'ordinateur Content Gateway (par exemple, `eth0` sous Linux).

dest correspond au port de destination du trafic (par exemple, `80` pour le trafic HTTP).

adresseIP correspond à l'adresse IP de votre serveur Content Gateway.

proxy correspond au port du proxy Content Gateway (en général `8080` pour le trafic HTTP).

Exemples

L'exemple suivant configure le module ARM pour qu'il réadresse tout le trafic HTTP entrant vers l'adresse IP de Content Gateway (111.111.11.1) sur le port du proxy Content Gateway 8080 :

```
rdr hme0 0.0.0.0/0 port 80 -> 111.111.11.1 port 8080 tcp
```

Fichier de configuration log_hosts.config

Pour enregistrer les transactions HTTP et FTP des différents serveurs d'origine dans des fichiers journaux distincts, vous devez répertorier le nom d'hôte de chaque serveur d'origine dans le fichier **log_hosts.config**. Vous devez également activer l'option de division des hôtes HTTP (voir *Division des journaux des hôtes HTTP*, page 224).

> **Remarque**
> Il est recommandé d'utiliser le même fichier **log_hosts.config** dans chaque nœud Content Gateway de votre cluster.

> **Important**
> Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Le format de chaque ligne du fichier **log_hosts.config** doit être le suivant :

```
nomhôte
```

où *nomhôte* correspond au nom d'hôte du serveur d'origine.

> **Remarque**
> Dans le fichier **log_hosts.config**, vous pouvez spécifier des mots-clés afin d'enregistrer dans un fichier journal distinct la totalité des transactions des serveurs d'origine dont le nom contient les mots-clés définis. Reportez-vous à l'exemple ci-dessous.

Exemples

L'exemple suivant demande à Content Gateway de créer des fichiers journaux distincts contenant toutes les transactions HTTP et FTP destinées aux serveurs d'origine serveurweb1, serveurweb2 et serveurweb3.

```
serveurweb1
serveurweb2
serveurweb3
```

L'exemple suivant enregistre toutes les transactions HTTP et FTP provenant des serveurs d'origine dont le nom contient sports (par exemple, `sports.yahoo.com` et www.foxsports.com) dans un fichier journal intitulé **squid-sport.log** (le format Squid est activé) :

```
sports
```

Fichier de configuration logs_xml.config

Le fichier **logs_xml.config** définit les formats, les filtres et les options de traitement des fichiers journaux personnalisés. Le format de ce fichier est de type XML (Extensible Markup Language).

Format

Le fichier **logs_xml.config** contient les spécifications suivantes :

- `LogFormat` spécifie les champs devant être collectés pour chaque accès d'événement de protocole. Voir *LogFormat*, page 365.
- `LogFilter` spécifie les filtres utilisés pour inclure ou exclure certaines entrées de la journalisation, en fonction de la valeur d'un champ de ces entrées. Voir *LogFilter*, page 366.
- `LogObject` spécifie un objet contenant un format, un nom de fichier local, des filtres et des serveurs de collecte spécifiques. Voir *LogObject*, page 367.

Remarque

Le fichier **logs_xml.config** ignore les espaces supplémentaires, les lignes vides et tous les commentaires.

LogFormat

Le tableau suivant présente la liste des spécifications `LogFormat`.

Champ	Entrées autorisées
`<Name = "nom_format_valide"/>`	Obligatoire. Les noms de format valides incluent tous les noms à l'exception des formats Squid, Common, Extended ou Extended-2 (formats prédéfinis). Cette balise n'est pas associée à une valeur par défaut.
`<Format = "spécification_format_valide"/>`	Obligatoire. Une spécification de format valide est une chaîne de style `printf` décrivant chaque entrée du journal pour les résultats au format ASCII. Servez-vous de l'espace réservé `'%<champ>'` pour les noms de champ valides. Pour plus d'informations, consultez la section *Champs de journalisation personnalisés*, page 337. Le champ spécifié peut être de deux types : Simple : par exemple, `%<cqu>` Un champ au sein d'un conteneur, par exemple un en-tête HTTP ou une statistique Content Gateway. La syntaxe de ce type de champ est la suivante : `'%<{champ}container>'`.
`<Interval = "sec_intervalle_regr"/>`	Servez-vous de cette balise lorsque le format contient des opérateurs de regroupement. La valeur `"sec_intervalle_regr"` représente le nombre de secondes devant s'écouler entre la production des différentes valeurs de regroupement individuelles. Les opérateurs de regroupement valides sont les suivants : • COUNT • SUM • AVG • FIRST • LAST

LogFilter

Le tableau suivant présente la liste des spécifications `LogFilter`.

Champ	Entrées autorisées
`<Name = "nom_filtre_valide"/>`	Obligatoire. Tous les filtres doivent avoir un nom unique.
`<Condition = "champ_journal_valide opérateur_valide valeur_comparaison_valide"/>`	Obligatoire. Ce champ contient les éléments suivants : `champ_journal_valide` : champ à comparer à la valeur donnée. Pour plus d'informations, consultez la section *Référence croisée pour le format de journalisation*, page 341. `champ_opérateur_valide` : l'un des éléments suivants : `MATCH`, `CASE_INSENSITIVE_MATCH`, `CONTAIN`, `CASE_INSENSITIVE_CONTAIN`. `MATCH` est true lorsque le champ et la valeur sont identiques (respect de la casse). `CASE_INSENSITIVE_MATCH` est similaire à `MATCH`, sans respect de la casse. `CONTAIN` est true lorsque le champ contient la valeur (la valeur est une sous-chaîne du champ). `CASE_INSENSITIVE_CONTAIN` est une version de `CONTAIN` sans respect de la casse. `valeur_comparaison_valide` : chaîne ou entier correspondant au type de champ. Pour les valeurs d'entiers, tous les opérateurs sont équivalents, c'est-à-dire que le champ doit être égal à la valeur spécifiée. Remarque : Il n'existe pas d'opérateur de comparaison négative. Pour définir une condition négative, servez-vous du champ **Action** pour refuser (REJECT) l'enregistrement.
`<Action = "champ_action_valide"/>`	Obligatoire. `ACCEPT` ou `REJECT`. Demande à Content Gateway d'accepter ou de refuser les enregistrements répondant à la condition du filtre.

LogObject

Le tableau suivant présente la liste des spécifications `LogObject`.

Champ	Entrées autorisées
`<Format = "nom_format_valide"/>`	Obligatoire. Les noms de format valides incluent les formats de journalisation prédéfinis : squid, common, extended et extended2, ainsi que les formats de journaux personnalisés précédemment définis. Cette balise n'est pas associée à une valeur par défaut.
`<Filename = "nom_fichier"/>`	Obligatoire. Nom du fichier dans lequel le journal donné est écrit dans le système de fichiers local ou dans un serveur de collecte distant. Si vous ne spécifiez pas cette balise, aucun fichier journal local n'est créé. Tous les noms de fichier sont relatifs au répertoire de journalisation par défaut. Lorsque le nom ne contient pas d'extension (par exemple, `squid`), l'extension `.log` est automatiquement ajoutée pour les journaux ASCII et l'extension `.blog` pour les journaux binaires. (Voir `<Mode = "mode_journalisation_valide" />` ci-dessous.) Lorsque vous ne voulez pas qu'une extension soit ajoutée, insérez un point (`.`) à la fin du nom de fichier : par exemple, `squid.`

Champ	Entrées autorisées
`<Mode = "mode_journalisation_valide"/>`	Les modes de journalisation valides incluent `ascii`, `binary` et `ascii_pipe`. Le mode par défaut est `ascii`. Servez-vous du mode `ascii` pour créer des fichiers journaux d'événements dans un format lisible (ASCII en clair). Servez-vous du mode `binary` pour créer des fichiers journaux d'événements au format binaire. Les fichiers journaux binaires réduisent la charge du système et occupent généralement moins d'espace disque (selon le type d'informations enregistrées). Vous devez utiliser l'application `logcat` pour convertir les fichiers journaux binaires au format ASCII avant de les lire. Servez-vous du mode `ascii_pipe` pour écrire les entrées du journal dans un canal UNIX nommé (tampon en mémoire). Les autres processus peuvent ensuite lire les données à l'aide des fonctions d'E/S standard. Content Gateway n'a pas besoin d'écrire sur le disque, ce qui libère l'espace et la bande passante pour d'autres tâches. Par ailleurs, l'écriture dans un canal ne s'interrompt pas lorsque l'espace réservé à la journalisation commence à manquer puisque ce canal n'utilise pas d'espace disque. Remarque : si vous utilisez un serveur de collecte, le journal est écrit dans un canal de ce serveur de collecte. Un canal local étant créé avant même que la première transaction ne soit traitée, vous pouvez voir le canal dès que Content Gateway démarre. Toutefois, dans un serveur de collecte, les canaux *sont* créés au démarrage de Content Gateway.
`<Filters = "liste_des_noms_de_filtre_valides"/>`	Liste des noms des filtres de journaux précédemment définis, séparés par des virgules. Lorsque plusieurs filtres sont spécifiés, ils doivent tous accepter un enregistrement pour que celui-ci soit enregistré dans le journal.

Champ	Entrées autorisées
`<Protocols = "liste_des_protocoles_valides" />`	Liste des protocoles que cet objet doit enregistrer, séparés par des virgules. Les noms de protocoles valides incluent `HTTP`.
`<ServerHosts = "liste_des_serveurs_valides"/>`	Liste des noms d'hôte valides, séparés par des virgules. Cette balise indique que seules les entrées issues des serveurs nommés seront incluses dans le fichier.
`<CollationHosts = "liste_des_nomdhôte_valides"/>`	Liste des serveurs de collecte auxquels sont transmises toutes les entrées du journal (pour cet objet), séparés par des virgules. Les serveurs de collecte peuvent être spécifiés par leur nom ou leur adresse IP. Pour spécifier le port de collecte, insérez le caractère deux points après le nom (par exemple, `hôte:port`).
`<Header = "en-tête"/>`	Le texte d'en-tête à insérer dans les fichiers journaux. Ce texte s'affiche au début du fichier journal, juste avant le premier enregistrement.
`<RollingEnabled = "valeur vraie"/>`	Active ou désactive la rotation des fichiers journaux pour la spécification *`LogObject`*. Ce paramètre remplace valeur du paramètre de configuration **Log Rolling: Enabled/Disabled (Rotation des journaux : activée/désactivée)** dans Content Gateway Manager ou le paramètre *`proxy.config.log2.rolling_enabled`* du fichier **records.config**. Définissez la « valeur vraie » sur `1` ou `true` pour activer la rotation. Définissez-la sur `0` ou `false` pour désactiver la rotation dans cette spécification *`LogObject`* spécifique.

Champ	Entrées autorisées
`<RollingIntervalSec = "secondes"/>`	Définit le nombre de secondes devant s'écouler entre les rotations des fichiers journaux pour *LogObject*. Ce paramètre remplace valeur du paramètre de configuration **Log Rolling: Interval (Rotation des journaux : Intervalle)** dans Content Gateway Manager ou le paramètre *proxy.config.log2.rolling_interval_sec* du fichier **records.config**. Cette option vous permet de définir des intervalles de rotation distincts pour les différentes spécifications *LogObject*.
`<RollingOffsetHr = "heure"/>`	Définit l'heure (de 0 à 23) sur laquelle la rotation doit obligatoirement « s'aligner ». La rotation peut démarrer avant l'heure indiquée, mais un fichier en rotation ne peut être généré qu'à cette heure-là. L'impact de ce paramètre ne se remarque que si l'intervalle de rotation dépasse une heure. Ce paramètre remplace le paramètre de configuration **Log Rolling: Offset Hour (rotation des journaux : Heure de décalage)** dans Content Gateway Manager ou le paramètre *proxy.config.log2.rolling_offset_hr* du fichier **records.config**.

Exemples

Dans l'exemple suivant, la spécification `LogFormat` collecte des informations via trois champs communs :

```
<LogFormat>
<Name = "minimal"/>
<Format = "%<chi> : %<cqu> : %<pssc>"/>
</LogFormat>
```

Dans l'exemple suivant, une spécification `LogFormat` utilise des opérateurs de regroupement :

```
<LogFormat>
<Name = "Résumé"/>
<Format = "%<LAST(cqts)> : %<COUNT(*)> : %<SUM(psql)>"/>
<Interval = "10"/>
</LogFormat>
```

Dans l'exemple suivant, la spécification `LogFilter` entraîne uniquement l'enregistrement des entrées `REFRESH_HIT` :

```
<LogFilter>
<Name = "only_refresh_hits"/>
<Action = "ACCEPT"/>
<Condition = "%<pssc> MATCH REFRESH_HIT"/>
</LogFilter>
```

Remarque

Lorsque vous spécifiez le champ de la condition du filtre, vous pouvez ignorer le caractère `%<>`. En conséquence, le filtre suivant équivaut à l'exemple précédent :

```
<LogFilter>
   <Name = "only_refresh_hits"/>
   <Action = "ACCEPT"/>
   <Condition = "pssc MATCH REFRESH_HIT"/>
</LogFilter>
```

Dans l'exemple suivant, la spécification `LogObject` crée un fichier journal local pour le format minimal défini précédemment. Le nom du fichier journal sera **minimal.log**, car il s'agit d'un fichier journal ASCII (par défaut).

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
</LogObject>
```

Dans l'exemple suivant, la spécification `LogObject` n'inclut que les requêtes HTTP desservies par les hôtes du domaine `entreprise.com` ou par le serveur spécifique `serveur.quelconque.com`. Les entrées du journal sont envoyées au port 4000 de l'hôte de collecte `logs.entreprise.com` et au port 5000 de l'hôte de collecte `209.131.52.129`.

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
<ServerHosts = "entreprise.com,serveur.quelconque.com"/>
<Protocols = "http"/>
<CollationHosts =
"logs.entreprise.com:4000,209.131.52.129:5000"/>
</LogObject>
```

Format WELF (WebTrends Enhanced Log Format)

Content Gateway reconnaissant le format WELF, vous pouvez analyser les fichiers journaux de Content Gateway à l'aide des outils de rapport WebTrends. Une spécification `<LogFormat>` compatible avec le format WELF est fournie à la fin du fichier `logs.config` (illustré ci-dessous). Pour créer un fichier journal au format WELF, créez une spécification `<LogObject>` utilisant ce format prédéfini.

```
<LogFormat>
<Name = "welf"/>
<Format = "id=firewall time=\"%<cqtd> %<cqtt>\" fw=%<phn>
pri=6 proto=%<cqus> duration=%<ttmsf> sent=%<psql>
rcvd=%<cqhl> src=%<chi> dst=%<shi> dstname=%<shn>
user=%<caun> op=%<cqhm> arg=\"%<cqup>\" result=%<pssc>
ref=\"%<{Referer}cqh>\" agent=\"%<{user-agent}cqh>\"
cache=%<crc>"/>
</LogFormat>
```

Fichier de configuration mgmt_allow.config

Le fichier **mgmt_allow.config** spécifie les adresses IP des hôtes distants autorisés ou non à accéder à Content Gateway Manager.

> **Important**
> Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Le format de chaque ligne du fichier **mgmt_allow.config** doit être le suivant :

```
src_ip=adresseIP action=ip_allow|ip_deny
```

où *adresseIP* correspond à l'adresse IP ou à la plage d'adresses IP autorisées à accéder à Content Gateway Manager.

`action` doit spécifier soit `ip_allow` pour autoriser l'accès à Content Gateway Manager, soit `ip_deny` pour refuser l'accès.

Par défaut, le fichier **mgmt_allow.config** contient la ligne suivante, qui autorise tous les hôtes distants à accéder à Content Gateway Manager. Avant d'ajouter d'autres lignes pour limiter l'accès, supprimez cette ligne ou placez-la dans des commentaires.

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

Exemples

L'exemple suivant configure Content Gateway pour qu'il n'autorise qu'un seul utilisateur à accéder à Content Gateway Manager :

```
src_ip=123.12.3.123 action=ip_allow
```

L'exemple suivant configure Content Gateway pour qu'il autorise une plage d'adresses IP à accéder à Content Gateway Manager :

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

L'exemple suivant configure Content Gateway pour qu'il refuse l'accès à Content Gateway Manager à l'adresse IP 123.45.67.8 :

```
src_ip=123.45.67.8 action=ip_deny
```

Fichier de configuration parent.config

Le fichier **parent.config** identifie les proxy HTTP parents utilisés dans une hiérarchie de caches HTTP. Servez-vous de ce fichier pour obtenir la configuration suivante :

- Configuration des hiérarchies de caches parents, avec plusieurs parents et basculement des parents
- Configuration des requêtes URL sélectionnées pour ignorer les proxy parents

Les règles sont appliquées selon leur ordre d'apparition dans la liste, de haut en bas. La première correspondance étant appliquée en premier. Les règles de contournement sont généralement placées au-dessus de la ou des règles de désignation des proxy parents.

Content Gateway utilise le fichier **parent.config** uniquement lorsque l'option de mise en cache des parents HTTP est activée. Voir *Configuration de Content Gateway pour l'utilisation d'un cache parent HTTP*, page 86.

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Chaque ligne du fichier **parent.config** doit contenir une règle de mise en cache de parent. Content Gateway reconnaît trois balises délimitées par un espace :

```
primary_destination=valeur secondary_specifier=valeur
action=valeur
```

Le tableau suivant répertorie les destinations principales possibles et leurs valeurs autorisées.

Destination principale	Valeur autorisée
dest_domain	Nom du domaine demandé
dest_host	Nom de l'hôte demandé
dest_ip	Adresse IP ou plage d'adresses IP demandées, séparées par un tiret (-)
url_regex	Expression régulière que l'on retrouve dans une URL

Dans le fichier `parent.config`, les spécificateurs secondaires sont facultatifs. Le tableau suivant répertorie les spécificateurs secondaires possibles et leurs valeurs autorisées.

Spécificateur secondaire	Valeur autorisée
time	Plage horaire, par exemple 08:00-14:00, pendant laquelle le cache parent est utilisé pour desservir les requêtes
prefix	Préfixe du chemin d'une URL
suffix	Suffixe de fichier dans l'URL
src_ip	Adresse IP du client
port	Port d'URL demandé
scheme	Protocole d'URL demandé, l'un des deux suivants : • HTTP • FTP
method	Méthode d'URL demandée, l'une des deux suivantes : • get • post • put • trace
user_agent	Valeur User-Agent de l'en-tête de la requête

Le tableau suivant répertorie les actions possibles et leurs valeurs autorisées.

Action	Valeur autorisée
parent	Liste ordonnée des serveurs parents. Lorsque la requête ne peut pas être traitée par le dernier serveur parent de cette liste, elle est acheminée vers le serveur d'origine. Vous pouvez spécifier un nom d'hôte ou une adresse IP. Vous devez spécifier le numéro du port.
round_robin	L'une des valeurs suivantes : • `true` : Content Gateway effectue une recherche circulaire basée sur l'adresse IP du client dans la liste des caches parents. • `strict` : Content Gateway dessert strictement les requêtes dans leur ordre d'arrivée. Par exemple, l'ordinateur `proxy1` dessert la première requête, `proxy2` dessert la seconde, etc. • `false` : aucune recherche circulaire n'est effectuée.
go_direct	L'une des valeurs suivantes : • `true` : les requêtes ignorent les hiérarchies parentes et sont envoyées directement au serveur d'origine. • `false` : les requêtes n'ignorent pas les hiérarchies de parents.

Exemples

La règle suivante configure une hiérarchie de caches parents constituée de Content Gateway (l'enfant) et de deux parents, `p1.x.com` et `p2.x.com`. Le proxy transmet les requêtes qu'il ne peut pas desservir aux serveurs parents `p1.x.com` et `p2.x.com` dans une recherche circulaire car `round_robin=true`.

```
dest_domain=. method=get parent="p1.x.com:8080;
p2.y.com:8080" round_robin=true
```

La règle suivante demande à Content Gateway d'acheminer directement toutes les requêtes contenant l'expression régulière `politique` et le chemin **/viewpoint** vers le serveur d'origine (en ignorant les hiérarchies parentes) :

```
url_regex=politique prefix=/viewpoint go_direct=true
```

La règle suivante est une règle de contournement de destination typique :

```
dest_domain=exemple.com go_direct=true
```

Important

Chaque ligne du fichier **parent.config** doit contenir ***soit*** une directive `parent=`, soit une directive `go_direct=`.

Une règle de contournement incluant `parent=` ***et*** `go_direct=true` entraîne l'envoi du `dest_domain` spécifié au parent, tandis que tous les autres domaines sont ignorés (soit l'opposé de l'action prévue à l'origine).

Fichier de configuration partition.config

Le fichier **partition.config** vous permet de gérer l'espace de votre cache avec plus d'efficacité en créant des partitions de tailles différentes. Vous pouvez encore configurer davantage ces partitions pour stocker des données provenant de certains serveurs d'origine et domaines dans le *Fichier de configuration hosting.config*. Vous pouvez ainsi mieux exploiter la mise en cache des sites fréquemment consultés dont le contenu ne change que rarement.

> **Important**
> La configuration du partitionnement doit être identique dans tous les nœuds d'un cluster.

Vous devez arrêter Content Gateway avant de changer la taille des partitions de cache.

Format

Pour chaque partition que vous souhaitez créer, entrer une ligne au format suivant :

```
partition=numéro_partition scheme=type_protocol
size=taille_partition
```

où :

numéro_partition est un nombre compris entre 1 et 255 (le nombre maximal de partitions est 255).

type_protocole est **http.**

> **Remarque**
> Seul le protocole HTTP est pris en charge pour l'instant. La diffusion de contenu multimédia (**combinaison**) n'est pas prise en charge.

taille_partition correspond au volume d'espace du cache alloué à la partition. Cette valeur peut être un pourcentage de l'espace total du cache ou une valeur absolue. La valeur absolue doit être un multiple de 128 Mo (128 Mo étant la valeur minimale). Si vous définissez un pourcentage, la taille est arrondie au multiple de 128 Mo inférieur le plus proche. Pour atteindre un parallélisme des E/S, chaque partition est répartie sur plusieurs disques. Par exemple, lorsqu'il y a 4 disques, une partition de 1 Go disposera de 256 Mo sur chaque disque (en supposant que chaque disque dispose de suffisamment d'espace libre).

> **Remarque**
> Si vous n'allouez pas la totalité de l'espace disque disponible dans le cache, l'espace disque supplémentaire n'est pas utilisé. Vous pouvez alors utiliser cet espace supplémentaire pour créer ensuite de nouvelles partitions, sans supprimer ni effacer les partitions existantes.

Exemples

L'exemple suivant partitionne le cache de façon égale :

```
partition=1 scheme=http size=50%
partition=2 scheme=http size=50%
```

Fichier de configuration records.config

Le fichier **records.config** contient la liste des variables configurables utilisées par Content Gateway.

La plupart des valeurs sont définies à l'aide des commandes de Content Gateway Manager. Certaines options ne peuvent être définies qu'en modifiant les variables dans le fichier **records.config**.

Avertissement

Ne modifiez pas les variables du fichier **records.config**, à moins d'être certain de leur impact. Beaucoup de variables sont couplées, c'est-à-dire qu'elles interagissent avec d'autres variables. La modification isolée d'une variable seule peut donc nuire au fonctionnement de Content Gateway. **Dans la mesure du possible, utilisez Content Gateway Manager pour configurer Content Gateway.**

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications.

Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Le format de chaque variable est le suivant :

```
CONFIG nom_variable DATATYPE valeur_variable
```

où *DATATYPE* est `INT` (un entier), `STRING` (une chaîne) ou `FLOAT` (une virgule flottante).

Exemples

Dans l'exemple suivant, le type de données de la variable **proxy.config.proxy_name** est **string** et sa valeur est **contenuserveur1**. Cela signifie que le nom du proxy Content Gateway est **contenuserveur1**.

```
CONFIG proxy.config.proxy_name STRING contenuserveur1
```

Dans l'exemple suivant, la variable **proxy.config.winauth.enabled** est un indicateur oui/non. La valeur 0 (zéro) désactive l'option. La valeur 1 active l'option.

```
CONFIG proxy.config.winauth.enabled INT 0
```

Dans l'exemple suivant, la variable définit le délai d'expiration du démarrage du cluster sur 10 secondes.

```
CONFIG proxy.config.cluster.startup_timeout INT 10
```

Variables de configuration

Les tableaux suivants décrivent les variables de configuration répertoriées dans le fichier **records.config**.

Durée de vie des documents FTP mis en cache

Mode de transfert FTP

Moteur FTP

Pages de réponse personnalisables

Processeur SOCKS

Sous-système réseau

Sous-système de cluster

Cache

DNS

Proxy DNS

Base de données des hôtes (HostDB)

Configuration de la journalisation

Règles de remappage des URL

Configuration des mises à jour planifiées

Configuration WCCP

Décryptage SSL

ICAP

Connectivité, analyse et conditions de limites

Variables système

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.proxy_name`	`CHAÎNE`		Indique le nom du nœud Content Gateway
`proxy.config.bin_path`	`CHAÎNE`	`bin`	Définit l'emplacement du répertoire **bin** de Content Gateway C'est dans ce répertoire que le programme d'installation stocke les fichiers binaires de Content Gateway.
`proxy.config.proxy_ binary`	`CHAÎNE`	`content_gateway`	Définit le nom du fichier exécutable qui exécute le processus **content_gateway**

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.proxy_ binary_opts	CHAÎNE	-M	Définit les options de ligne de commande qui permettent de démarrer **content_gateway**
proxy.config.manager_ binary	CHAÎNE	content_manager	Définit le nom du fichier exécutable qui exécute le processus **content_manager**
proxy.config.cli_binary	CHAÎNE	content_line	Définit le nom du fichier exécutable qui exécute le processus **content_line**
proxy.config.watch_ script	CHAÎNE	content_cop	Définit le nom du fichier exécutable qui exécute le processus **content_cop**
proxy.config.env_prep	CHAÎNE	example_prep.sh	Spécifie le script exécuté avant que le processus **content_manager** ne lance le processus **content_gateway**
proxy.config.config_dir	CHAÎNE	config	Spécifie le répertoire, par rapport au chemin bin_path (ci-dessus), qui contient les fichiers de configuration de Content Gateway
proxy.config.temp_dir	CHAÎNE	/tmp	Spécifie le répertoire utilisé pour les fichiers temporaires de Content Gateway
proxy.config.alarm_email	CHAÎNE	websense	Spécifie l'adresse électronique à laquelle Content Gateway envoie les messages d'alarme Vous pouvez spécifier cette adresse électronique pendant l'installation. Si vous l'omettez, Content Gateway utilise le nom du compte Content Gateway comme valeur par défaut.
proxy.config.syslog_ facility	CHAÎNE	LOG_DAEMON	Spécifie le mécanisme utilisé pour enregistrer les fichiers journaux système Voir *Utilisation des fichiers journaux*, page 211.
proxy.config.cop.core_ signal	ENTIER	3	Spécifie le signal envoyé par **content_cop** à ses processus gérés (**content_manager** et **content_gateway**) pour les arrêter **Remarque : ne modifiez pas la valeur de cette variable.**

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.cop.sleep_time	ENTIER	45	Spécifie l'intervalle, en secondes, devant s'écouler entre les tests de pulsation exécutés par **content_cop** pour vérifier le fonctionnement des processus **content_manager** et **content_gateway** **Remarque : ne modifiez pas la valeur de cette variable.**
proxy.config.cop.linux_min_swapfree_kb	ENTIER	10240	Cette variable n'est pas utilisée.
proxy.config.cop.linux_min_memfree_kb	ENTIER	10240	Cette variable n'est pas utilisée.
proxy.config.output.logfile	CHAÎNE	content_gateway.out	Spécifie le nom et l'emplacement du fichier qui contient les avertissements, les messages d'état et les messages d'erreur générés par les processus Content Gateway. Lorsque le chemin n'est pas spécifié, Content Gateway crée le fichier dans son répertoire de journalisation.
proxy.config.snapshot_dir	CHAÎNE	snapshots	Spécifie le répertoire du système local dans lequel Content Gateway stocke les instantanés de votre configuration. À moins que vous ne spécifiez un chemin absolu, ce répertoire est situé dans le répertoire **config** de Content Gateway.
proxy.config.attach_debugger_script	CHAÎNE	attach_debugger	Cette variable ne doit être utilisée que sur instruction du Support technique de Websense. Lorsqu'elle est définie, un script de débogage (situé dans /opt/WCG/bin) est exécuté lors de la réinitialisation du processus **content_gateway**.
proxy.config.diags.debug.clients_ips	CHAÎNE	NULL	

Gestionnaire local

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.lm.sem_id	ENTIER	11452	Spécifie l'ID du sémaphore du gestionnaire local **Remarque : ne modifiez pas la valeur de cette variable.**
proxy.local.cluster.type	ENTIER	3	Définit le mode de clustering : • 2 = mode gestion uniquement • 3 = aucun clustering
proxy.config.cluster. rsport	ENTIER	8087	Spécifie le port de service fiable. Ce port sert à échanger les informations de configuration entre les nœuds d'un cluster. Tous les nœuds de ce cluster doivent utiliser le même port de service fiable.
proxy.config.cluster. mcport	ENTIER	8088	Spécifie le port de multidiffusion. Ce port est utilisé pour l'identification des nœuds. Tous les nœuds du cluster doivent utiliser le même port de multidiffusion.
proxy.config.cluster. mc_group_addr	CHAÎNE	224.0.1.37	Spécifie l'adresse de multidiffusion pour les communications du cluster. Tous les nœuds du cluster doivent utiliser la même adresse de multidiffusion.
proxy.config.cluster. mc_ttl	ENTIER	1	Spécifie la durée de vie de multidiffusion des communications du cluster
proxy.config.cluster. log_bogus_mc_msgs	ENTIER	1	Active (1) ou désactive (0) la journalisation des messages de multidiffusion non valides
proxy.config.admin. html_doc_root	CHAÎNE	ui	Spécifie la racine du document pour Content Gateway Manager
proxy.config.admin. web_interface_port	ENTIER	8081	Spécifie le port de Content Gateway Manager
proxy.config.admin. autoconf_port	ENTIER	8083	Spécifie le port d'auto-configuration
proxy.config.admin. overseer_port	ENTIER	-1	Spécifie le port utilisé pour récupérer et définir les statistiques et les variables de configuration. Ce port est désactivé par défaut.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.admin.admin_user	CHAÎNE	admin	Spécifie l'ID de l'administrateur contrôlant l'accès à Content Gateway Manager
proxy.config.admin.admin_password	CHAÎNE		Spécifie le mot de passe crypté de l'administrateur contrôlant l'accès à Content Gateway Manager. Vous ne pouvez pas modifier ce mot de passe, mais vous pouvez spécifier la valeur NULL pour l'effacer. Voir *Comment accéder à Content Gateway Manager si j'ai oublié le mot de passe de l'administrateur principal ?*, page 466.
proxy.config.admin.basic_auth	ENTIER	1	Active (1) ou désactive (0) l'authentification de base des utilisateurs afin de contrôler l'accès à Content Gateway Manager Remarque : lorsque l'authentification de base n'est *pas* activée, tous les utilisateurs peuvent accéder à Content Gateway Manager pour surveiller et configurer Content Gateway.
proxy.config.admin.use_ssl	ENTIER	1	Active l'option SSL de Content Gateway Manager afin de sécuriser les communications entre un hôte distant et Content Gateway Manager
proxy.config.admin.ssl_cert_file	CHAÎNE	server.pem	Spécifie le nom de fichier du certificat SSL installé dans le système Content Gateway pour sécuriser les communications entre un hôte distant et Content Gateway Manager
proxy.config.admin.number_config_bak	ENTIER	3	Spécifie le nombre maximal de copies à conserver pour les fichiers de configuration ayant subi une rotation
proxy.config.admin.user_id	CHAÎNE	root	Spécifie le compte d'utilisateur sans privilège désigné pour Content Gateway

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.admin. ui_refresh_rate	ENTIER	30	Spécifie la fréquence d'actualisation de l'affichage des statistiques dans les pages Monitor (Surveiller) de Content Gateway Manager
proxy.config.admin. log_mgmt_access	ENTIER	0	Active (1) ou désactive (0) la journalisation de toutes les transactions de Content Gateway Manager dans le fichier **lm.log**
proxy.config.admin. log_resolve_hostname	ENTIER	1	Lorsque cette option est activée (1), le nom d'hôte du client qui se connecte à Content Gateway Manager est enregistré dans le fichier **lm.log**. Lorsque cette option est désactivée (0), l'adresse IP du client qui se connecte à Content Gateway Manager est enregistrée dans le fichier **lm.log**.
proxy.config.admin. subscription	CHAÎNE	NULL	Non utilisée
proxy.config.admin. supported_cipher_list	CHAÎNE	AES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA	Liste des algorythmes de cryptage autorisés (sans espace et séparés par des virgules) lorsqu'un navigateur établit une connexion sécurisée avec Content Gateway Manager Cette chaîne n'est pas validée. La première valeur correcte est utilisée. En l'absence d'une valeur correcte, le navigateur n'est pas autorisé à se connecter à Content Gateway Manager et une erreur est renvoyée.
proxy.config.lm. display_reset_alarm	ENTIER	0	Lorsque cette option est activée (1), un courrier électronique est envoyé à l'administrateur (**proxy.config.alarm_email**) à chaque réinitialisation de Content Gateway. La valeur par défaut est 0.

Gestionnaire des processus

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.process_ manager.mgmt_port	ENTIER	8084	Spécifie le port utilisé pour les communications internes entre les processus **content_manager** et **content_gateway**

Gestionnaire d'adresses IP virtuelles

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.vmap. enabled	ENTIER	0	Active (1) ou désactive (0) l'option IP virtuel

Configuration des alarmes

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.alarm.bin	CHAÎNE	example_alarm_ bin.sh	Spécifie le nom du script exécutant certaines actions lorsqu'une alarme est signalée. Le fichier par défaut est un exemple de script intitulé **example_alarm_bin.sh** situé dans le répertoire **bin**. Vous devez modifier ce script en fonction de vos besoins.
proxy.config.alarm.abs_ path	CHAÎNE	NULL	Spécifie le chemin complet du fichier script spécifié par **proxy.config.alarm.bin** (entrée précédente)

ARM

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.arm.ignore_ifp`	ENTIER	1	Lorsque des règles NAT sont appliquées, indique à Content Gateway d'utiliser n'importe quelle interface disponible pour renvoyer les paquets au client, plutôt que celle qui a déclenché la règle NAT.
`proxy.config.arm.always_query_dest`	ENTIER	0	Lorsque cette option est activée (1), Content Gateway demande systématiquement au module ARM l'adresse IP de destination d'origine des requêtes entrantes. Cette opération remplace la recherche DNS effectuée sur le nom d'hôte de la requête. Lorsque cette option est activée, les adresses IP sont enregistrées à la place des noms de domaine. Lorsqu'elle est désactivée, les noms de domaine sont enregistrés dans le journal. Pour plus d'informations, consultez la section *Réduction des recherches DNS*, page 71. Il est préférable de ne pas activer cette variable lorsque Content Gateway s'exécute *à la fois* en mode proxy explicite et en mode proxy transparent. En mode proxy explicite, le client n'effectue pas de recherche DNS sur le nom d'hôte du serveur d'origine. Cette opération doit donc être effectuée par Content Gateway.
`proxy.config.http.outgoing_ip_spoofing_enabled`	ENTIER	0	Active (1) ou désactive (0) l'option d'usurpation d'adresse IP, qui permet à Content Gateway d'établir des connexions au serveur d'origine avec l'adresse IP du client et non pas avec l'adresse IP de Content Gateway Voir *Usurpation d'adresse IP*, page 72.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.arm.bypass_dynamic_enabled	ENTIER	0	Active (1) ou désactive (0) l'option de contournement adaptatif de manière à ignorer le proxy et à accéder directement au serveur d'origine en cas de problème avec des clients ou des serveurs. Voir *Règles de contournement dynamique*, page 68.
proxy.config.arm.bypass_use_and_rules_bad_client_request	ENTIER	0	Active (1) ou désactive (0) le contournement dynamique source/destination en cas de trafic non HTTP sur le port 80. Remarque : la variable **proxy.config.arm.bypass_on_bad_client_request** doit également être activée pour que cette option fonctionne.
proxy.config.arm.bypass_use_and_rules_400	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 400. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_400** doit également être activée.
proxy.config.arm.bypass_use_and_rules_401	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 401. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_401** doit également être activée.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.arm.bypass_use_and_rules_403	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 403. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_403** doit également être activée.
proxy.config.arm.bypass_use_and_rules_405	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 405. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_405** doit également être activée.
proxy.config.arm.bypass_use_and_rules_406	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 406. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_406** doit également être activée.
proxy.config.arm.bypass_use_and_rules_408	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 408. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_408** doit également être activée.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.arm.bypass_use_and_rules_500	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement source/destination lorsqu'un serveur d'origine renvoie une erreur 500. Remarque : pour que cette option fonctionne, la variable **proxy.config.arm.bypass_on_500** doit également être activée.
proxy.config.arm.bypass_on_bad_client_request	ENTIER	0	Active (1) ou désactive (0) le contournement dynamique de la destination en cas de trafic non HTTP sur le port 80
proxy.config.arm.bypass_on_400	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 400
proxy.config.arm.bypass_on_401	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 401
proxy.config.arm.bypass_on_403	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 403
proxy.config.arm.bypass_on_405	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 405
proxy.config.arm.bypass_on_406	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 406
proxy.config.arm.bypass_on_408	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 408
proxy.config.arm.bypass_on_500	ENTIER	0	Active (1) ou désactive (0) la génération dynamique de règles de contournement de la destination lorsqu'un serveur d'origine renvoie une erreur 500

Configuration du délestage de la charge (ARM)

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.arm.loadshedding.max_connections	ENTIER	1000000	Spécifie le nombre maximal de connexions de clients autorisées avant que le proxy ne commence à transmettre directement les requêtes entrantes au serveur d'origine
proxy.config.http.client.connection_control.enabled	ENTIER	1	Désactive (0) ou active (1) la possibilité de limiter le nombre de connexions issues d'un même ordinateur
proxy.config.http.client.concurrent_connection_control.close.enabled	ENTIER	1	Désactive (0) ou active (1) la fermeture des connections lorsque la limite de connexions simultanées définie est atteinte
proxy.config.http.client.concurrent_connection_control.alert.enabled	ENTIER	0	Désactive (0) ou active (1) l'alerte de violation de la limite de connexions simultanées
proxy.config.http.client.concurrent_connection_control.max_connections	ENTIER	1000	Configure le nombre maximal de connexions simultanées autorisées à partir d'une même adresse IP de client
proxy.config.http.client.connection_rate_control.close.enabled	ENTIER	0	Désactive (0) ou active (1) la fermeture des connections lorsque la limite de taux de connexions définie est atteinte
proxy.config.http.client.connection_rate_control.alert.enabled	ENTIER	1	Désactive (0) ou active (1) les alertes de dépassement de la limite de taux de connexions
proxy.config.http.client.connection_rate_control.second	ENTIER	100	Configure le nombre maximal de connexions autorisées par seconde à partir d'une même adresse IP de client
proxy.config.http.client.connection_control.exceptions	CHAÎNE	NULL	Spécifie la liste des adresses IP (séparées par des virgules) auxquelles les limites du nombre de connexions ne s'appliquent pas

Domaine Kerberos d'authentification de base

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.proxy.authenticate.basic.realm	CHAÎNE	NULL	Spécifie le nom du domaine Kerberos d'authentification. Si la valeur **NULL** par défaut est définie, **Content Gateway** est utilisé.
proxy.config.auth_type	ENTIER	0	Spécifie le type d'authentification des clients • 0 = Aucune • 1 = LDAP • 2 = RADIUS • 3 = NTLM héritée • 4 = Authentification Windows intégrée • 5 = Authentification dans plusieurs domaines Kerberos
proxy.config.multiauth.enabled	ENTIER	0	Active (1) ou désactive (0) l'authentification dans plusieurs domaines Kerberos. Indique à Content Gateway d'utiliser le fichier auth.config pour les méthodes d'authentification dans plusieurs domaines Kerberos.

LDAP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ldap.auth.enabled	ENTIER	0	Active (1) ou désactive (0) l'authentification de proxy LDAP. Voir *Authentification LDAP*, page 188.
proxy.config.ldap.cache.size	ENTIER	5000	Spécifie le nombre maximal d'entrées autorisées dans le cache LDAP Lorsque cette valeur est modifiée, la valeur de **proxy.config.ldap.cache.storage_size** doit également être modifiée en proportion. Par exemple, si vous doublez la taille du cache, doublez également celle du stockage du cache.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ldap.cache.storage_size	ENTIER	24582912	Spécifie la taille du cache LDAP, en octets. Cette option est directement liée au nombre d'entrées du cache. Lorsque cette valeur est modifiée, la valeur de **proxy.config.ldap.cache.size** doit également être modifiée en proportion. Par exemple, si vous doublez la taille du stockage, doublez également la taille du cache. Si vous modifiez cette variable sans modifier la valeur de **proxy.config.ldap.cache.size** , le sous-système LDAP cesse de fonctionner.
proxy.config.ldap.auth.ttl_value	ENTIER	3000	Spécifie le délai (en minutes) pendant lequel les entrées du cache demeurent valides
proxy.config.ldap.auth.purge_cache_on_auth_fail	ENTIER	1	Lorsque cette option est activée (1), configure Content Gateway pour qu'il supprime l'entrée de l'autorisation du client dans le cache LDAP en cas d'échec de l'authentification.
proxy.config.ldap.proc.ldap.server.name	CHAÎNE	NULL	Spécifie le nom du serveur LDAP
proxy.config.ldap.proc.ldap.server.port	ENTIER	389	Spécifie le port du serveur LDAP
proxy.config.ldap.proc.ldap.base.dn	CHAÎNE	NULL	Spécifie le Nom unique de la base de recherche LDAP (DN). Demandez cette valeur à votre administrateur LDAP.
proxy.config.ldap.proc.ldap.uid_filter	CHAÎNE	**sAMAccountName**	Spécifie le nom/ID de connexion LDAP. Utilisez cette option comme un filtre pour rechercher le non unique complet dans la base de données. Pour eDirectory ou les autres services d'annuaire, saisissez **uid** dans ce champ.
proxy.config.ldap.secure.bind.enabled	ENTIER	0	Lorsque cette option est activée (1), configure le proxy pour qu'il utilise une communication LDAP sécurisée (LDAPS) pour communiquer avec le serveur LDAP. La communication sécurisée est généralement établie sur le port 636 ou 3269.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ldap.proc.ldap.server.bind_dn	CHAÎNE	NULL	Spécifie le Nom distinctif complet (FDN) d'un utilisateur dans le service d'annuaire de type LDAP. Par exemple : CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM Entrez un maximum de 128 caractères dans ce champ. Lorsqu'aucune valeur n'est saisie dans ce champ, le proxy tente une liaison anonyme.
proxy.config.ldap.proc.ldap.server.bind_pwd	CHAÎNE	NULL	Spécifie le mot de passe de l'utilisateur identifié par la variable **proxy.config.ldap.proc.ldap.server.bind_dn**

Authentification RADIUS

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.radius.auth.enabled	ENTIER	0	Active (1) ou désactive (0) l'authentification RADIUS du proxy
proxy.config.radius.proc.radius.primary_server.name	CHAÎNE	NULL	Spécifie le nom d'hôte ou l'adresse IP du serveur d'authentification RADIUS principal
proxy.config.radius.proc.radius.primary_server.auth_port	ENTIER	1812	Spécifie le port utilisé par Content Gateway pour communiquer avec le serveur RADIUS
proxy.config.radius.proc.radius.primary_server.shared_key	CHAÎNE	NULL	Spécifie la clé d'encodage utilisée avec le premier serveur d'authentification RADIUS
proxy.config.radius.proc.radius.secondary_server.name	CHAÎNE	NULL	Spécifie le nom d'hôte ou l'adresse IP du serveur d'authentification RADIUS secondaire
proxy.config.radius.proc.radius.secondary_server.auth_port	ENTIER	1812	Spécifie le port utilisé par le proxy pour communiquer avec le serveur d'authentification RADIUS secondaire

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.radius.proc.radius.secondary_server.shared_key	CHAÎNE	NULL	Spécifie la clé d'encodage utilisée avec le serveur d'authentification RADIUS secondaire
proxy.config.radius.auth.min_timeout	ENTIER	10	Spécifie le délai pendant lequel la connexion au serveur RADIUS peut rester inactive avant que Content Gateway ne la ferme
proxy.config.radius.auth.max_retries	ENTIER	10	Spécifie le nombre maximal de tentatives de connexion au serveur RADIUS effectuées par Content Gateway
proxy.config.radius.cache.size	ENTIER	1000	Spécifie le nombre d'entrées autorisées dans le cache RADIUS La valeur minimale est 256 entrées.
proxy.config.radius.cache.storage_size	ENTIER	15728640	Spécifie le volume maximal d'espace que peut occuper le cache RADIUS sur le disque Cette valeur doit être d'au moins cent fois le nombre d'entrées. Il est recommandé d'utiliser la quantité d'espace disque maximale possible.
proxy.config.radius.auth.ttl_value	ENTIER	60	Spécifie la durée (en minutes) pendant laquelle Content Gateway stocke les entrées de nom d'utilisateur et de mot de passe dans le cache RADIUS

NTLM

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ntlm.auth.enabled	ENTIER	0	Active (1) ou désactive (0) l'authentification NTLM du proxy

proxy.config.ntlm.dc.list	CHAÎNE	NULL	Définit les noms d'hôte des contrôleurs de domaine. Séparez chaque entrée de la liste par une virgule. Le format est le suivant :
			`nom_hôte[:port] [%nom_netbios]`
			ou
			`adresse_IP[:port] [%nom_netbios]`
			Si vous utilisez Active Directory 2008, vous devez inclure le **nom_netbios** ou utiliser le port SMB 445.

proxy.config.ntlm.dc.load_balance	ENTIER	0	Active (1) ou désactive (0) l'équilibrage de la charge. Lorsque cette option est activée, Content Gateway équilibre la charge lorsqu'il envoie des requêtes d'authentification aux contrôleurs de domaine. **Remarque :** lorsque plusieurs contrôleurs de domaine sont spécifiés, si la charge du contrôleur de domaine principal atteint le nombre maximal de connexions autorisées, les nouvelles requêtes sont envoyées à un contrôleur de domaine secondaire en tant que provision de basculement à court terme, jusqu'à ce que le contrôleur de domaine principal puisse accepter de nouvelles connexions, et ce y compris lorsque l'équilibrage de la charge est désactivé.
proxy.config.ntlm.dc.max_connections	ENTIER	10	Spécifie le nombre maximal de connexions que Content Gateway peut ouvrir sur le contrôleur de domaine

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ntlm.cache.enabled	ENTIER	1	Active (1) ou désactive (0) le cache NTLM. Cette option s'applique uniquement lorsque Content Gateway est un proxy explicite. Lorsque cette option est désactivée, Content Gateway ne stocke pas les informations d'identification dans le cache NTLM en vue de leur utilisation ultérieure. Content Gateway envoie systématiquement les informations d'identification au serveur de domaine en vue de leur validation.
proxy.config.ntlm.cache.ttl_value	ENTIER	900	Spécifie le nombre de secondes pendant lesquelles Content Gateway stocke des entrées dans le cache NTLM. La plage des valeurs prises en charge va de 300 à 86 400 secondes.
proxy.config.ntlm.cache.size	ENTIER	5000	Spécifie le nombre d'entrées autorisées dans le cache NTLM
proxy.config.ntlm.cache.storage_size	ENTIER	15728640	Spécifie le volume maximal d'espace que peut occuper le cache NTLM sur le disque. Cette valeur doit être proportionnelle au nombre d'entrées du cache NTLM. Par exemple, lorsque chaque entrée du cache NTLM fait environ 128 octets et que 5 000 entrées sont autorisées dans le cache NTLM, la taille de stockage du cache doit être d'au moins 64 000 octets.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ntlm.cache_exception.list	CHAÎNE	NULL	Gère la liste des adresses IP et des plages d'adresses IP qui ne seront pas mises en cache. La valeur de cette variable provient du champ NTLM Multi-Host IP addresses (Adresses IP multi-hôtes NTLM) de Content Gateway Manager.
proxy.config.ntlm.fail_open	ENTIER	1	Active (1) ou désactive (0) l'option autorisant le traitement des requêtes des clients lorsque l'authentification échoue dans les cas suivants : • Aucune réponse du contrôleur de domaine • Messages malformés provenant du client • Réponses SMB non valides **Remarque :** les échecs d'authentification du mot de passe sont toujours des échecs.

Authentification Windows intégrée

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.winauth.enabled	ENTIER	0	Active (1) ou désactive (0) l'Authentification Windows intégrée (Kerberos)
proxy.config.winauth.realm	CHAÎNE	NULL	Spécifie le nom du domaine Windows Active Directory. La saisie de « * », permet d'utiliser tous les contrôleurs de domaine détectés dans les enregistrements DNS SRV.
proxy.config.winauth.log_denied_requests	ENTIER	1	Active (1) ou désactive (0) la journalisation des requêtes d'authentification refusées

Authentification transparente

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.http.transparent_auth_hostname`	CHAÎNE	NULL	Spécifie un autre nom d'hôte du proxy pouvant être résolu via DNS pour tous les clients. Cette option est nécessaire lorsque le nom d'hôte ordinaire de l'ordinateur Content Gateway ne peut pas être résolu via DNS pour tous les utilisateurs. Pour plus d'informations, consultez la section *Paramètres de l'authentification transparente du proxy*, page 178.
`proxy.config.http.transparent_auth_type`	ENTIER	1	Spécifiez : • 0 pour associer un ID de session au nom d'utilisateur après l'authentification. Ce paramètre est obligatoire pour que les utilisateurs qui partagent une même adresse IP soient identifiés de façon unique, par exemple en cas de chaîne de proxy ou de traduction d'adresses réseau (NAT). • 1 pour associer une adresse IP de client à un nom d'utilisateur après l'authentification de la session de l'utilisateur Dans les deux modes, le délai devant s'écouler avant que le client ne soit à nouveau authentifié dépend de la valeur de l'option **proxy.config.http.transparent_auth_session_time**.
`proxy.config.http.transparent_auth_session_time`	ENTIER	15	Spécifie le délai devant s'écouler (en minutes) avant que le navigateur ne doive recommencer l'authentification. Cette valeur est utilisée dans les modes IP et cookie.

Moteur HTTP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. server_port	ENTIER	8080	Spécifie le port utilisé par Content Gateway lorsqu'il joue le rôle de serveur proxy Web pour le trafic Web ou lorsqu'il dessert le trafic Web en transparence
proxy.config.http. server_port_attr	CHAÎNE	X	Spécifie les options de port du serveur. Vous pouvez spécifier l'un des éléments suivants : • C=SERVER_PORT_COMPRESSED • X=SERVER_PORT_DEFAULT • T=SERVER_PORT_BLIND_ TUNNEL
proxy.config.http. server_other_ports	CHAÎNE	NULL	Spécifie les ports autres que celui défini par la variable **proxy.config.http.server_port** à relier aux requêtes HTTP entrantes
proxy.config.http. ssl_ports	CHAÎNE	443 563 8081 8071 9443 9444	Spécifie les ports utilisés pour la mise en tunnel. Il s'agit d'une liste séparée par des espaces qui inclut également des plages de ports (ex. : 1-65535) Content Gateway autorise uniquement les tunnels sur les ports spécifiés.
proxy.config.http. insert_request_via_str	ENTIER	1	Spécifiez l'un des éléments suivants : • 0 = aucune information supplémentaire n'est ajoutée à la chaîne. • 1 = toutes les informations supplémentaires sont ajoutées. • 2 = certaines informations supplémentaires sont ajoutées.
proxy.config.http. insert_response_via_str	ENTIER	1	Spécifiez l'un des éléments suivants : • 0 = aucune information supplémentaire n'est ajoutée à la chaîne. • 1 = toutes les informations supplémentaires sont ajoutées. • 2 = certaines informations supplémentaires sont ajoutées.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. enable_url_expandomatic	ENTIER	1	Active (1) ou désactive (0) l'extension de domaine **.com**, qui configure Content Gateway de sorte qu'il tente de résoudre les noms d'hôte non qualifiés en les redirigeant vers l'adresse étendue en insérant **www.** devant l'adresse et **.com** après. Par exemple, lorsqu'un client demande **hote**, Content Gateway redirige la requête vers www.hote.com.
proxy.config.http. no_dns_just_forward_ to_parent	ENTIER	0	Lorsque cette option est activée (1), de même que la mise en cache des parents HTTP, Content Gateway n'effectue pas de recherches DNS sur les noms d'hôte demandés.
proxy.config.http. uncacheable_requests_ bypass_parent	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ignore le proxy parent d'une requête qui ne peut pas être mise en cache.
proxy.config.http. keep_alive_enabled	ENTIER	1	Active (1) ou désactive (0) le maintien des connexions aux serveurs d'origine ou aux clients
proxy.config.http. chunking_enabled	ENTIER	1	Indique si Content Gateway doit générer une réponse fragmentée : • 0 = Jamais • 1 = Toujours

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. send_http11_requests	ENTIER	3	Configure Content Gateway pour qu'il utilise HTTP Version 1.1 pour communiquer avec les serveurs d'origine. Vous pouvez spécifier l'une des valeurs suivantes : • 0 = ne jamais utiliser HTTP 1.1 pour communiquer avec les serveurs d'origine • 1 = Toujours utiliser HTTP 1.1 pour communiquer avec les serveurs d'origine • 2 = Utiliser HTTP 1.1 lorsque le serveur d'origine a déjà utilisé HTTP 1.1 • 3 = Utiliser HTTP 1.1 lorsque la demande du client est HTTP 1.1 et que le serveur d'origine a déjà utilisé HTTP 1.1 Remarque : lorsque HTTP 1.1 est utilisé, Content Gateway peut maintenir les connexions actives en effectuant une mise en tunnel vers les serveurs d'origine. Lorsque HTTP 0.9 est utilisé, Content Gateway ne peut pas maintenir les connexions aux serveurs d'origine. Lorsque HTTP 1.0 est utilisé, Content Gateway peut maintenir les connexions actives sans effectuer de mise en tunnel vers les serveurs d'origine.
proxy.config.http.send_ http11_asfirstrequest	ENTIER	1	Activée (1), cette option indique à Content Gateway d'envoyer HTTP 1.1 dans la première requête au serveur. Autrement, le comportement par défaut est défini par l'option **proxy.config.http. send_http11_requests**.
proxy.config.http. share_server_sessions	ENTIER	1	Active (1) ou désactive (0) la réutilisation des sessions de serveurs. Remarque : lorsque l'usurpation d'adresse IP est activée, Content Gateway désactive automatiquement cette variable.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. ftp_enabled	ENTIER	1	Active (1) ou désactive (0) l'option permettant à Content Gateway de desservir les requêtes FTP envoyées via HTTP
proxy.config.http. record_heartbeat	ENTIER	0	Active (1) ou désactive (0) la journalisation des pulsations du processus **content_cop**
proxy.config.http. large_file_support	ENTIER	1	Lorsque cette option est activée (1), Content Gateway prend en charge le téléchargement des fichiers dont la taille dépasse 2 Go.

Configuration des proxy parents

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. parent_proxy_ routing_enable	ENTIER	0	Active (1) ou désactive (0) l'option de mise en cache des parents HTTP Voir *Mise en cache hiérarchique*, page 85.
proxy.config.http. parent_proxy.retry_time	ENTIER	300	Spécifie le délai autorisé entre les tentatives de connexions à un cache parent non disponible
proxy.config.http. parent_proxy. fail_threshold	ENTIER	10	Spécifie le nombre d'échecs de connexion au cache parent pouvant se produire avant que Content Gateway ne considère que ce parent est indisponible
proxy.config.http. parent_proxy. total_connect_attempts	ENTIER	4	Spécifie le nombre total de tentatives de connexion à un cache parent autorisées avant que Content Gateway ignore le parent ou indique un échec de la requête (selon l'option **go_direct** définie dans le fichier **bypass.config**)
proxy.config.http. parent_proxy. per_parent_ connect_attempts	ENTIER	2	Spécifie le nombre total de tentatives de connexion autorisées par parent lorsque plusieurs parents sont utilisés
proxy.config.http. parent_proxy. connect_attempts_timeout	ENTIER	30	Spécifie la valeur du délai d'expiration, en secondes, des tentatives de connexion au cache parent

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. forward. proxy_auth_to_parent	ENTIER	0	Lorsque cette option est activée (1), l'en-tête Proxy-Authorization (Autorisation du proxy) n'est *pas* extrait des requêtes envoyées à un proxy parent. Activez cette option lorsque Content Gateway est un proxy enfant et que l'authentification est effectuée par le proxy parent.
proxy.config.http. child_proxy. read_auth_from_header	ENTIER	0	Lorsque Content Gateway est le proxy parent, lit les champs X-Authenticated-User et X-Forwarded-For des en-têtes des requêtes entrantes. 1 = activé 0 = désactivé
proxy.local.http. parent_proxy. disable_ssl_ connect_tunneling	ENTIER	0	Lorsque cette option est activée (1), les requêtes HTTPS ignorent le proxy parent.
proxy.local.http. parent_proxy. disable_ unknown_connect_ tunneling	ENTIER	0	Lorsque cette option est activée (1), les requêtes de tunnel non HTTPS ignorent le proxy parent.

Délais d'expiration des connexions HTTP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. keep_alive_no_activity_ timeout_in	ENTIER	60	Spécifie la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux clients en vue de la requête suivante après la fin d'une transaction.
proxy.config.http. keep_alive_no_activity_ timeout_out	ENTIER	60	Spécifie la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux serveurs d'origine en vue du prochain transfert de données après la fin d'une transaction

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.transaction_no_activity_timeout_in	ENTIER	120	Spécifie la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux clients lorsqu'une transaction est périmée
proxy.config.http.transaction_no_activity_timeout_out	ENTIER	120	Spécifie la durée pendant laquelle Content Gateway doit maintenir ouvertes les connexions aux serveurs d'origine lorsqu'une transaction est périmée
proxy.config.http.transaction_active_timeout_in	ENTIER	0	Spécifie la durée pendant laquelle Content Gateway doit rester connecté à un client. Si le transfert vers le client n'est pas terminé avant l'expiration de ce délai, Content Gateway ferme la connexion. La valeur 0 par défaut indique qu'il n'y a pas de délai d'expiration.
proxy.config.http.transaction_active_timeout_out	ENTIER	0	Spécifie la durée pendant laquelle Content Gateway doit attendre que la demande de connexion à un serveur d'origine soit satisfaite. Lorsque Content Gateway ne termine pas le transfert vers le serveur d'origine avant l'expiration de ce délai, il met fin à la demande de connexion. La valeur 0 par défaut indique qu'il n'y a pas de délai d'expiration.
proxy.config.http.accept_no_activity_timeout	ENTIER	120	Spécifie l'intervalle d'expiration, en secondes, devant s'écouler avant que Content Gateway ne ferme une connexion inactive

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.background_fill_active_timeout	ENTIER	60	Spécifie le délai pendant lequel Content Gateway poursuit le traitement en arrière-plan avant d'abandonner la connexion au serveur d'origine
proxy.config.http.background_fill_completed_threshold	VIRGULE FLOTTANTE	0.50000	Spécifie la proportion déjà transférée par rapport à la taille totale du document lorsqu'un client interrompt l'opération alors que le proxy récupère le document sur le serveur d'origine pour le mettre en cache (*traitement en arrière-plan*)

Nombre de tentatives de connexion au serveur d'origine

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.connect_attempts_max_retries	ENTIER	6	Spécifie le nombre maximal de tentatives de connexion effectuées par Content Gateway lorsque le serveur d'origine ne répond pas
proxy.config.http.connect_attempts_max_retries_dead_server	ENTIER	2	Spécifie le nombre maximal de tentatives de connexion effectuées par Content Gateway lorsque le serveur d'origine est indisponible
proxy.config.http.connect_attempts_rr_retries	ENTIER	2	Spécifie le nombre maximal d'échecs de tentatives de connexion autorisés avant qu'une entrée de recherche circulaire ne soit désignée en échec lorsqu'un serveur présente des entrées DNS de recherche circulaire (round-robin)
proxy.config.http.connect_attempts_timeout	ENTIER	60	Spécifie la valeur du délai d'expiration, en secondes, d'une connexion au serveur d'origine
proxy.config.http.streaming_connect_attempts_timeout	ENTIER	1800	Spécifie la valeur du délai d'expiration, en secondes, d'une connexion de contenu en streaming

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. down_server.cache_time	ENTIER	30	Spécifie le délai, en secondes, pendant lequel Content Gateway doit se souvenir qu'un serveur d'origine était inaccessible
proxy.config.http. down_server. abort_threshold	ENTIER	10	Spécifie le nombre de secondes devant s'écouler avant que Content Gateway ne désigne un serveur d'origine comme indisponible lorsqu'un client abandonne une requête parce que le serveur d'origine tarde trop à renvoyer l'en-tête de réponse

Mise en cache des réponses négatives

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. negative_caching_enabled	ENTIER	0	Lorsque cette option est activée (1), Content Gateway met en cache les réponses négatives, par exemple les réponses *404 - Introuvable*, lorsque la page demandée n'existe pas. Lorsqu'un client demande ensuite la même page, Content Gateway dessert la réponse négative stockée dans le cache. Content Gateway met en cache les réponses négatives suivantes : 204 Pas de contenu 305 Utiliser le proxy 400 Demande incorrecte 403 Refusé 404 Non trouvé 405 Méthode non autorisée 500 Erreur interne du serveur 501 Non implémenté 502 Passerelle incorrecte 503 Service indisponible 504 Expiration du délai de la passerelle
proxy.config.http. negative_caching_ lifetime	ENTIER	1800	Spécifie le délai pendant lequel Content Gateway considère les réponses négatives mises en cache comme valides

Variables des utilisateurs du proxy

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http. anonymize_remove_from	ENTIER	0	Lorsque cette option est activée (1), Content Gateway supprime l'en-tête **From** associé aux transactions pour préserver la confidentialité de vos utilisateurs.
proxy.config.http. anonymize_remove_referer	ENTIER	0	Lorsque cette option est activée (1), Content Gateway supprime l'en-tête **Referer** associé aux transactions pour préserver la confidentialité de votre site et de vos utilisateurs.
proxy.config.http. anonymize_remove_ user_agent	ENTIER	0	Lorsque cette option est activée (1), Content Gateway supprime l'en-tête **User-agent** associé aux transactions pour préserver la confidentialité de votre site et de vos utilisateurs.
proxy.config.http. anonymize_remove_cookie	ENTIER	0	Lorsque cette option est activée (1), Content Gateway supprime l'en-tête **Cookie** associé aux transactions pour préserver la confidentialité de votre site et de vos utilisateurs.
proxy.config.http. anonymize_remove_ client_ip	ENTIER	1	Lorsque cette option est activée (1), Content Gateway supprime les en-têtes **Client-IP** pour renforcer la confidentialité.
proxy.config.http. anonymize_insert_ client_ip	ENTIER	0	Lorsque cette option est activée (1), Content Gateway insère des en-têtes **Client-IP** pour conserver l'adresse IP des clients.
proxy.config.http. append_xforwards_header	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ajoute des en-têtes **X-Forwards** dans les requêtes sortantes.
proxy.config.http. anonymize_other_ header_list	CHAÎNE	NULL	Spécifie les en-têtes que Content Gateway doit supprimer des requêtes sortantes

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.snarf_username_from_authorization	ENTIER	0	Lorsque cette option est activée (1), Content Gateway récupère le nom d'utilisateur et le mot de passe dans l'en-tête d'authentification LDAP lorsque le modèle d'authentification est *De base*.
proxy.config.http.insert_squid_x_forwarded_for	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ajoute l'adresse IP du client dans l'en-tête **X-Forwarded-For**.
proxy.config.http.insert_x_authenticated user	ENTIER	0	Lorsque cette option est activée (1), Content Gateway insère l'en-tête **X-Authenticated-User** pour signaler au proxy que l'utilisateur a été authentifié.

Sécurité

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.push_method_enabled	ENTIER	0	Lorsque cette option est activée (1), les règles du fichier **filter.config** peuvent être utilisées pour envoyer directement le contenu dans le cache sans requête d'utilisateur. Vous devez ajouter une règle de filtrage contenant l'action PUSH afin d'être certain que seules les adresses IP sources connues implémentent des requêtes PUSH dans le cache. Cette variable doit être activée pour que l'action PUSH soit disponible dans la liste déroulante des méthodes de l'éditeur de fichiers de configuration.

Contrôle du cache

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.cache.http	ENTIER	1	Active (1) ou désactive (0) la mise en cache des requêtes HTTP
proxy.config.http.cache.ftp	ENTIER	1	Active (1) ou désactive (0) la mise en cache des requêtes FTP envoyées via HTTP
proxy.config.http.cache.ignore_client_no_cache	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ignore les requêtes des clients pour contourner le cache.
proxy.config.http.cache.ims_on_client_no_cache	ENTIER	0	Lorsque cette option est activée (1), Content Gateway envoie une requête conditionnelle au serveur d'origine lorsqu'une requête entrante contient un en-tête **no-cache**.
proxy.config.http.cache.ignore_server_no_cache	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ignore les requêtes des serveurs d'origine pour contourner le cache.
proxy.config.http.cache.cache_responses_to_cookies	ENTIER	3	Définit le mode de mise en cache des cookies : • 0 = Ne pas mettre en cache les réponses dans des cookies • 1 = Mettre en cache tous les types de contenu • 2 = Mettre en cache les types Image uniquement • 3 = Tout mettre en cache sauf le texte
proxy.config.http.cache.ignore_authentication	ENTIER	0	Lorsque cette option est activée (1), Content Gateway ignore les en-têtes **WWW-Authentication** présents dans les réponses. Les en-têtes **WWW-Authentication** sont supprimés et ne sont pas mis en cache.
proxy.config.http.cache.cache_urls_that_look_dynamic	ENTIER	0	Active (1) ou désactive (0) la mise en cache des URL qui semblent dynamiques
proxy.config.http.cache.enable_default_vary_headers	ENTIER	0	Active (1) ou désactive (0) la mise en cache des versions alternatives d'objets HTTP qui ne contiennent pas l'en-tête **Vary**

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.cache.when_to_revalidate	ENTIER	0	Définit la fréquence de revalidation du contenu : • 0 = Utiliser les directives du cache ou les règles heuristiques (valeur par défaut) • 1 = Périmé si heuristique • 2 = Toujours périmé (toujours revalider) • 3 = Jamais périmé • 4 = Utiliser les directives du cache ou les règles heuristiques (0), sauf si la requête contient un en-tête **If-Modified-Since**. Lorsque la requête contient un en-tête **If-Modified-Since**, Content Gateway revalide systématiquement le contenu mis en cache et utilise l'en-tête **If-Modified-Since** du client pour la requête du proxy.
proxy.config.http.cache.when_to_add_no_cache_to_msie_requests	ENTIER	0	Indique quand ajouter des directives **no-cache** dans les requêtes provenant de Microsoft Internet Explorer (MSIE). Vous pouvez spécifier les éléments suivants : • 0 = en-tête **no-cache** non ajouté dans les requêtes MSIE • 1 = en-tête **no-cache** ajouté dans les requêtes MSIE IMS • 2 = en-tête **no-cache** ajouté dans toutes les requêtes MSIE
proxy.config.http.cache.required_headers	ENTIER	0	Définit le type d'en-têtes requis dans une requête pour que celle-ci puisse être mise en cache • 0 = aucun en-tête requis pour que le document soit mis en cache • 1 = au moins un en-tête **Last-Modified** requis • 2 = durée de vie explicite requise (en-tête **Expires** ou **Cache-Control**)

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.cache.max_stale_age	ENTIER	604800	Définit l'âge maximal que peut atteindre une réponse périmée avant de ne plus être mise en cache
proxy.config.http.cache.range.lookup	ENTIER	1	Lorsque cette option est activée (1), Content Gateway recherche des requêtes de plage dans le cache.
proxy.config.http.cache.cache_301_responses	ENTIER	0	Active (1) ou désactive (0) la mise en cache des pages de réponse « 301 »

Expiration heuristique

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.cache.heuristic_min_lifetime	ENTIER	3600	Définit la durée minimale pendant laquelle un document du cache peut être considéré comme récent
proxy.config.http.cache.heuristic_max_lifetime	ENTIER	86400	Définit la durée maximale pendant laquelle un document du cache peut être considéré comme récent
proxy.config.http.cache.heuristic_lm_factor	VIRGULE FLOTTANTE	0.10000	Définit le facteur de vieillissement associé aux calculs de l'actualité des objets
proxy.config.http.cache.fuzz.time	ENTIER	240	Définit l'intervalle, en secondes, devant s'écouler avant que la date de péremption du document vérifiée précédemment par le proxy ne soit réactualisée
proxy.config.http.cache.fuzz.probability	VIRGULE FLOTTANTE	0.00500	Définit la probabilité selon laquelle un document peut être réactualisé autour de l'heure spécifiée

Contenu dynamique et négociation

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.cache.vary_default_text	CHAÎNE	NULL	Définit l'en-tête pris en compte par Content Gateway pour les documents texte. Par exemple, si vous spécifiez **user-agent**, le proxy met en cache toutes les différentes versions user-agent des documents qu'il rencontre.
proxy.config.http.cache.vary_default_images	CHAÎNE	NULL	Définit l'en-tête pris en compte par Content Gateway pour les images
proxy.config.http.cache.vary_default_other	CHAÎNE	NULL	Définit l'en-tête pris en compte par Content Gateway pour les éléments qui ne correspondent ni à du texte ni à des images

Mot de passe FTP anonyme

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.ftp.anonymous_passwd	CHAÎNE	*Valeur associée à l'adresse électronique de l'administrateur, fournie pendant l'installation*	Définit le mot de passe anonyme permettant d'accéder aux serveurs FTP qui exigent un mot de passe Content Gateway utilise le nom du compte Content Gateway comme valeur par défaut de cette variable.

Durée de vie des documents FTP mis en cache

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.http.ftp.cache.document_lifetime	ENTIER	259200	Définit la durée maximale pendant laquelle un document FTP peut rester dans le cache

Mode de transfert FTP

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.http.ftp.binary_transfer_only`	ENTIER	0	Lorsque cette option est activée (1), tous les documents FTP demandés par des clients HTTP sont transférés en mode binaire uniquement. Lorsque cette option est désactivée (0), les documents FTP demandés par des clients HTTP sont transférés en mode ASCII ou binaire, selon le type de document.

Pages de réponse personnalisables

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.body_factory.enable_customizations`	ENTIER	0	Indique si les pages de réponse personnalisables sont activées ou désactivées et définit les pages de réponse utilisées : • 0 = désactiver les pages de réponses personnalisables • 1 = activer les pages de réponses personnalisables dans le répertoire par défaut uniquement • 2 = activer les pages de réponse utilisateur dans la langue cible
`proxy.config.body_factory.enable_logging`	ENTIER	0	Active (1) ou désactive (0) la journalisation des pages de réponses personnalisables. Lorsque cette option est activée, Content Gateway enregistre un message dans le journal des erreurs dès qu'une page de réponse personnalisée est utilisée ou modifiée.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.body_factory.template_sets_dir	CHAÎNE	config/body_factory	Définit le répertoire par défaut des pages de réponse personnalisables
proxy.config.body_factory.response_suppression_mode	ENTIER	0	Indique quand Content Gateway doit supprimer les pages de réponse générées : • 0 = ne jamais supprimer les pages de réponse générées • 1 = toujours supprimer les pages de réponse générées • 2 = supprimer les pages de réponses pour le trafic intercepté uniquement

Moteur FTP

Variable de configuration	Type de données	Valeur par défaut	Description
FTP sur HTTP			
proxy.config.ftp.data_connection_mode	ENTIER	1	Définit le mode de connexion FTP : • 1 = PASV, puis PORT • 2 = PORT uniquement • 3 = PASV uniquement
proxy.config.ftp.control_connection_timeout	ENTIER	300	Définit la durée pendant laquelle Content Gateway doit attendre une réponse d'un serveur FTP
proxy.config.ftp.rc_to_switch_to_PORT	CHAÎNE	NULL	Définit les codes de réponse pour lesquels Content Gateway bascule automatiquement sur la commande PORT en cas d'échec de PASV lorsque la variable de configuration **proxy.config.ftp.data_connection_mode** est définie sur 1 Cette variable est utilisée pour les requêtes FTP provenant de clients HTTP uniquement.
Proxy FTP			
proxy.config.ftp.ftp_enabled	ENTIER	0	Active (1) ou désactive (0) le traitement des requêtes FTP envoyées par des clients FTP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ftp. logging_enabled	ENTIER	1	Active (1) ou désactive (0) la journalisation des transactions FTP
proxy.config.ftp. proxy_server_port	ENTIER	2121	Définit le port utilisé pour les connexions FTP
proxy.config.ftp. open_lisn_port_mode	ENTIER	1	Indique comment FTP ouvre un port d'écoute pour le transfert de données : • 1 = le système d'exploitation choisit un port disponible. Content Gateway envoie 0 et récupère le nouveau numéro de port si l'écoute réussit. • 2 = le port d'écoute est déterminé selon la plage de ports spécifiée par les variables **proxy.config.ftp. min_lisn_port** et **proxy.config.ftp. max_lisn_port** de Content Gateway, décrites ci-dessous.
proxy.config.ftp. min_lisn_port	ENTIER	32768	Définit le port le plus bas de la plage des ports d'écoute utilisée par Content Gateway pour les connexions de données lorsque le client FTP envoie une commande PASV ou lorsque Content Gateway envoie une commande PORT au serveur FTP
proxy.config.ftp. max_lisn_port	ENTIER	65535	Définit le port le plus haut de la plage des ports d'écoute utilisée par Content Gateway pour les connexions de données lorsque le client FTP envoie une commande PASV ou lorsque Content Gateway envoie une commande PORT au serveur FTP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ftp.server_data_default_pasv	ENTIER	1	Définit la méthode utilisée par défaut pour configurer les connexions de données côté serveur : • 1 = Content Gateway envoie une commande PASV au serveur FTP et laisse ce dernier ouvrir un port d'écoute. • 0 = Content Gateway essaie d'abord PORT (configure un port d'écoute sur le côté proxy de la connexion).
proxy.config.ftp.different_client_port_ip_allowed	ENTIER	0	Lorsque cette option est activée (1), Content Gateway peut se connecter à un autre ordinateur que celui sur lequel s'exécute le client FTP pour établir une connexion de données. Le client FTP utilise PORT pour configurer un port d'écoute de son côté et autorise Content Gateway à se connecter à ce port pour établir la connexion de données (pour les transferts de fichiers). Lorsqu'il configure le port d'écoute, le client FTP définit son adresse IP et son numéro de port. Lorsque cette variable est définie sur 0 (zéro), Content Gateway ne peut pas se connecter au client FTP si l'adresse IP envoyée par le client ne correspond pas à celle de l'ordinateur qui exécute le client FTP.
proxy.config.ftp.try_pasv_times	ENTIER	1024	Définit le nombre de tentatives d'ouverture de port d'écoute que peut effectuer Content Gateway lorsque le client FTP envoie une commande PASV
proxy.config.ftp.try_port_times	ENTIER	1024	Définit le nombre maximal de tentatives d'ouverture de port d'écoute que peut effectuer Content Gateway lors de l'envoi d'une commande PORT au serveur FTP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ftp.try_server_ctrl_connect_times	ENTIER	6	Définit le nombre maximal de tentatives de connexion au port d'écoute de contrôle du serveur FTP que peut effectuer Content Gateway
proxy.config.ftp.try_server_data_connect_times	ENTIER	3	Définit le nombre maximal de tentatives de connexion au port d'écoute de données du serveur FTP que peut effectuer Content Gateway lorsqu'il envoie une commande PASV au serveur FTP et récupère les informations IP/port d'écoute
proxy.config.ftp.try_client_data_connect_times	ENTIER	3	Définit le nombre maximal de tentatives de connexion au port d'écoute de données du client FTP que peut effectuer Content Gateway lorsque le client FTP envoie une commande PORT avec les informations IP/port d'écoute
proxy.config.ftp.client_ctrl_no_activity_timeout	ENTIER	900	Définit le délai d'expiration de l'inactivité, en secondes, de la connexion de contrôle au client FTP
proxy.config.ftp.client_ctrl_active_timeout	ENTIER	14400	Définit le délai d'expiration de l'activité, en secondes, de la connexion de contrôle au client FTP
proxy.config.ftp.server_ctrl_no_activity_timeout	ENTIER	120	Définit le délai d'expiration de l'inactivité, en secondes, de la connexion de contrôle au serveur FTP
proxy.config.ftp.server_ctrl_active_timeout	ENTIER	14400	Définit le délai d'expiration de l'activité, en secondes, de la connexion de contrôle au serveur FTP
proxy.config.ftp.client_data_no_activity_timeout	ENTIER	120	Définit le délai maximal, en secondes, pendant lequel une connexion de transfert de données FTP de client peut rester inactive avant d'être abandonnée
proxy.config.ftp.client_data_active_timeout	ENTIER	14400	Définit le délai maximal, en secondes, d'une connexion de transfert de données FTP de client

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ftp.server_data_no_activity_timeout	ENTIER	120	Définit le délai maximal, en secondes, pendant lequel une connexion de transfert de données FTP de serveur peut rester inactive avant d'être abandonnée
proxy.config.ftp.server_data_active_timeout	ENTIER	14400	Définit le délai maximal, en secondes, d'une connexion de transfert de données FTP de serveur
proxy.config.ftp.pasv_accept_timeout	ENTIER	120	Définit la valeur d'expiration d'un port d'écoute de données dans Content Gateway (pour PASV, la connexion de données du client)
proxy.config.ftp.port_accept_timeout	ENTIER	120	Définit la valeur d'expiration d'un port d'écoute de données dans Content Gateway (pour PORT, la connexion de données du serveur)
proxy.config.ftp.share_ftp_server_ctrl_enabled	ENTIER	1	Active (1) ou désactive (0) le partage des connexions de contrôle des serveurs entre plusieurs clients FTP anonymes
proxy.config.ftp.share_only_after_session_end	ENTIER	1	Définit le mode de partage des connexions de contrôle des serveurs FTP entre les différentes sessions de clients FTP : • 1 = la connexion de contrôle au serveur FTP peut *uniquement* être utilisée par une autre session de client FTP lorsque la session du client FTP est terminée (en général, lorsqu'il envoie une commande QUIT). • 0 = la connexion de contrôle au serveur FTP peut *uniquement* être utilisée par une autre session de client FTP lorsque la session du client FTP n'utilise pas activement la connexion au serveur FTP : par exemple, lorsque la requête est un accès fructueux au cache ou pendant une session inactive.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ftp.server_ctrl_keep_alive_no_activity_timeout	ENTIER	90	Définit la valeur d'expiration lorsque la connexion de contrôle aux serveurs FTP n'est utilisée par aucun client FTP.
proxy.config.ftp.reverse_ftp_enabled	ENTIER	0	Non pris en charge
proxy.config.ftp.login_info_fresh_in_cache_time	ENTIER	604800	Définit le délai pendant lequel les réponses 220/230 (messages de connexion) stockées dans le cache peuvent être considérées comme récentes
proxy.config.ftp.data_source_port_20_enabled	ENTIER	0	Lorsque cette option est activée (1), relie le port source 20 des connexions de transfert de données sortantes aux clients FTP en mode actif.

Processeur SOCKS

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.socks.socks_needed	ENTIER	0	Active (1) ou désactive (0) l'option SOCKS Voir *Configuration de l'intégration du pare-feu SOCKS*, page 171.
proxy.config.socks.socks_version	ENTIER	4	Définit la version SOCKS
proxy.config.socks.default_servers	CHAÎNE	s1.exemple.com:1080;socks2:4080	Définit les noms et les ports des serveurs SOCKS avec lesquels Content Gateway communique
proxy.config.socks.accept_enabled	ENTIER	0	Active (1) ou désactive (0) l'option de proxy SOCKS. En tant que proxy SOCKS, Content Gateway reçoit le trafic SOCKS (en général sur le port 1080) et transmet directement toutes les requêtes au serveur SOCKS.
proxy.config.socks.accept_port	ENTIER	1080	Définit le port sur lequel Content Gateway accepte le trafic SOCKS

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.socks.socks_server_enabled	ENTIER	0	Remarque : cette option ne doit être configurée que si Content Gateway est installé dans un dispositif.
proxy.config.socks.socks_server_port	ENTIER	61080	Remarque : cette option ne doit être configurée que si Content Gateway est installé dans un dispositif.

Sous-système réseau

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.net.connections_throttle	ENTIER	45000	Définit le nombre maximal de connexions que Content Gateway peut traiter. Lorsque Content Gateway reçoit des requêtes de clients supplémentaires, celles-ci sont mises en file d'attente jusqu'à ce que les requêtes existantes aient été desservies. Ne définissez pas cette variable au-dessous de 100.

Sous-système de cluster

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.cluster.cluster_port	ENTIER	8086	Définit le port utilisé pour la communication avec le cluster
proxy.config.cluster.ethernet_interface	CHAÎNE	*votre_interface*	Définit l'interface réseau utilisée pour le trafic du cluster. Tous les nœuds de ce cluster doivent utiliser la même interface réseau.

Cache

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.cache.permit.pinning`	ENTIER	0	Active (1) ou désactive (0) l'option d'épinglage dans le cache, qui vous permet de conserver des objets dans le cache pour une durée spécifiée. Définissez les règles d'épinglage du cache dans le fichier **cache.config** (voir *Fichier de configuration cache.config*, page 352).
`proxy.config.cache.ram_cache.size`	ENTIER	-1	Définit la taille du cache de mémoire RAM, en octets -1 signifie que la taille du cache de mémoire RAM est automatiquement définie sur 41 Mo environ par Go de disque.
`proxy.config.cache.limits.http.max_alts`	ENTIER	3	Définit le nombre maximal d'alternatives HTTP que Content Gateway peut mettre en cache
`proxy.config.cache.max_doc_size`	ENTIER	0	Définit la taille maximale des documents du cache (en octets) : 0 = aucune limite de taille

DNS

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.dns. search_default_domains	ENTIER	1	Active (1) ou désactive (0) l'extension de domaine local de sorte que Content Gateway puisse résoudre les noms d'hôte non qualifiés en étendant le domaine local. Par exemple, lorsqu'un client demande un nom d'hôte non qualifié nommé **host_x** et que le domaine local Content Gateway est **y.com**, Content Gateway étend le nom d'hôte en **host_x.y.com**.
proxy.config.dns. splitDNS.enabled	ENTIER	0	Active (1) ou désactive (0) la sélection du serveur DNS. Lorsque cette option est activée, Content Gateway recherche la spécification de la sélection dans le fichier **splitdns.config**. Voir *Utilisation de l'option de division DNS*, page 175.
proxy.config.dns. splitdns.def_domain	CHAÎNE	NULL	Définit le domaine utilisé par défaut pour diviser les requêtes DNS. Cette valeur est automatiquement ajoutée à la fin du nom d'hôte lorsque celui-ci n'inclut pas de domaine avant que la division DNS n'identifie le serveur DNS à utiliser.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.dns. url_expansions	CHAÎNE	NULL	Définit la liste des extensions de noms d'hôte ajoutées automatiquement au nom d'hôte après un échec de recherche. Par exemple, pour que Content Gateway ajoute l'extension **.org** au nom d'hote, définissez cette variable sur la valeur **org** (Content Gateway ajoute le point (.) automatiquement) Remarque : si la variable **proxy.config.http.enable_url_expandomatic** est définie sur 1 (valeur par défaut), il n'est pas nécessaire d'ajouter **www.** et **.com** dans cette liste. Content Gateway essaie automatiquement **www.** et **.com** après avoir tenté les valeurs que vous avez définies.
proxy.config.dns. lookup_timeout	ENTIER	20	Défini le délai d'expiration des recherches DNS, en secondes. Lorsque ce délai expire, la tentative de recherche cesse.
proxy.config.dns.retries	ENTIER	5	Définit le nombre de tentatives de recherche DNS pouvant être effectuées avant l'abandon
proxy.config.dns. prefer_ipv4	ENTIER	1	Définit le type d'adresse favori, lorsqu'un nom peut être résolu à la fois en adresses IPv4 et IPv6
proxy.config.ipv6. ipv6_enabled	ENTIER	0	Indique si la prise en charge d'IPv6 est activée (1) ou désactivée (0)

Proxy DNS

Variable de configuration Type de données	Type de données	Valeur par défaut	Description
proxy.config.dns.proxy.enabled	ENTIER	0	Active (1) ou désactive (0) l'option de mise en cache du proxy DNS qui vous permet de résoudre les requêtes DNS au nom des clients. Cette option décharge les serveurs DNS distants et réduit les délais de réponse des recherches DNS. Voir *Mise en cache du proxy DNS*, page 95.
proxy.config.dns.proxy_port	ENTIER	5353	Définit le port utilisé par Content Gateway pour le trafic DNS

Base de données des hôtes (HostDB)

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.hostdb.size	ENTIER	200000	Définit le nombre maximal d'entrées autorisées dans la base de données des hôtes
proxy.config.hostdb.ttl_mode	ENTIER	0	Définit le mode de durée de vie (TTL) de la base de données des hôtes. Vous pouvez spécifier l'un des éléments suivants : • 0 = respecter • 1 = ignorer • 2 = min(X,durée de vie) • 3 = max(X,durée de vie)
proxy.config.hostdb.timeout	ENTIER	86400	Définit le délai d'expiration au premier plan, en secondes
proxy.config.hostdb.fail.timeout	ENTIER	60	Définit le délai pendant lequel un échec DNS doit être mis en cache, en secondes
proxy.config.hostdb.strict_round_robin	ENTIER	0	Lorsque cette option est désactivée (0), Content Gateway utilise systématiquement le même serveur d'origine pour un même client tant que le serveur d'origine est disponible.

Configuration de la journalisation

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.log2.logging_enabled	ENTIER	1	Active et désactive la journalisation des événements : • 0 = journalisation désactivée • 1 = enregistrer les erreurs uniquement • 2 = enregistrer les transactions uniquement • 3 = journalisation complète (erreurs + transactions) Voir *Utilisation des fichiers journaux*, page 211.
proxy.config.log2.max_secs_per_buffer	ENTIER	5	Définit le délai maximal pouvant s'écouler avant que les données mises en mémoire tampon soient effacées et envoyées sur le disque
proxy.config.log2.max_space_mb_for_logs	ENTIER	5120 ou 20480	Définit la quantité d'espace allouée au répertoire de journalisation, en méga-octets Lorsque Content Gateway est installé dans un dispositif V-series, la taille est définie sur 5 120 (5 Go) et n'est pas modifiable. Lorsque Content Gateway est installé dans un serveur autonome, la taille par défaut est de 20 480 (20 Go) et peut être configurée.
proxy.config.log2.max_space_mb_for_orphan_logs	ENTIER	25	Définit la quantité d'espace allouée au répertoire de journalisation, en méga-octets, lorsque ce nœud joue le rôle de client de collecte
proxy.config.log2.max_space_mb_headroom	ENTIER	100	Définit la tolérance vis-à-vis de la limite d'espace occupé par les journaux, en octets. Si la variable **proxy.config.log2.auto_delete_rolled_file** est définie sur 1 (activée), l'auto-suppression des fichiers journaux se déclenche lorsque la quantité d'espace disponible dans le répertoire de journalisation descend au-dessous de la valeur définie ici.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.log2.hostname	CHAÎNE	localhost	Définit le nom d'hôte de l'ordinateur exécutant Content Gateway
proxy.config.log2.logfile_dir	CHAÎNE	/opt/WCG/logs	Définit le chemin complet du répertoire de journalisation
proxy.config.log2.logfile_perm	CHAÎNE	rw-r--r--	Définit les autorisations des fichiers journaux. Les autorisations de fichier UNIX standard sont utilisées (propriétaire, groupe, autre). Les valeurs valides sont les suivantes : • - = aucune autorisation • r = autorisation de lecture • w = autorisation d'écriture • x = autorisation d'exécution Les autorisations dépendent des paramètres umask du processus Content Gateway. Cela signifie qu'un paramètre umask de 002 n'accordera pas d'autorisation en écriture aux autres, même si cela est spécifié dans le fichier de configuration. Les autorisations des fichiers journaux existants ne sont pas modifiées lorsque la configuration est modifiée. Pour Linux uniquement
proxy.config.log2.custom_logs_enabled	ENTIER	0	Lorsque cette option est activée (1), prend en charge la définition et la génération des fichiers journaux personnalisés conformément aux spécifications du fichier **logs_xml.config**. Voir *Fichier de configuration logs_xml.config*, page 364.
proxy.config.log2.xml_logs_config	ENTIER	1	Définit la taille (en Mo) qui, une fois atteinte, entraîne la rotation des fichiers journaux. Voir *Rotation des fichiers journaux d'événements*, page 221.
proxy.config.log2.squid_log_enabled	ENTIER	0	Active (1) ou désactive (0) le format de fichier journal Squid

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.log2. squid_log_is_ascii	ENTIER	1	Définit le type de fichier journal Squid : • 1 = ASCII • 0 = binaire
proxy.config.log2. squid_log_name	CHAÎNE	squid	Définit le nom du fichier journal Squid
proxy.config.log2. squid_log_header	CHAÎNE	NULL	Définit le texte de l'en-tête du fichier journal Squid
proxy.config.log2. common_log_enabled	ENTIER	0	Active (1) ou désactive (0) le format de fichier journal Netscape Common
proxy.config.log2. common_log_is_ascii	ENTIER	1	Définit le type de fichier journal Netscape Common : • 1 = ASCII • 0 = binaire
proxy.config.log2. common_log_name	CHAÎNE	common	Définit le nom du fichier journal Netscape Common
proxy.config.log2. common_log_header	CHAÎNE	NULL	Définit le texte de l'en-tête du fichier journal Netscape Common
proxy.config.log2. extended_log_enabled	ENTIER	1	Active (1) ou désactive (0) le format de fichier journal Netscape Extended
proxy.confg.log2. extended_log_is_ascii	ENTIER	1	Définit le type de fichier journal Netscape Extended : • 1 = ASCII • 0 = binaire
proxy.config.log2. extended_log_name	CHAÎNE	extended	Définit le nom du fichier journal Netscape Extended
proxy.config.log2. extended_log_header	CHAÎNE	NULL	Définit le texte de l'en-tête du fichier journal Netscape Extended
proxy.config.log2. extended2_log_enabled	ENTIER	0	Active (1) ou désactive (0) le format de fichier journal Netscape Extended-2
proxy.config.log2. extended2_log_is_ascii	ENTIER	1	Définit le type de fichier journal Netscape Extended-2 : • 1 = ASCII • 0 = binaire
proxy.config.log2. extended2_log_name	CHAÎNE	extended2	Définit le nom du fichier journal Netscape Extended-2
proxy.config.log2. extended2_log_header	CHAÎNE	NULL	Définit le texte de l'en-tête du fichier journal Netscape Extended-2

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.log2. separate_host_logs	ENTIER	0	Lorsque cette option est activée (1), configure Content Gateway pour qu'il crée un fichier journal distinct pour les transactions HTTP/FTP de chaque serveur d'origine répertorié dans le fichier **log_hosts.config** (voir *Division des journaux des hôtes HTTP*, page 224).
proxy.local.log2. collation_mode	ENTIER	0	Définit le mode de collecte des journaux : • 0 = collecte désactivée • 1 = cet hôte est un serveur de collecte des journaux • 2 = cet hôte est un client de collecte des journaux et envoie les entrées au serveur de collecte dans des formats standard Pour plus d'informations sur l'envoi des formats personnalisés de type XML au serveur de collecte, consultez la section *Fichier de configuration logs_xml.config*, page 364.
proxy.confg.log2. collation_host	CHAÎNE	NULL	Définit le nom d'hôte du serveur de collecte des journaux
proxy.config.log2. collation_port	ENTIER	8085	Définit le port utilisé pour la communication entre le serveur et le client de collecte
proxy.config.log2. collation_secret	CHAÎNE	foobar	Définit le mot de passe utilisé pour valider la journalisation des données et interdire tout échange d'informations non autorisées lors de l'utilisation d'un serveur de collecte
proxy.config.log2. collation_host_tagged	ENTIER	0	Activée (1), cette option configure Content Gateway pour qu'il inclut dans chaque entrée du journal le nom d'hôte du client de collecte ayant généré cette entrée
proxy.config.log2. collation_retry_sec	ENTIER	5	Définit le nombre de secondes devant s'écouler entre les tentatives de connexion au serveur de collecte

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.log2. rolling_enabled	ENTIER	1	Active (1) ou désactive (0) la rotation des fichiers journaux Voir *Rotation des fichiers journaux d'événements*, page 221.
proxy.config.log2. rolling_interval_sec	ENTIER	21600	Définit l'intervalle de rotation des fichiers journaux, en secondes. La valeur minimale est 300 (5 minutes). La valeur maximale est 86 400 secondes (un jour).
proxy.config.log2. rolling_offset_hr	ENTIER	0	Définit l'heure de décalage de la rotation des fichiers, c'est-à-dire l'heure de la journée à laquelle commence la période de rotation des journaux
proxy.config.log2. rolling_size_mb	ENTIER	10	Définit la taille (en méga-octets) qui, une fois atteinte, entraîne la fermeture du fichier en cours et la création d'un nouveau fichier
proxy.config.log2. auto_delete_rolled_files	ENTIER	1	Active (1) ou désactive (0) la suppression automatique des fichiers journaux ayant subi une rotation
proxy.config.log2. sampling_frequency	ENTIER	1	Configure Content Gateway pour qu'il enregistre uniquement un échantillon de transactions et non pas chaque transaction. Vous pouvez spécifier les valeurs suivantes : • 1 = enregistrer chaque transaction • 2 = enregistrer chaque deuxième transaction • 3 = enregistrer chaque troisième transaction etc...

Règles de remappage des URL

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.url_remap.default_to_server_pac`	ENTIER	0	Active (1) ou désactive (0) la redirection des requêtes portant sur un fichier PAC du port de service du proxy (8080 par défaut) au port PAC Pour que ce type de redirection fonctionne, la variable proxy.config.reverse_proxy.enabled doit être définie sur 1.
`proxy.config.url_remap.default_to_server_pac_port`	ENTIER	-1	Définit le port PAC de sorte que les requêtes PAC envoyées au port de service du proxy Content Gateway soient redirigées vers ce port **-1** indique que le port PAC doit être défini sur le port d'auto-configuration (le port d'auto-configuration est le 8083). Il s'agit là du paramètre par défaut. Cette variable peut être combinée à la variable **proxy.config.url_remap.default_to_server_pac** pour récupérer un fichier PAC à partir d'un port différent. Vous devez créer et exécuter un processus desservant un fichier PAC sur ce port. Par exemple, si vous créez un script Perl qui écoute sur le port 9000 et écrit un fichier PAC en réponse à chaque requête, vous pouvez définir cette variable sur 9000 pour que les navigateurs qui demandent le fichier PAC à partir d'un serveur proxy sur le port 8080 obtiennent ce fichier PAC desservi par le script Perl.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.url_remap. remap_required	ENTIER	0	Définissez cette variable sur 1 pour que Content Gateway desservent uniquement les requêtes provenant des serveurs d'origine répertoriés dans les règles de mappage du fichier remap.config. Lorsqu'une requête n'a pas de correspondance, le navigateur reçoit une erreur.
proxy.config.url_remap. pristine_host_hdr	ENTIER	0	Définissez cette variable sur 1 pour conserver l'en-tête de l'hôte du client présent dans une requête lors du remappage

Configuration des mises à jour planifiées

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.update. enabled	ENTIER	0	Active (1) ou désactive (0) l'option de mise à jour planifiée
proxy.config.update. force	ENTIER	0	Active (1) ou désactive (0) l'option de mise à jour immédiate imposée. Lorsque cette option est activée, Content Gateway ignore le délai d'expiration de la planification pour toutes les entrées de mise à jour planifiées et déclenche des mises à jour jusqu'à la désactivation de cette option.
proxy.config.update. retry_count	ENTIER	10	Définit le nombre de nouvelles tentatives de mises à jour d'une URL que Content Gateway peut effectuer en cas d'échec
proxy.config.update. retry_interval	ENTIER	2	Définit le délai (en secondes) devant s'écouler entre chaque nouvelle tentative de mise à jour d'une URL en cas d'échec
proxy.config.update. concurrent_updates	ENTIER	100	Définit le nombre maximal de requêtes de mises à jour simultanées autorisées à tout moment. Cette option empêche le processus de mise à jour planifiée de surcharger l'hôte.

Configuration SNMP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.snmp.master_agent_enabled	ENTIER	0	
proxy.config.snmp_encap_enabled	ENTIER	0	

Configuration des plug-in

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.plugin.plugin_dir	CHAÎNE	config/plugins	Définit le répertoire dans lequel sont stockés les plug-ins

Configuration WCCP

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.wccp.enabled	ENTIER	0	Active (1) ou désactive (0) WCCP

FIPS (Configuration de la sécurité)

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.fips.security_enabled	ENTIER	0	Préserve les paramètres FIPS des clients qui effectuent la mise à niveau de la version 7.5.3 de FIPS vers la version 7.7 uniquement
proxy.config.fips.security_enabled_ui	ENTIER	0	Préserve les paramètres de l'interface utilisateur FIPS des clients qui effectuent la mise à niveau de la version 7.5.3 de FIPS vers la version 7.7 uniquement

Décryptage SSL

> **Remarque**
> La configuration du décryptage SSL doit être effectuée dans Content Gateway Manager. Aucune des variables décrites dans le tableau ci-dessous ne doit être modifiée directement dans le fichier records.config.

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.ssl_decryption.use_decryption	ENTIER	0	Lorsque cette option est activée (1), Content Gateway effectue le décryptage SSL.
proxy.config.ssl_decryption_ports	ENTIER	443	Définit les ports HTTPS. Content Gateway autorise le décryptage SSL et la recherche de stratégie sur les ports spécifiés uniquement.
proxy.config.ssl_decryption.ui_enabled	ENTIER	0	Lorsque cette option est activée (1), l'onglet de configuration SSL s'affiche dans Content Gateway Manager.
proxy.config.ssl_management_port	ENTIER	8071	Port de gestion sur lequel SSL Manager est à l'écoute
proxy.config.ssl_inbound_port	ENTIER	8070	Port sur lequel SSL Manager est à l'écoute du trafic entrant (face au client)
proxy.config.ssl_outbound_port	ENTIER	8090	Port utilisé par SSL Manager pour le trafic sortant (face à Internet)

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config. ssl_outbound_ip	CHAÎNE	127.0.0.1	Adresse IP du proxy entrant et sortant de SSL Manager
proxy.config. ssl_forward_to_inbound	ENTIER	1	Ne pas modifier Lorsque SSL Manager est activé, entraîne le transfert du trafic SSL vers le port du proxy approprié.
proxy.config. administrator_id	CHAÎNE	NULL	Ne pas modifier Conserve l'ID de l'administrateur crypté. Cette variable est utilisée par SSL Manager.
proxy.config. ssl_decryption. tunnel_skype	ENTIER	0	Lorsque cette option est activée (1), Content Gateway identifie et met en tunnel le trafic Skype (déploiement de proxy explicite uniquement). Les stratégies d'utilisateurs doivent être ajustées en conséquence. Consultez les informations de configuration de la section *Activation de SSL Manager*, page 132.
proxy.config. ssl_decryption. master_cas	CHAÎNE	127.0.0.1	Ne pas modifier La valeur est définie automatiquement lorsque **SSL Manager Configuration Server (Serveur de configuration SSL Manager)** est spécifié dans l'interface utilisateur. La valeur 127.0.0.1 signifie que le serveur de configuration SSL maître est l'hôte local.

ICAP

Variable de configuration	Type de données	Valeur par défaut	Description
`proxy.config.icap.enabled`	`ENTIER`	`0`	Active (1) ou désactive (0) la prise en charge du service ICAP avec Websense Data Security Suite (DSS). Voir *Utilisation de Websense Data Security*, page 119.

`proxy.config.icap.ICAPUri`	`CHAÎNE`	`NULL`	Définit l'URI (Uniform Resource Identifier) du service ICAP
			Un serveur de sauvegarde peut être spécifié dans une liste séparée par des virgules.
			Demandez l'identifiant à votre administrateur DSS. Entrez l'URI au format suivant :
			`icap://nomhôte:port/chemin`
			Pour *`nomhôte`*, saisissez l'adresse IP ou le nom d'hôte du dispositif DSS Protector.
			Le port ICAP par défaut est le 1344.
			`Chemin` correspond au chemin d'accès du service ICAP dans l'ordinateur hôte.
			Par exemple :
			`icap://ordinateur_ICAP:1344/opt/icap_services`
			Si vous utilisez le port ICAP par défaut 1344, vous n'avez pas besoin de spécifier le port.

`proxy.config.icap.FailOpen`	`ENTIER`	`1`	Définissez cette valeur sur : • 1 pour autoriser le trafic lorsque le ou les serveurs ICAP sont en panne • 0 pour envoyer une page de blocage lorsque le ou les serveurs ICAP sont en panne

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.icap. BlockHugeContent	ENTIER	0	Définissez cette valeur sur : • 0 pour envoyer une page de blocage lorsque la taille du fichier envoyé est supérieure à la limite de taille définie par Data Security Suite. Dans DSS, la limite de taille par défaut est de 12 Mo. • 1 pour autoriser le trafic
proxy.config.icap. AnalyzeSecureContent	ENTIER	1	Définissez cette valeur sur : • 0 lorsque le trafic décrypté doit être directement envoyé à destination • 1 lorsque le trafic décrypté doit être envoyé à Data Security Suite pour analyse
proxy.config.icap. AnalyzeFTP	ENTIER	1	Lorsque cette option est activée (1), envoie les transferts de chargement de fichier FTP natifs au serveur ICAP pour analyse.
proxy.config.icap. ActiveTimeout	ENTIER	5	Délai d'expiration de la lecture/réponse, en secondes. L'activité est considérée comme défaillante lorsque le délai d'expiration est dépassé.
proxy.config.icap. RetryTime	ENTIER	5	Intervalle de récupération, en secondes, permettant de tester la remise en activité d'un serveur défaillant
proxy.config.icap. LoadBalance	ENTIER	1	Lorsque des serveurs ICAP sont spécifiés, définissez cette option sur : • 1 pour envoyer les requêtes à tous les serveurs disponibles • 0 pour envoyer les requêtes au serveur principal uniquement

Data Security

Variable de configuration	Type de données	Valeur par défaut	Description
proxy.config.dss.enabled	ENTIER	0	Active (1) ou désactive (0) la prise en charge de Data Security prêt à l'emploi. Voir *Utilisation de Websense Data Security*, page 119.
proxy.config.dss. AnalyzeFTP	ENTIER	1	Lorsque cette option est activée (1), envoie les transferts de chargement de fichier FTP natifs au moteur de stratégies Data Security prêt à l'emploi pour analyse.
proxy.config.dss. AnalyzeSecureContent	ENTIER	1	Définissez cette valeur sur : • 0 lorsque le trafic décrypté doit être directement envoyé à destination • 1 lorsque le trafic décrypté doit être envoyé à Data Security Suite pour analyse
proxy.config.dss. analysis_timeout	ENTIER	10000	Définit le délai maximal, en millisecondes, pendant lequel l'analyse d'un même fichier peut être effectuée avant que cette analyse ne soit abandonnée

Connectivité, analyse et conditions de limites

Variable de configuration	Type de données	Valeur par défaut	Description
wtg.config. subscription_key	CHAÎNE	NULL	Conserve la valeur de la clé d'abonnement Websense Security Gateway ou Websense Security Gateway Anywhere
wtg.config. download_server_ip	CHAÎNE	download. websense.com	Conserve le nom d'hôte ou l'adresse IP du serveur de téléchargement Websense
wtg.config. download_server_port	ENTIER	80	Conserve le numéro de port du serveur de téléchargement Websense
wtg.config. policy_server_ip	CHAÎNE		Conserve l'adresse IP de Websense Policy Server
wtg.config. policy_server_port	ENTIER	55806	Conserve le numéro de port du serveur Websense Policy Server

Variable de configuration	Type de données	Valeur par défaut	Description
wtg.config.wse_server_ip	CHAÎNE		Conserve l'adresse IP du service de filtrage Websense
wtg.config. wse_server_port	ENTIER	15868	Conserve le numéro de port de l'interface WISP du service de filtrage Websense
wtg.config.wse_server_timeout	ENTIER	5000	Définit le délai maximal, en millisecondes, de la communication avec le service de filtrage
wtg.config. ssl_bypassed_categories	CHAÎNE	NULL	Cette variable récupère la liste des identificateurs de catégories qui ignorent le décryptage SSL. **Ne modifiez pas la valeur de cette variable.** Son inclusion vise exclusivement à simplifier le dépannage. Servez-vous de Web Security Manager pour définir les catégories devant ignorer le décryptage SSL.
wtg.config. ssl_decryption_bypass_ ip_based	ENTIER	0	Indique que le processus de contournement de catégories SSL utilise uniquement l'adresse IP (pas le nom d'hôte) lors de la recherche de catégorie 0 = désactivé 1 = activé
wtg.config.fail_open	ENTIER	1	Indique si Content Gateway doit autoriser ou bloquer la requête lorsque le service de filtrage Web de Websense n'est pas disponible Définissez cette valeur sur : • 0 pour envoyer une page de blocage • 1 pour autoriser la requête

Variable de configuration	Type de données	Valeur par défaut	Description
wtg.config. fail_open_analytic_scan	ENTIER	1	Définit le comportement que Content Gateway doit adopter lorsque l'analyse ne fonctionne plus Définissez cette valeur sur : • 0 pour bloquer le trafic • 1 pour effectuer une recherche dans la base de données principale des URL et appliquer la stratégie **Remarque :** une alarme se déclenche dès qu'une analyse ne fonctionne plus.
wtg.config.archive_depth	ENTIER	5	Définit la profondeur maximale des analyses effectuées dans les fichiers d'archive
wtg.config. max_decompressions	ENTIER	10	Définit le nombre maximal de décompressions totales à effectuer dans les fichiers d'archives (par transaction). Cette valeur ne doit pas dépasser 25.
wtg.config. max_subsamples	ENTIER	10000	Définit le nombre maximal de fichiers discrets d'un fichier d'archive que Content Gateway peut décompresser et analyser pour classifier une transaction donnée
wtg.config. zipbomb_action	ENTIER	1	Réservée à l'usage interne. Indique l'état d'analyse « zip bomb ». **Ne modifiez pas la valeur de cette variable.**
wtg.config. max_mem_allowed	ENTIER	1500	Définit la quantité maximale de mémoire (en méga-octets) qui, une fois consommée, oblige Content Gateway à surveiller plus attentivement la mémoire
wtg.config.lowmem_behavior	ENTIER	0	Active (1) ou désactive (0) le contournement de l'analyse, tout en assurant le filtrage
wtg.config.lowmem_timeout	ENTIER	120	Valeur du délai d'expiration (en minutes) de la gestion de mémoire insuffisante. Lorsque ce délai est écoulé, l'état « no management (pas de gestion) » est réinitialisé.

Variable de configuration	Type de données	Valeur par défaut	Description
wtg.config.rdnsclients	ENTIER	0	Active (1) ou désactive (0) la journalisation des noms d'hôte des clients dans les enregistrements des journaux via la réalisation d'une recherche DNS inversée sur chaque nom
wtg.config. ip_ranges_not_to_scan	CHAÎNE	10.0.0.0- 10.255.255.255, 172.16.0.0- 172.31.255.255, 192.168.0.0- 192.168.255.255	Définit les plages d'adresses IP internes à ne pas analyser. Par défaut, la liste correspond aux adresses IP privées standard non routables. Les adresses des plages sont séparées par des tirets et les plages sont séparées par une virgule. Cette option se révèle particulièrement utile dans les déploiements de proxy explicite qui n'utilisent pas de fichier PAC et lorsque vous souhaitez exclure de l'analyse des adresses IP internes standard.
wtg.config. scan_ip_ranges	ENTIER	1	Active (1) ou désactive (0) le contournement des plages d'adresses IP internes définies dans wtg.config. ip_ranges_not_to_scan. Voir ci-dessus.

Fichier de configuration remap.config

Le fichier `remap.config` contient les règles de mappage que Websense Content Gateway utilise pour rediriger définitivement ou temporairement les requêtes HTTP sans que Content Gateway ne contacte aucun serveur d'origine :

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Chaque ligne du fichier **remap.config** doit contenir une règle de mappage. Content Gateway reconnaît trois champs délimités par un espace : type, cible et remplacement. Le tableau suivant décrit le format de chacun de ces champs.

Champ	Description
type	Spécifiez l'un des éléments suivants : • `redirect` : redirige définitivement les requêtes HTTP sans que le serveur d'origine n'ait besoin d'être contacté. Les redirections permanentes signalent la modification d'URL au navigateur (en renvoyant l'état HTTP de code 301) pour que celui-ci puisse mettre à jour les signets. • `redirect_temporary` : redirige temporairement les requêtes HTTP sans que le serveur d'origine n'ait besoin d'être contacté. Les redirections temporaires signalent la modification d'URL au navigateur pour la requête en cours uniquement (en renvoyant l'état HTTP de code 307).
target	Saisissez l'URL d'origine ou *from*. Vous pouvez saisir jusqu'à quatre composants : *schéma://hôte:port/préfixe_chemin* Le *schéma* peut être `http, https` ou `ftp`.
replacement	Saisissez l'URL de destination ou *to*. Vous pouvez saisir jusqu'à quatre composants : *schéma://hôte:port/préfixe_chemin* Le *schéma* peut être `http, https` ou `ftp`.

> **Remarque**
> Le type de schéma (HTTP, HTTPS, FTP) de la cible et du remplacement doivent correspondre.

Exemples

La section suivante présente des exemples de règles de mappage dans le fichier **remap.config**.

Règles de mappage de redirection

La règle suivante redirige *en permanence* toutes les requêtes HTTP de `www.entreprise.com` vers `www.entreprise2.com` :

```
redirect http://www.entreprise.com http://
www.entreprise2.com
```

La règle suivante redirige *temporairement* toutes les requêtes HTTP de `www.entreprise.com` vers `www.entreprise2.com` :

```
redirect_temporary http://www.entreprise1.com http://
www.entreprise2.com
```

Fichier de configuration socks.config

Le fichier **socks.config** spécifie :

- Serveurs SOCKS que le proxy doit utiliser pour accéder à certains serveurs d'origine, et ordre dans lequel le proxy doit parcourir la liste des serveurs SOCKS
- Serveurs d'origine auxquels Content Gateway peut accéder directement, *sans* passer par un serveur SOCKS

Remarque
Il est recommandé d'effectuer l'ensemble de la configuration SOCKS dans Content Gateway Manager.

Important
Après avoir modifié ce fichier, vous devez redémarrer le proxy.

Le trafic qui ne correspond pas à une règle configurée manuellement est traité via la règle par défaut. Une règle par défaut est établie pour chaque serveur SOCKS pour lequel l'option **par défaut** est activée dans le tableau **Serveurs Socks**. Les règles par défaut sont créées automatiquement et s'affichent dans la page Serveur SOCKS. Les règles par défaut ne sont pas écrites dans le fichier **socks.config**. L'adresse IP de destination est 'All' (Toutes).

Format

Pour définir les serveurs SOCKS que le proxy doit utiliser pour atteindre certains serveurs d'origine, ajoutez des règles dans le fichier **socks.config** au format suivant :

```
dest_ip=adresseIP socksparent="alias1" [round_robin=valeur]
```

où :

adresseIP correspond à l'adresse IP du serveur d'origine ou à une plage d'adresses IP séparées par `-` ou `/`.

alias1 est le nom d'alias du serveur SOCKS nommé dans la liste **Serveurs SOCKS**.

La *valeur* est soit `strict`, si vous voulez que Content Gateway essaie les serveurs SOCKS un par un, soit `false` lorsque vous ne voulez pas qu'une recherche circulaire (round-robin) soit effectuée.

Pour définir les serveurs d'origine auxquels Content Gateway doit pouvoir accéder directement, *sans* passer par le(s) serveur(s) SOCKS, saisissez une règle dans le fichier **socks.config** au format suivant :

```
no_socks adresseIP
```

où *adresseIP* est une liste d'adresses IP ou de plages d'adresses IP séparées par des virgules associées aux serveurs d'origine auxquels Content Gateway doit pouvoir accéder directement. Ne spécifiez pas l'adresse de diffusion de tous les réseaux : 255.255.255.255.

> **Remarque**
> Chaque règle du fichier **socks.config** ne doit pas dépasser 400 caractères. L'ordre d'apparition des règles dans le fichier **socks.config** n'a pas d'importance.

Exemples

L'exemple suivant configure le proxy pour qu'il envoie des requêtes aux serveurs d'origine associés à la plage d'adresses IP 123.15.17.1 - 123.14.17.4 via les alias de serveurs SOCKS 'alias1' et 'alias2'. Le spécificateur facultatif de recherche circulaire (**round_robin**) étant défini sur **strict**, le proxy envoie la première requête à alias1, la deuxième à alias2, la troisième à alias1, etc.

```
dest_ip=123.14.15.1 - 123.14.17.4
socksparent="alias; alias2" round_robin=strict
```

L'exemple suivant configure le proxy pour qu'il accède directement au serveur d'origine associé à l'adresse IP 11.11.11.1, *sans* passer par le serveur SOCKS :

```
no_socks 11.11.11.1
```

L'exemple suivant configure Content Gateway pour qu'il accède directement aux serveurs d'origine associés à la plage d'adresses IP 123.14.15.1 - 123.14.17.4 et à l'adresse IP 113.14.18.2, *sans* passer par le serveur SOCKS :

```
no_socks 123.14.15.1 - 123.14.17.4, 113.14.18.2
```

Fichier de configuration socks_server.config

Le fichier **socks_server.config** définit les serveurs SOCKS disponibles pour Content Gateway.

Format

Pour définir les serveurs SOCKS, utilisez le format suivant :

```
alias=nom host=adresse_IP|nom_domaine port=numéro_port
[username=nom_utilisateur password=motdepasse]
default=true|false
```

où :

nom correspond au nom d'un serveur SOCKS.

adresse_IP ou *nom_domaine* correspond à une adresse IP ou un nom de domaine que votre service DNS peut résoudre.

numéro_port correspond au port sur lequel le serveur SOCKS est à l'écoute.

nomutilisateur et *motdepasse* correspond à la paire nom d'utilisateur/mot de passe de l'authentification SOCKS 5. Le mot de passe est crypté.

Définissez la valeur par défaut sur *true* pour que le serveur spécifié soit le serveur SOCKS par défaut. Lorsque l'option de serveur par défaut est activée, le serveur SOCKS est utilisé lorsque aucune règle SOCKS ne correspond.

Lorsqu'aucun serveur SOCKS n'est désigné comme serveur par défaut, le trafic qui ne correspond à aucune règle ne passe pas par un serveur SOCKS.

Exemples :

Cet exemple ajoute le serveur SOCKS 'pardéfaut1' à l'adresse 127.0.0.1 sur le port 61080. Ce serveur est désigné comme serveur SOCKS par défaut.

```
alias=pardéfaut1 host=127.0.0.1 port=61080 default=true
```

Cet exemple ajoute un serveur SOCKS qui utilise l'authentification. Notez que le mot de passe « 465751475058 » n'est pas le vrai mot de passe, mais le mot de passe crypté.

```
alias=test1 host=socks5.exemple.com port=1080 username=test
password=465751475058 default=false
```

Si vous modifiez ce fichier, vous devez redémarrer Content Gateway.

> **Remarque**
> Chaque règle du fichier **socks_server.config** ne doit pas dépasser 400 caractères.

Fichier de configuration splitdns.config

Le fichier **splitdns.config** vous permet de définir le serveur DNS que Content Gateway doit utiliser pour résoudre les hôtes dans certains cas particuliers.

Pour définir un serveur DNS, vous devez fournir les informations suivantes dans chaque ligne active du fichier :

- Un spécificateur de destination principale sous forme de domaine de destination, d'hôte de destination ou d'expression régulière d'URL
- Un ensemble de directives, répertoriant un ou plusieurs serveurs DNS et leurs numéros de port

Vous pouvez également inclure les informations facultatives suivantes pour chaque spécification de serveur DNS :

- Un domaine par défaut pour la résolution des hôtes
- Une liste de recherches déterminant l'ordre des recherches lorsque plusieurs domaines sont spécifiés

Pour plus d'informations, consultez la section *Utilisation de l'option de division DNS*, page 175.

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (/opt/WCG/bin) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

Format

Chaque ligne du fichier **splitdns.config** utilise l'un des formats suivants :

```
dest_domain=domaine_dest | hôte_dest | url_regex
named=serveur_dns
def_domain=domaine_def search_list=liste_recherches
```

Chaque champ est décrit dans le tableau suivant.

Champ	Valeur autorisée
dest_domain	Nom de domaine valide. Cette valeur indique que la sélection du serveur DNS est basée sur le domaine de destination. Vous pouvez ajouter un point d'exclamation (`!`) devant le domaine pour indiquer l'opérateur logique NOT.
dest_host	Nom d'hôte valide. Cette valeur indique que la sélection du serveur DNS est basée sur l'hôte de destination. Vous pouvez ajouter un point d'exclamation (`!`) devant l'hôte pour indiquer l'opérateur logique NOT.
url_regex	Expression régulière d'URL valide. Cette valeur indique que la sélection du serveur DNS est basée sur une expression régulière.
dns_server	Directive requise. Elle identifie le serveur DNS que Content Gateway doit utiliser avec le spécificateur de destination. Vous pouvez spécifier un port en utilisant le caractère deux points (`:`). Si vous ne spécifiez pas de port, le port 53 est utilisé. Vous pouvez spécifier plusieurs serveurs DNS séparés par des espaces ou des point-virgules (`;`). Vous devez spécifier les domaines qui utilisent des adresses IP dans une notation par points.

Champ	Valeur autorisée
def_domain	Nom de domaine valide. Cette directive facultative définit le nom de domaine par défaut à utiliser pour la résolution des hôtes. Une seule entrée est autorisée. Si vous ne fournissez pas de domaine par défaut, le système détermine sa valeur via le fichier **/etc/resolv.conf**.
liste_recherches	Liste des domaines séparés par des espaces ou des points virgules (;). Définit l'ordre de recherche des domaines. Si vous ne fournissez pas de liste de recherches, le système détermine sa valeur via le fichier **/etc/resolv.conf**.

Exemples

Examinez les spécifications de sélection de serveurs DNS suivantes :

```
dest_domain=internal.company.com named=255.255.255.255:212
255.255.255.254 def_domain=company.com
search_list=company.com company1.com
dest_domain=!internal.company.com named=255.255.255.253
```

Examinons maintenant les deux requêtes suivantes :

- `http://minstar.internal.company.com`

  Cette requête correspond à la première ligne et sélectionne le serveur DNS 255.255.255.255 sur le port 212. Toutes les requêtes du résolveur utiliseront le domaine par défaut **company.com** et **company.com** et **company1.com** comme ensemble de domaines dans lesquels la recherche doit d'abord s'effectuer.
- `http://www.microsoft.com`

  Cette requête correspondra à la seconde ligne. Par conséquent, Content Gateway sélectionne le serveur DNS 255.255.255.253. Aucun **domaine_def** ou **liste_recherches** n'ayant été fourni, Content Gateway récupère ces informations dans le fichier **/etc/resolv.conf**.

Fichier de configuration storage.config

Le fichier **storage.config** présente la liste de tous les fichiers, répertoires ou partitions de disque dur qui composent le cache.

Important

Après avoir modifié ce fichier, vous devez redémarrer le proxy.

Format

Le format du fichier **storage.config** est le suivant :

```
nomchemin taille
```

où *nomchemin* correspond au nom d'une partition, d'un répertoire ou d'un fichier et *taille* à la taille de la partition, du répertoire ou du fichier nommé(e), en octets. Vous devez spécifier une taille pour les répertoires et les fichiers. Pour les partitions brutes, la taille est facultative.

Vous pouvez utiliser n'importe quelle partition, de n'importe quelle taille. Pour des performances optimales, il est recommandé de respecter les directives suivantes :

- Utilisez des partitions de disque brut.
- Pour chaque disque, utilisez des partitions de même taille.
- Pour chaque nœud, utilisez le même nombre de partitions sur tous les disques.

Définissez les noms de chemin conformément aux exigences de votre système d'exploitation. Reportez-vous aux exemples suivants.

Important

Dans le fichier **storage.config**, tout disque brut ou formaté doit avoir une capacité minimale de 2 Go. La taille recommandée pour le cache disque est de 147 Go.

Fichier de configuration update.config

Le fichier **update.config** contrôle le mode de mise à jour du contenu d'un cache local spécifique par Websense Content Gateway. Le fichier contient la liste des URL définissant les objets dont vous souhaitez planifier la mise à jour.

Une mise à jour planifiée effectue une opération HTTP `GET` locale sur les objets à l'heure ou à l'intervalle spécifique. Pour chaque objet spécifié, vous pouvez contrôler les paramètres suivants :

- L'URL
- Les en-têtes de requête spécifiques à l'URL, qui remplacent les valeurs par défaut
- L'heure et l'intervalle de mise à jour

- La profondeur de récursion

Important

Après avoir modifié ce fichier, vous devez exécuter la commande `content_line -x` dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin**) pour appliquer vos modifications. Lorsque vous appliquez les modifications à un nœud d'un cluster, Content Gateway applique les modifications à tous les nœuds de ce cluster.

La mise à jour planifiée prend en charge les paires balise/attribut suivantes lors de l'exécution des mises à jour d'URL récursives :

- <a href=“ ”>
- <img src=“ ”>
- <img href=“ ”>
- <body background=“ ”>
- <frame src=“ ”>
- <iframe src=“ ”>
- <fig src=“ ”>
- <overlay src=“ ”>
- <applet code=“ ”>
- <script src=“ ”>
- <embed src=“ ”>
- <bgsound src=“ ”>
- <area href=“ ”>
- <base href=“ ”>
- <meta content=“ ”>

La mise à jour planifiée est conçue pour fonctionner sur des jeux d'URL composés de centaines d'URL saisies (s'étendant à des milliers lorsque les URL récursives sont incluses). Elle n'est *pas* conçue pour fonctionner sur des jeux d'URL réellement volumineux, tels que ceux qu'utilisent les aspirateurs Internet.

Format

Le format de chaque ligne du fichier `update.config` doit être le suivant :

*URL**en-têtes_requête**heure_décalage**intervalle**profondeur_récursion*\

Chaque champ est décrit dans le tableau suivant.

Champ	Entrées autorisées
URL	Les URL de type HTTP et FTP
en-têtes_requête	(*Facultatif*) Liste des en-têtes (séparés par des points-virgules) transmis dans chaque requête `GET`. Vous pouvez définir tout en-tête de requête respectant les spécifications du protocole HTTP. Le paramètre par défaut consiste à ne pas utiliser d'en-tête de requête.
heure_décalage	Heure de base à partir de laquelle découlent les périodes de mise à jour. La plage est 00-23 heures.
intervalle	Intervalle, en secondes, selon lequel les mises à jour doivent être effectuées, à partir de l'heure de décalage
profondeur_récursion	Profondeur à laquelle les URL référencées sont mises à jour de façon récursive, à partir de l'URL donnée

Exemples

L'exemple suivant présente une mise à jour planifiée HTTP :

```
http://www.entreprise.com\User-Agent: noname user
agent\13\3600\5\
```

Cet exemple définit l'URL et les en-têtes de requête, l'heure de décalage 13 (13h00), un intervalle d'une heure et une profondeur de récursion de 5. Les mises à jour auront donc lieu à 13:00, 14:00, 15:00, etc. Pour planifier une mise à jour devant être effectuée une fois par jour uniquement, utilisez une valeur d'intervalle de 24 heures x 60 minutes x 60 secondes = 86400.

L'exemple suivant présente une mise à jour planifiée FTP :

```
ftp://anonymous@ftp.entreprise.com/pub/misc/
test_file.cc\\18\120\0\
```

Cet exemple définit la requête FTP, l'heure de décalage 18 (18h00) et un intervalle de deux minutes. L'utilisateur doit être *anonyme* et le mot de passe doit être spécifié par la variable *proxy.config.http.ftp.anonymous_passwd* dans le fichier **records.config**.

Fichier de configuration wccp.config

Le fichier **wccp.config** stocke les informations de la configuration WCCP et les paramètres des groupes de services. Lorsque WCCP est activé dans la page **Configurer > Mon proxy > De base**, les paramètres de groupe de services WCCP peuvent être configurés dans la page **Configurer > Networking (Mise en réseau) > WCCP**. Les groupes de services doivent être définis lorsque WCCP doit être utilisé pour la redirection transparente vers Content Gateway. Pour plus d'informations, consultez la section *Interception transparente avec dispositifs WCCP v2*, page 50.

F Messages d’erreur

Messages d’erreur de Websense Content Gateway

Le tableau suivant dresse la liste des messages qui apparaissent dans les fichiers journaux du système. Cette liste n’est pas exhaustive ; elle décrit les messages d’avertissement susceptibles de réclamer votre attention. Pour des informations sur les messages d’avertissement non présents dans cette liste, visitez www.websense.com et accédez à la Base de connaissances et au portail de Support.

Erreurs fatales pour le traitement

Message	Description
Accept port is not between 1 and 65535. Please check configuration. (Le port accepté n’est pas compris entre 1 et 65535. Veuillez vérifier votre configuration.)	Le port spécifié dans le fichier records.config pour accepter les requêtes HTTP entrantes n’est pas valide.
Ftp accept port is not between 1 and 65535. (Le port FTP accepté n’est pas compris entre 1 et 65535.)	Le port spécifié dans le fichier records.config pour accepter les requêtes FTP entrantes n’est pas valide.
Self loop is detected in parent proxy configuration. (Une boucle fermée a été détectée dans la configuration du proxy parent.)	Le nom et le port du proxy parent sont les mêmes que ceux de Content Gateway. Ceci crée une boucle lorsque Content Gateway tente d’envoyer les requêtes au proxy parent.
Could not open the ARM device (Impossible d’ouvrir le périphérique ARM)	Le module ARM ne parvient pas à se charger. La plupart du temps, il s’agit du noyau du système hôte qui n’est pas compatible. Pour savoir si le module ARM est chargé, exécutez la commande suivante : /sbin/lsmod | grep arm
content_manager failed to set cluster IP address (Le processus content_manager n’a pas réussi à définir l’adresse IP du cluster.)	Le processus content_manager n’a pas réussi à définir l’adresse IP du cluster. Vérifiez l’adresse IP du cluster. Assurez-vous qu’elle ne soit pas déjà utilisée par un autre périphérique du réseau.
Unable to initialize storage. (Impossible d’initialiser le stockage.) (Re)Configuration required. (Nouvelle configuration requise.)	L’initialisation du cache a échoué au démarrage. Vous devez vérifier et configurer ou reconfigurer le cache.

Avertissements

Message	Description
Erreur du *fichier journal* : *numéro_erreur*	Erreur de journalisation générique
Bad cluster major version range *version1-version2* for node *IP address* connect failed	Versions logicielles non compatible provoquant un problème
can't open config file *filename* for reading custom formats	La journalisation personnalisée est activée, mais Content Gateway ne parvient pas à localiser le fichier **logs.config**.
connect by disallowed client *IP address*, closing connection	Le client spécifié n'est pas autorisé à se connecter à Content Gateway. Son adresse IP ne figure pas dans le fichier **ip_allow.config**.
Could not rename log *filename* to *rolled filename*	Erreur système lors du changement de nom du fichier journal pendant le déploiement
Did *this_amount* of backup still to do *remaining_amount*	Le système va bientôt être surchargé.
Different clustering minor versions *version 1, version 2* for node *IP address* continuing	Versions logicielles non compatible provoquant un problème
log format symbol *symbol_name* not found	Le format de journalisation personnalisée fait référence à un symbole de champ qui n'existe pas. Voir *Formats de journalisation des événements*, page 337.
missing field for field marker	Erreur de lecture dans le tampon du journal
Unable to accept cluster connections on port: *cluster_port_number*	Contactez le support technique de Websense. Pour obtenir les coordonnées du support technique, accédez à la page www.websense.com/support/.
Unable to open log file *filename*, errno=*error_number*	Impossible d'ouvrir le fichier journal
Error accessing disk *disk_name*	Content Gateway peut avoir un problème de lecture du cache. Le disque doit éventuellement être remplacé.
Too many errors accessing disk *disk_name:* declaring disk bad	Content Gateway n'utilise pas le cache disque car il a rencontré trop d'erreurs. Le disque est éventuellement endommagé et doit être remplacé.
No cache disks specified in **storage.config** file: cache disabled	Le fichier **storage.config** de Content Gateway ne contient pas de liste de disques cache. Content Gateway s'exécute en mode proxy uniquement. Vous devez ajouter les disques à utiliser pour le cache dans le fichier **storage.config** (voir *Fichier de configuration storage.config*, page 447).
All disks are bad, cache disabled	Le ou les disques cache ont un problème et la mise en cache a été désactivée. Veuillez vérifier le fonctionnement de ces disques et que leur formatage convient à la mise en cache. Voir *Configuration du cache*, page 87.

Message	Description
Missing DC parameter <missing_param> on auth.profile line	Un paramètre obligatoire a été omis. Veuillez fournir une valeur pour ce paramètre manquant.
Bad DC parameter <bad_param> - <dc_name>	Un paramètre du contrôleur de domaine spécifié n’est pas valide. Veuillez fournir une valeur valide pour ce paramètre.
[ParentSelection] <error_description> for default parent proxy	Le chaînage des proxy ne fonctionne pas du fait d’une configuration incorrecte du proxy parent dans le proxy enfant. Veuillez vérifier la configuration du chaînage des valeurs de proxy parent dans le proxy enfant.
WCCP2: Cannot find Interface name. Please check that the variable proxy.local.wccp2. ethernet_interface is set correctly	Aucune valeur n’est spécifiée pour l’interface WCCP. Dans Content Gateway Manager, vérifiez **Configurer > Networking (Mise en réseau) > WCCP > Général**. Ou affectez une valeur à proxy.local.wccp2.ethernet_interface dans le fichier **records.config**.
ARMManager: Unable to read network interface configuration	Une erreur de format ou de configuration est présente dans le fichier **ipnat.conf**. Dans Content Gateway Manager, accédez à **Configurer > Networking (Mise en réseau) > ARM > Général** et cliquez sur **Edit File (Modifier le fichier)** pour afficher et corriger le fichier **ipnat.conf**.

Messages d’alarme

Le tableau suivant décrit les messages d’alarme susceptibles de s’afficher dans Content Gateway Manager.

Message	Description/Solution
The Content Gateway subscription has expired. (L’abonnement à Content Gateway est arrivé à expiration.)	Veuillez contacter votre représentant Websense ou le Support technique pour obtenir de l’aide.
Content Gateway subscription download failed. (Le téléchargement de l’abonnement Content Gateway a échoué.)	Content Gateway n’a pas pu se connecter au serveur de téléchargement pour vérifier les informations de votre abonnement. Veuillez vérifier votre connexion au serveur de téléchargement.
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. (Après plusieurs tentatives, Content Gateway n’a pas réussi à se connecter au service Websense Database Download Service.) Please troubleshoot the connection. (Veuillez réparer votre connexion.)	Vérifiez que Content Gateway a accès à Internet. Vérifiez les paramètres de votre serveur proxy en amont et de votre pare-feu qui sont susceptibles d’empêcher Content Gateway de se connecter au serveur de téléchargement.

Message	Description/Solution
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. (Après plusieurs tentatives, Content Gateway n'a pas réussi à se connecter à Policy Server.) Please troubleshoot the connection. (Veuillez réparer votre connexion.)	Vérifiez la présence d'une connectivité réseau entre Content Gateway et Web Security. Parfois, les paramètres du pare-feu bloquent la connectivité. Vérifiez également que le service Policy Server s'exécute dans l'hôte de Web Security.
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. (Après plusieurs tentatives, Content Gateway n'a pas réussi à se connecter à Policy Broker.) Please troubleshoot the connection. (Veuillez réparer votre connexion.)	Vérifiez la présence d'une connectivité réseau entre Content Gateway et Web Security. Parfois, les paramètres du pare-feu bloquent la connectivité. Vérifiez également que le service Policy Broker s'exécute dans l'hôte de Web Security.
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. (Après plusieurs tentatives, Content Gateway n'a pas réussi à se connecter au service Filter.) Please troubleshoot the connection. (Veuillez réparer votre connexion.)	Vérifiez la présence d'une connectivité réseau entre Content Gateway et Web Security. Parfois, les paramètres du pare-feu bloquent la connectivité. Vérifiez également que le service Filter s'exécute dans l'hôte de Web Security.
Communication with the analytics engine has failed. (Échec de la communication avec le moteur d'analyse.) Please restart Content Gateway. (Veuillez redémarrer Content Gateway.)	Redémarrez Content Gateway.
SSL decryption has been disabled due to an internal error, please restart Content Gateway. (Le décryptage SSL a été désactivé à cause d'une erreur interne. Veuillez redémarrer Content Gateway.)	Il y a eu une erreur fatale dans le module SSL Manager. Veuillez redémarrer Content Gateway.
[Rollback::Rollback] Config file is read-only: *filename*	Accédez au répertoire **config** de Content Gateway (l'emplacement par défaut est **/opt/WCG/config**) et vérifiez les autorisations indiquées pour ce fichier. Modifiez-les si nécessaire.
[Rollback::Rollback] Unable to read or write config file *filename*	Accédez au répertoire **config** de Content Gateway et vérifiez la présence du fichier indiqué. Vérifiez ses autorisations et modifiez-les si nécessaire.
[Content Gateway Manager] Configuration File Update Failed *error_number*	Accédez au répertoire **config** de Content Gateway et vérifiez les autorisations du fichier indiqué. Modifiez-les si nécessaire.
Access logging suspended - configured space allocation exhausted.	L'espace alloué aux journaux d'événements est saturé. Vous devez soit augmenter cet espace, soit supprimer certains fichiers journaux pour que la journalisation des accès se poursuive. Pour éviter cette erreur à l'avenir, envisagez une rotation plus fréquente des fichiers journaux et activez la fonction de suppression automatique. Voir *Rotation des fichiers journaux d'événements*, page 221.

Message	Description/Solution
Access logging suspended - no more space on the logging partition.	Toute la partition qui contient les journaux d'événements est saturée. Pour que la journalisation des accès se poursuive, vous devez supprimer ou déplacer certains fichiers journaux. Pour éviter cette erreur à l'avenir, envisagez une rotation plus fréquente des fichiers journaux et activez la fonction de suppression automatique. Voir *Rotation des fichiers journaux d'événements*, page 221.
Created zero length place holder for config file *filename*	Accédez au répertoire **config** de Content Gateway et vérifiez le fichier indiqué. Si le fichier est bien vide, utilisez une copie de sauvegarde de ce fichier de configuration.
Content Gateway can't open *filename* for reading custom formats	Assurez-vous que la variable *proxy.config.log2.config_file*, présente dans le fichier **records.config**, contient bien le chemin correct vers le fichier de configuration de la journalisation personnalisée (**logging/logs.config** par défaut).
Content Gateway could not open logfile *filename*	Vérifiez les autorisations du fichier indiqué et du répertoire de la journalisation.
Content Gateway failed to parse line *line_number* of the logging config file *filename*	Vérifiez le fichier de configuration de votre journalisation personnalisée. Il peut y avoir des erreurs de syntaxe. Pour connaître les champs corrects du format de la journalisation personnalisée, consultez la section *Champs de journalisation personnalisés*, page 337.
vip_config binary is not setuid root, manager will be unable to enable virtual ip addresses	Le processus **content_manager** ne parvient pas à définir les adresses IP virtuelles. Vous devez définir un ID racine pour le fichier **vip_config** dans le répertoire **bin** de Content Gateway.
Content Gateway cannot parse the ICAP URI. Please ensure that the URI is entered correctly in Content Gateway Manager or in the *proxy.config.icap.ICAPUri* configuration variable.	L'URI (Universal Resource Identifier) n'est pas dans un format correct. Entrez l'URI comme suit : `icap://nomhôte:port/chemin` Pour plus de détails sur le format des URI, consultez la section *Utilisation de Websense Data Security*, page 119.
The specified ICAP server does not have a DNS entry. Please ensure that a valid DSS hostname is entered correctly in Content Gateway Manager or in the *proxy.config.icap.ICAPUri* configuration variable.	Dans le fichier **records.config**, le nom d'hôte ne correspond à aucune entrée du système DNS. Assurez-vous que le nom d'un serveur Websense Data Security Suite valide soit saisi correctement dans Content Gateway Manager. Pour plus de détails sur le format des URI, consultez la section *Utilisation de Websense Data Security*, page 119.
Content Gateway is not able to communicate with the DSS server. Please try again.	Vérifiez que le serveur Websense Data Security Suite est bien en état de fonctionnement, et qu'il accepte les connexions sur le port spécifié dans la variable *proxy.config.icap.ICAPUri*. Si ce message persiste, contactez votre administrateur Websense Data Security Suite.
Domain controller *domain_controller_name:port* is down.	Le contrôleur de domaine NTLM nommé ne répond plus aux requêtes et est marqué hors service. Examinez son statut.

Messages HTML envoyés aux clients

En cas de problème avec les transactions HTTP demandées par le navigateur, Websense Content Gateway renvoie des messages d'erreur détaillés aux navigateurs des clients. Ces messages de réponse correspondent aux codes de réponses HTTP standard, mais avec plus d'informations. Vous trouverez une liste des codes de réponses HTTP les plus fréquents à la section *Messages de réponse HTTP standard*, page 461. Vous pouvez personnaliser les messages de réponse.

Le tableau suivant énumère la liste des messages HTTP codés en dur dans Content Gateway, leurs codes de réponse HTTP correspondants et leurs fichiers personnalisables correspondants.

Titre	Code HTTP	Description	Nom de fichier personnalisable
Accès refusé	403	Vous n'êtes pas autorisé à accéder au document de cette *URL*.	access#denied
Requête HTTP incorrecte pour un objet FTP	400	Requête HTTP incorrecte pour un objet FTP	ftp#bad_request
Erreur de lecture du cache	500	Erreur de lecture à partir du cache. Relancez votre requête.	cache#read_error
Expiration de la connexion	504	Le serveur n'a envoyé aucune donnée depuis trop longtemps.	timeout#inactivity
Longueur du contenu requise	400	Impossible de traiter cette requête, car la valeur Content-Length n'a pas été spécifiée.	request#no_content_length
Cycle détecté	400	Votre requête est interdite, car elle provoquerait un cycle de proxy HTTP.	request#cycle_detected
Interdit	403	*numéro_port* n'est pas un port autorisé pour les connexions SSL. (Vous avez demandé une connexion SSL sécurisée sur un numéro de port interdit.)	access#ssl_forbidden
Authentification FTP requise	401	Vous devez spécifier un nom d'utilisateur et un mot de passe corrects pour accéder à l'*URL* du document FTP demandé.	ftp#auth_required
Échec de la connexion FTP	502	Impossible de se connecter au serveur *nom_serveur*	connect#failed_connect
Erreur FTP	502	Le serveur FTP *nom_serveur* a renvoyé une erreur. La requête pour l'*URL* du document a échoué.	ftp#error

Titre	Code HTTP	Description	Nom de fichier personnalisable
En-tête de l'hôte requis	400	Une tentative d'envoi de votre requête par proxy transparent a eu lieu, mais elle a échoué car votre navigateur n'a pas envoyé d'en-tête HTTP pour l'hôte `Host`. Configurez votre navigateur manuellement de sorte qu'il utilise `https://` *nom_proxy:port_proxy* en tant que proxy HTTP. Pour plus d'informations, consultez la documentation de votre navigateur. Les utilisateurs peuvent également passer à un navigateur plus récent qui prend en charge le champ d'en-tête `Host` HTTP.	interception#no_host
En-tête de l'hôte requis	400	Votre navigateur n'a pas envoyé de champ d'en-tête `Host` HTTP et cela a empêché d'identifier l'hôte virtuel qui doit satisfaire la requête. Pour accéder correctement à ce site Web, vous devez passer à un navigateur plus récent qui prend en charge le champ d'en-tête `Host` HTTP.	request#no_host
Version HTTP non prise en charge	505	Le serveur d'origine *`nom_serveur`* utilise une version non prise en charge du protocole HTTP.	response#bad_version
Requête HTTP non valide	400	Impossible de traiter cette requête de méthode HTTP *`requête_client`* pour l'*`URL`*.	request#syntax_error
Réponse HTTP non valide	502	L'hôte *`nom_serveur`* n'a pas renvoyé correctement l'*`URL`* du document.	response#bad_response
Réponse du serveur erronée	502	L'hôte *`nom_serveur`* n'a pas renvoyé correctement l'*`URL`* du document.	response#bad_response
Statut erroné de la réponse du serveur	502	L'hôte *`nom_serveur`* n'a pas renvoyé correctement l'*`URL`* du document.	response#bad_response
Expiration du délai de transaction	504	Trop de temps s'est écoulé pour la transmission de l'*`URL`* du document.	timeout#activity

Titre	Code HTTP	Description	Nom de fichier personnalisable
Aucune en-tête de réponse reçu du serveur	502	L'hôte *nom_serveur* n'a pas renvoyé correctement l'*URL* du document.	response#bad_response
Non mis en cache	504	Ce document n'était pas disponible dans le cache, et vous (le client) n'acceptez que les copies mises en cache.	cache#not_in_cache
Non détecté dans l'Accélérateur	404	La requête de l'*URL* dans l'hôte *nom_serveur* n'a pas été détectée. Vérifiez l'emplacement et recommencez.	urlrouting#no_mapping
NULL	502	L'hôte *nom_serveur* n'a pas renvoyé correctement l'*URL* du document.	response#bad_response
Authentification du proxy requise	407	Veuillez vous connecter avec un nom d'utilisateur et un mot de passe.	access#proxy_auth_required
Raccrochage du serveur	502	Le serveur *nom_hôte* a fermé la connexion avant la fin de la transaction.	connect#hangup
Déplacement temporaire	302	Le document que vous avez demandé, *URL*, a été déplacé. Le nouvel emplacement est *nouvelle_URL*.	redirect#moved_temporarily
Transcodage non disponible	406	Impossible de fournir l'*URL* du document au format demandé par votre navigateur.	transcoding#unsupported
Échec de la connexion en tunnel	502	Impossible de se connecter au serveur *nom_hôte*	connect#failed_connect
Erreur inconnue	502	L'hôte *nom_serveur* n'a pas renvoyé correctement l'*URL* du document.	response#bad_response
Hôte inconnu	500	Impossible de localiser le serveur nommé *nom_hôte*. Ce serveur n'a pas d'entrée DNS. Son nom est peut-être mal orthographié ou il n'existe plus. Revérifiez le nom et recommencez.	connect#dns_failed
Schéma d'URL non pris en charge	400	Impossible de satisfaire votre requête pour l'*URL* du document, car le schéma du protocole est inconnu.	request#scheme_unsupported

Messages de réponse HTTP standard

Les messages de réponse HTTP standard suivants sont fournis à titre indicatif. Pour une liste plus exhaustive, consultez la spécification *Hypertext Transfer Protocol — HTTP/1.1 Specification*.

Message	Description
200	OK
202	Accepté
204	Aucun contenu
206	Contenu partiel
300	Plusieurs choix
301	Déplacé définitivement
302	Détecté
303	Voir Autre
304	Non modifié
400	Requête incorrecte
401	Non autorisé, réessayer
403	Interdit
404	Introuvable
405	Méthode non autorisée
406	Pas acceptable
408	Expiration de la requête
500	Erreur interne du serveur
501	Pas implémenté
502	Passerelle incorrecte
504	Expiration de la passerelle

G Fichier req_ca.cnf

Créez un fichier **req_ca.cnf** et copiez-y le code ci-dessous. Pour plus d'informations sur le fichier **req_ca.cnf**, consultez la section *Création d'une autorité de certification subordonnée*, page 136.

```
#
# Fichier de configuration permettant de générer une demande
d'autorité de certification (CA)
#
HOME = .
RANDFILE = $ENV::HOME/.rnd
#
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
##########################################################################
#
[ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
string_mask = nombstr
req_extensions = v3_req # Extensions à ajouter à une demande de
certificat
[ req_distinguished_name ]
countryName = Country Name (code à 2 lettres)
countryName_default = US
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (nom complet)
stateOrProvinceName_default = Some-State
localityName = Locality Name (ex, ville)
0.organizationName = Organization Name (ex, entreprise)
```

```
0.organizationName_default = Internet Widgits Pty Ltd
#organizationalUnitName = Organizational Unit Name (ex, section)
#organizationalUnitName_default =
commonName = Common Name (Nom de la sous-CA)
commonName_max = 64
emailAddress = Adresse e-mail
emailAddress_max = 64
[ v3_req ]
# Extensions à ajouter à une demande de certificat pour en faire une
autorité de certification
basicConstraints=CA:TRUE
nsCertType = sslCA
keyUsage = cRLSign, keyCertSign
```

H FAQ et conseils de dépannage

FAQ (Questions les plus fréquentes)

Pour plus d'informations, consultez la section *Conseils de dépannage*, page 471.

À partir de combien d'erreurs d'E/S du disque le cache est-il affecté et que fait Content Gateway lorsqu'un cache sur disque est défaillant ?

Si un lecteur de disque fait échouer cinq opérations d'E/S successives, Content Gateway considère ce lecteur comme inaccessible et retire la totalité de ce disque du cache. Le fonctionnement normal du cache continue dans tous les autres disques de Content Gateway.

Si un client se déconnecte pendant que Content Gateway télécharge un objet volumineux, une partie de cet objet est-elle enregistrée dans le cache ?

Lorsqu'un client se déconnecte pendant une opération HTTP ou FTP, Content Gateway continue à télécharger l'objet auprès du serveur d'origine pendant 10 secondes. Si le transfert depuis le serveur d'origine se termine avec succès pendant les 10 secondes qui suivent la déconnexion du client, Content Gateway stocke l'objet dans le cache. Si le téléchargement depuis le serveur d'origine ne se termine pas dans les 10 secondes, Content Gateway se déconnecte du serveur d'origine et supprime l'objet dans le cache. Content Gateway ne stocke pas des documents partiels dans le cache.

Content Gateway peut-il mettre en cache des applets Java, des programmes JavaScript ou d'autres fichiers d'application comme VBScript ?

Content Gateway peut stocker et fournir des applets Java, des programmes JavaScript, des scripts VBScript et d'autres objets exécutables à partir de son cache, selon les règles d'actualité et de capacité de mise en cache définies pour les objets HTTP.

Content Gateway n'exécute pas les applets, scripts ou programmes. Ces objets s'exécutent uniquement lorsque le système du client qui a envoyé la requête les charge.

Comment accéder à Content Gateway Manager si j'ai oublié le mot de passe de l'administrateur principal ?

Pendant l'installation, vous pouvez spécifier un mot de passe d'administration. Le programme d'installation crypte automatiquement ce mot de passe et le stocke dans le fichier `records.config`. À chaque modification des mots de passe dans Content Gateway Manager, Content Gateway met le fichier **records.config** à jour.

Si vous oubliez le mot de passe de l'administrateur et ne pouvez plus accéder à Content Gateway Manager, effacez le mot de passe actuel dans le fichier **records.config** (définissez la valeur de la variable de configuration sur NULL), puis entrez un nouveau mot de passe dans Content Gateway Manager. Vous ne pouvez pas définir des mots de passe dans le fichier **records.config**, car les variables des mots de passe ne peuvent contenir que des mots de passe cryptés ou la valeur NULL.

1. Ouvrez le fichier **records.config** dans **/opt/WCG/config**.
2. Définissez la variable *`proxy.config.admin.admin_password`* sur NULL pour laisser le mot de passe vierge.

   Remarque

   Assurez-vous que le mot NULL ne soit pas suivi d'espaces.

3. Enregistrez et fermez le fichier.

4. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin)**, exécutez la commande `content_line -x` pour appliquer vos modifications.
5. Connectez-vous à Content Gateway Manager. Lorsque le système vous demande un nom d'utilisateur et un mot de passe, entrez l'ID d'administrateur et laissez le champ du mot de passe vide.

   Comme vous avez déjà effacé le mot de passe dans le fichier **records.config**, vous n'avez pas besoin de mot de passe pour vous connecter en tant qu'administrateur.
6. Ouvrez l'onglet **Configurer > Mon proxy > UI Setup (Configuration de l'interface utilisateur) > Connexion**.
7. Dans la section **Administrateur**, laissez le champ de l'ancien mot de passe vide. Saisissez le nouveau mot de passe dans le champ **Nouveau mot de passe**, puis à nouveau dans le champ **New Password (Retype) (Confirmer le nouveau mot de passe)**.
8. Cliquez sur **Appliquer**.

   Lors de votre prochain accès à Content Gateway Manager, vous devrez utiliser le nouveau mot de passe.

Comment appliquer les modifications du fichier logs_xml.config à tous les nœuds d'un cluster ?

Après avoir modifié le fichier `logs_xml.config` dans un nœud Content Gateway, entrez la commande suivante à partir du répertoire **bin** de Content Gateway (**/opt/WCG/bin)** :

```
content_line -x
```

Content Gateway applique alors les modifications à tous les nœuds du cluster. Les modifications entrent immédiatement en vigueur.

Dans les fichiers journaux au format Squid ou Netscape, que signifient les codes de résultat du cache ?

Le tableau suivant décrit les codes de résultat du cache dans les fichiers journaux Squid et Netscape.

Code de résultat du cache	Description
TCP_HIT	Indique qu'une copie valide de l'objet demandé était présente dans le cache et que le proxy a envoyé cet objet au client
TCP_MISS	Indique que l'objet demandé n'était pas présent dans le cache et que le proxy l'a récupéré auprès du serveur d'origine ou d'un proxy parent et l'a envoyé au client
TCP_REFRESH_HIT	Indique que l'objet était dans le cache, mais était périmé. Content Gateway a envoyé une requête `if-modified-since` au serveur d'origine, et ce dernier a renvoyé une réponse `304 not-modified`. Le proxy a envoyé l'objet mis en cache au client.

Code de résultat du cache	Description
TCP_REF_FAIL_HIT	Indique que l'objet était dans le cache, mais était périmé. Content Gateway a envoyé une requête `if-modified-since` au serveur d'origine, mais celui-ci n'a pas répondu. Le proxy a envoyé l'objet mis en cache au client.
TCP_REFRESH_MISS	Indique que l'objet était dans le cache, mais était périmé. Content Gateway a envoyé une requête `if-modified-since` au serveur d'origine, et celui-ci a renvoyé un nouvel objet. Le proxy a envoyé ce nouvel objet au client.
TCP_CLIENT_REFRESH	Indique que le client a envoyé une requête avec un en-tête `no-cache`. Le proxy a obtenu l'objet demandé auprès du serveur d'origine, puis en a envoyé une copie au client. Content Gateway a supprimé toute précédente copie de cet objet dans le cache.
TCP_IMS_HIT	Indique que le client a envoyé une requête `if-modified-since` et que l'objet demandé était dans le cache et plus récent que la date IMS, ou une requête `if-modified-since` envoyée au serveur d'origine a permis de déterminer que l'objet présent dans le cache était récent. Le proxy a envoyé l'objet mis en cache au client.
TCP_IMS_MISS	Indique que le client a envoyé une requête `if-modified-since` et que l'objet demandé était absent dans le cache ou était périmé. Le proxy a envoyé une requête `if-modified-since` au serveur d'origine et a reçu le nouvel objet. Le proxy a envoyé l'objet mis à jour au client.
TCP_SWAPFAIL	Indique que l'objet demandé était dans le cache, mais était inaccessible. Le client n'a pas reçu l'objet.
ERR_CLIENT_ABORT	Indique que le client s'est déconnecté avant la fin de l'envoi de l'objet
ERR_CONNECT_FAIL	Indique que Content Gateway n'a pas pu contacter le serveur d'origine
ERR_DNS_FAIL	Indique que le serveur DNS n'a pas pu résoudre le nom du serveur d'origine, ou que le système DNS était inaccessible
ERR_INVALID_REQ	Indique que la requête HTTP du client n'était pas valide. Content Gateway transmet les requêtes dont les méthodes ne sont pas reconnues au serveur d'origine.
ERR_READ_TIMEOUT	Indique que le serveur d'origine n'a pas répondu à la requête de Content Gateway dans l'intervalle d'expiration
ERR_PROXY_DENIED	Indique que le service a été refusé au client par la configuration du contrôle d'accès
ERR_UNKNOWN	Indique que le client s'est connecté, puis déconnecté, sans envoyer de requête

Qu'enregistre le champ cqtx dans un fichier journal personnalisé ?

Le champ `cqtx` enregistre le texte complet des requêtes des clients (sans les en-têtes) dans le fichier journal. Par exemple, `get http://www.entreprise.com HTTP/1.0`.

Content Gateway rafraîchit-il les entrées de sa base de données des hôtes après une certaine période sans utilisation ?

Par défaut, la base de données des hôtes de Content Gateway respecte les valeurs TTL (time-to-live, durée de vie) définies par les serveurs de noms. Vous pouvez reconfigurer Content Gateway avec une autre valeur.

1. Ouvrez le fichier **records.config** situé dans **/opt/WCG/config**.
2. Modifiez la variable suivante :

Variable	Description
`proxy.config.hostdb.ttl_mode`	Définissez cette valeur sur : **0** - pour respecter les valeurs TTL définies par les serveurs de noms **1** - pour ignorer les valeurs TTL définies par les serveurs de noms et utiliser la valeur définie par la variable de configuration de Content Gateway **proxy.config.hostdb.timeout**. Définissez cette variable sur la valeur qui convient à votre environnement. **2** - pour utiliser la plus petite des deux valeurs (celle définie par le serveur de noms ou celle définie par Content Gateway) **3** - pour utiliser la plus grande des deux valeurs (celle définie par le serveur de noms ou celle définie par Content Gateway)

3. Enregistrez et fermez le fichier.
4. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin)**, exécutez la commande `content_line -x` pour appliquer vos modifications.

Peut-on améliorer l'apparence des pages de réponse personnalisées à l'aide d'images, de gifs animés et d'applets Java ?

Content Gateway ne peut répondre aux clients qu'avec du texte ou un document HTML. Toutefois, dans vos pages de réponse personnalisées, vous pouvez fournir des références à des images, des gifs animés, des applets Java ou des objets autres que du texte. Ces objets référencés doivent être disponibles dans un serveur Web.

Ajoutez des liens dans les fichiers **body_factory** modèles comme vous le feriez pour toute image dans un document HTML, avec l'URL complète fournie dans l'attribut SRC.

Il est recommandé de ne pas exécuter le serveur Web et Content Gateway dans le même système, afin d'éviter aux deux programmes de tenter d'envoyer les documents sur le même numéro de port.

Comment configurer Content Gateway pour qu'il ne desserve que les requêtes transparentes ?

Vous pouvez configurer Content Gateway pour desservir *uniquement* les requêtes transparentes et l'empêcher de desservir les requêtes de proxy explicite de la manière suivante :

- Vous pouvez contrôler l'accès des clients à Content Gateway à partir du fichier **ip_allow.config** en spécifiant des plages d'adresses IP autorisées à utiliser le proxy. Si Content Gateway reçoit une requête provenant d'une adresse IP non énumérée dans la plage spécifiée dans ce fichier, il ne la traite pas. Voir *Fichier de configuration ip_allow.config*, page 360.
- Si vous ne connaissez pas les plages d'adresses IP autorisées à accéder à Content Gateway, vous pouvez ajouter des règles au fichier **ipnat.conf** afin que seules les requêtes redirigées par votre commutateur de niveau 4 ou votre routeur WCCP puissent contacter le port du proxy. Pour faire de Content Gateway un serveur uniquement transparent, ajoutez des règles au fichier **ipnat.conf** avant que la règle de redirection normale ne redirige le trafic du proxy explicite vers un port sur lequel aucun service n'est à l'écoute. Par exemple, si vous souhaitez que Content Gateway ignore les requêtes HTTP explicites, ajoutez des règles au-dessus de la règle de redirection HTTP normale dans le fichier **ipnat.conf** comme illustré ci-dessous (où *adresseip* correspond à l'adresse IP de votre système Content Gateway et *numéro_port* est un port sur lequel aucun service n'est à l'écoute) :

  rdr hme0 *adresseip* port 80 -> *adresseip* port *numéro_port* tcp

  rdr hme0 *adresseip* port 8080 -> *adresseip* port *numéro_port* tcp

  rdr hme0 0.0.0.0/0 port 80 -> *adresseip* port 8080 tcp

  Ajoutez des règles équivalentes au fichier **ipnat.conf** pour chaque port de service de protocole ou séparez l'interface réseau à desservir. Après avoir modifié le fichier **ipnat.conf**, vous devez redémarrer le proxy.
- Si votre système Content Gateway dispose de plusieurs interfaces réseau ou si vous configurez le système d'exploitation de Content Gateway pour qu'il utilise des adresses IP virtuelles, vous pouvez attribuer deux adresses IP à Content Gateway. Une de ces adresses doit être l'adresse *réelle* que le proxy utilise pour communiquer avec les serveurs d'origine, et l'autre doit être une adresse IP privée (par exemple 10.0.0.1) pour la redirection des commutateurs ou WCCP. Après avoir configuré l'adresse IP, vous devez ajouter les variables suivantes à la fin du fichier **records.config**. Remplacez *adresseip_privée* par l'adresse IP privée utilisée pour WCCP ou la redirection des commutateurs, et *adresseip_réelle* par l'adresse IP réelle utilisée par le proxy pour communiquer avec les serveurs d'origine.

  ```
  LOCAL proxy.local.incoming_ip_to_bind STRING
  adresseip_privée
  LOCAL proxy.local.incoming_ip_to_bind STRING
  adresseip_réelle
  ```

Conseils de dépannage

La statistique du débit est imprécise dans Content Gateway Manager.

Content Gateway met à jour la statistique du débit après chaque transfert d'un objet complet. Pour les fichiers plus volumineux, le nombre d'octets augmente brusquement à la fin de leur transfert. Le nombre final d'octets transférés est attribué lors du dernier intervalle de 10-secondes, bien que le transfert de l'objet puisse durer plusieurs minutes.

Cette imprécision est encore plus notable lorsque la charge est légère. Des charges plus lourdes améliorent la précision de cette statistique.

Impossible d'exécuter les commandes Content Gateway

Les commandes ne s'exécutent pas dans les cas suivants :

- Si le processus `content_manager` n'est pas en cours d'exécution.

  Pour vérifier que le processus `content_manager` fonctionne, entrez la commande suivante :

  ```
  ps aux | grep content_manager
  ```

  ou

```
./WCGAdmin status
```

Si le processus `content_manager` ne fonctionne pas, entrez la commande suivante dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin)** pour le démarrer :

```
./content_manager
```

Important

Si vous devez arrêter Content Gateway, il est conseillé de le redémarrer à l'aide de la commande **./WCGAdmin**. Arrêtez-le avec la commande **./WCGAdmin stop** et redémarrez-le avec la commande **./WCGAdmin start** afin de vous assurer que tous les processus s'arrêtent et démarrent correctement. Voir *Mise en route*, page 11.

- Si vous n'exécutez pas la commande depuis le répertoire **$WCGHome/bin**.

  Si le répertoire **bin** de Content Gateway n'est pas dans votre chemin, ajoutez `./` devant les commandes (par exemple, `./content_line -h`).
- Si plusieurs installations de Content Gateway sont présentes et que vous n'exécutez pas les commandes depuis le chemin actif spécifié dans **/etc/content_gateway**.

  Passez toujours au répertoire approprié à l'aide de la commande :

  ```
  cd `cat /etc/content_gateway`/bin
  ```

Vous observez un comportement incohérent lorsqu'un nœud obtient un objet d'un autre nœud du cluster.

Dans le cadre du processus de préparation du système, vous devez synchroniser les horloges de tous les nœuds de votre cluster. Des écarts temporels mineurs provoquent des problèmes, mais des différences de plusieurs minutes peuvent altérer le fonctionnement de Content Gateway.

Il est recommandé d'exécuter un démon de synchronisation des horloges tel que `xntpd`. Pour obtenir la dernière version du démon `xntpd`, visitez l'URL suivante :

http://www.ntp.org

Les navigateurs Web peuvent afficher une erreur de document avec un message de données manquantes.

Un message similaire à ce qui suit s'affiche dans les navigateurs Web :

```
Data Missing (Données manquantes)
This document resulted from a POST operation and has
expired from the cache. (Ce document est le résultat
d'une opération POST et a expiré dans le cache.) If you
wish you can repost the form data to re-create the
document by pressing the reload button. (Si vous le
souhaitez, vous pouvez republier les données du
formulaire pour recréer le document en appuyant sur
le bouton de rechargement.)
```

Les navigateurs Web conservent leur cache local en mémoire et/ou sur disque dans le système du client. Les navigateurs qui envoient des messages sur les documents expirés dans le cache consultent leur cache local, *pas* le cache de Content Gateway. Aucune condition de Content Gateway ne peut provoquer l'apparition de tels messages dans un navigateur Web.

Pour des informations sur les options et les effets du cache du navigateur, consultez la documentation de votre navigateur.

Content Gateway ne résout aucun site Web.

Le navigateur indique qu'il contacte actuellement l'hôte, puis expire avec le message suivant :

```
The document contains no data; Try again later, or contact
the server's Administrator.... (Le document ne contient
aucune donnée. Recommencez ultérieurement ou contactez
l'administrateur du serveur.)
```

Assurez-vous que système soit configuré correctement et que Content Gateway puisse lire le fichier de résolution des noms :

- Vérifiez si le serveur peut résoudre les recherches à l'aide de la commande `nslookup`. Par exemple :

  ```
  nslookup www.monhote.com
  ```

- Vérifiez que le fichier **/etc/resolv.conf** contient bien l'adresse IP valide de votre ou vos serveurs DNS.
- Dans certains systèmes, si le fichier **/etc/resolv.conf** est illisible ou n'a pas d'entrée de serveur de noms, le système d'exploitation utilise localhost comme serveur de noms. Toutefois, Content Gateway n'utilise pas cette convention. Si vous souhaitez utiliser localhost comme serveur de noms, vous devez ajouter une entrée de serveur de noms pour 127.0.0.1 ou 0.0.0.0 dans le fichier **/etc/resolv.conf**.
- Vérifiez que le compte d'utilisateur Content Gateway est bien autorisé à lire le fichier **/etc/resolv.conf**. Remplacez les autorisations du fichier par `rw-r--r-- (644)`.

Important

Si les adresses IP indiquées dans le fichier **/etc/resolv.conf** changent, vous devez redémarrer Content Gateway.

Message de dépassement de la taille maximale de document dans le fichier journal système

Le message suivant apparaît dans le fichier journal système.

```
WARNING (AVERTISSEMENT) : Maximum document size exceeded
(Taille maximale de document dépassée)
```

L'objet demandé était plus volumineux que la taille maximale autorisée dans le cache du proxy. Content Gateway a fourni un service de proxy pour cet objet, mais ne l'a pas mis en cache.

Pour définir la limite de taille des objets mis en cache, modifiez le champ **Maximum Object Size (Taille maximale des objets)** dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Cache > Général**. Si vous ne souhaitez pas limiter la taille des objets mis en cache, définissez la taille des documents sur `0` (zéro).

Message DrainIncomingChannel dans le fichier journal système

Les messages suivants apparaissent dans le fichier journal système :

```
Feb 20 23:53:40 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.telechamada.pt/ HTTP/1.0'
Feb 20 23:53:46 louis last message repeated 1 time
Feb 20 23:53:58 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.ip.pt/ HTTP/1.0'
```

Ces messages d'erreur indiquent qu'un navigateur envoie des requêtes HTTP à l'un des ports du cluster Content Gateway, soit `rsport` (par défaut, port 8087), soit `mcport` (par défaut, port 8088). Content Gateway ne traite pas cette requête. Cette erreur ne pose pas de problème à Content Gateway. Le navigateur doit être reconfiguré pour utiliser le port correct du proxy.

> **Remarque**
> Les clusters Content Gateway fonctionnent mieux lorsqu'ils sont configurés pour utiliser une interface réseau distincte et un sous-réseau privé, de sorte que les ordinateurs clients n'aient pas accès aux ports du cluster.

Message d'absence du fichier cop dans le fichier journal système

Le message suivant apparaît à plusieurs reprises dans le fichier journal système :

```
content_cop[16056]: encountered "config/internal/no_cop"
file...exiting
```

Le fichier **config/internal/no_cop** joue le rôle de contrôle administratif et indique au processus `content_cop` de s'arrêter immédiatement sans démarrer le processus `content_manager` ni vérifier le fonctionnement. Le fichier **no_cop** empêche le proxy de démarrer automatiquement lorsqu'il a été arrêté avec la commande `./WCGAdmin stop` ou `stop_content_gateway`. Sans un tel contrôle statique, Content Gateway redémarrerait automatiquement à chaque redémarrage du système. Le contrôle `no_cop` maintient Content Gateway à l'arrêt tant qu'il n'est pas redémarré à l'aide de la commande `./WCGAdmin start` ou `start_content_gateway`.

Le script d'installation de Content Gateway crée un fichier **no_cop** de sorte que Content Gateway ne démarre pas automatiquement. Après avoir terminé l'installation et la configuration, et redémarré le système d'exploitation, utilisez la commande `./WCGAdmin start` ou `start_content_gateway` pour démarrer Content Gateway. Pour des informations sur le démarrage et l'arrêt de Content Gateway, consultez la section *Mise en route*, page 11.

Avertissement dans le fichier journal système lors de la modification du fichier vaddrs.config (sous Linux)

Dans un système Linux, si vous modifiez le fichier `vaddrs.config` sans être connecté en tant qu'utilisateur racine, Content Gateway publie dans le fichier journal système un message d'avertissement similaire à celui-ci :

```
WARNING (AVERTISSEMENT) : interface is ignored: Operation
not permitted.
```

Vous pouvez ignorer ce message. Content Gateway n'applique pas vos modifications de la configuration.

Important

Il est recommandé de systématiquement configurer les adresses IP virtuelles à partir de Content Gateway Manager. La modification du fichier **vaddrs.config** peut entraîner des résultats imprévisibles.

Échec des requêtes non transparentes après l'activation de la variable always_query_destination

La variable **proxy.config.arm.always_query_dest**, présente dans le fichier **records.config**, configure Content Gateway en mode transparent afin d'ignorer les en-têtes des hôtes et de toujours demander l'adresse IP du serveur d'origine. Lorsque vous activez cette variable, Content Gateway obtient l'adresse IP du serveur d'origine dans une liste des correspondances NAT existantes au lieu de tenter de résoudre le nom de l'hôte de destination à l'aide d'une recherche DNS. En conséquence, les URL enregistrées ne contiennent que des adresses IP, pas de noms d'hôte. Pour enregistrer les noms de domaine, définissez la variable *`proxy.config.arm.always_query_dest`* sur 0. Toutefois, cette opération ne réduit pas le nombre de recherches DNS.

De plus, les requêtes explicites (non transparentes, y compris sur le port 80) échoueront, car il n'y a pas de correspondance dans la liste NAT.

Remarque

L'option `always_query_destination` ne fonctionne que sur le port principal du proxy.

Content Gateway fonctionne, mais aucun fichier journal n'est généré.

Content Gateway n'écrit des fichiers journaux d'événements que lorsqu'il y a des informations à enregistrer. Si Content Gateway est inactif, il est normal qu'il n'y ait pas de fichiers journaux.

Assurez-vous de rechercher dans le répertoire approprié. Par défaut, Content Gateway crée des fichiers journaux dans son répertoire **logs**. Pour vérifier l'emplacement des fichiers journaux dans Content Gateway Manager, examinez le champ **Log Directory (Répertoire des journaux)** dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Général**. Vous pouvez également vérifier la valeur de la variable `proxy.config.log2.logfile_dir` dans le fichier **records.config**.

Vérifiez que le répertoire est autorisé à lire et à écrire pour le compte d'utilisateur Content Gateway. Si le répertoire des journaux ne dispose pas des autorisations appropriées, le processus `content_gateway` est incapable d'ouvrir et de créer des fichiers journaux.

Vérifiez que la journalisation est bien activée. Dans Content Gateway Manager, examinez la zone **Logging (Journalisation)** dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Général**. Vous pouvez également vérifier la valeur de la variable `proxy.config.log2.logging_enabled` dans le fichier **records.config**.

Vérifiez qu'un format de journaux est bien activé. Dans Content Gateway Manager, vérifiez qu'un format standard est activé dans l'onglet **Configurer > Subsystems (Sous-systèmes) > Logging (Journalisation) > Formats**, ou que le format personnalisé est activé dans l'onglet **Custom (Personnalisé)**. Dans le fichier **records.config**, sélectionnez les formats standard ou personnalisé en modifiant les variables de la section **Logging Config (Configuration de la journalisation)**.

Erreur de Content Gateway indiquant trop de connexions réseau

Par défaut, Content Gateway prend en charge 8000 connexions réseau : une moitié est allouée aux connexions des clients et l'autre est réservée aux connexions des serveurs d'origine. Un événement de limite de connexions se produit lorsque les connexions des clients ou des serveurs d'origine atteignent 90 % de la moitié de la limite configurée (3600 par défaut). Lorsqu'un événement de limite de connexions se produit, Content Gateway continue à traiter toutes les connexions en cours, mais n'accepte plus les nouvelles requêtes des clients tant que le nombre de connexions n'est pas redescendu en-dessous de la limite.

Les événements de limite de connexions se produisent dans les cas suivants :

- Lorsqu'il y a un *pic de connexions* : des milliers de requêtes de clients contactent le proxy simultanément. De tels événements sont généralement transitoires et n'exigent aucune action corrective.
- Lorsqu'il y a une *surcharge du service* : les requêtes des clients arrivent continuellement trop vite pour que le proxy puisse toutes les satisfaire au même rythme. Ces surcharges du service indiquent souvent des problèmes réseau entre Content Gateway et les serveurs d'origine ou que Content Gateway a besoin de davantage de mémoire, de CPU, de cache disques ou d'autres ressources pour gérer la charge des clients.

Examinez les graphiques des performances pour identifier la nature de la surcharge de connexions. Vérifiez notamment les graphiques Client Connections (Nombre de connexions de clients), TCP Connections (Nombre de connexions TCP) et Client Ops Per Second (Nombre de transactions de clients par seconde). Vous pouvez également vérifier les messages d'erreur dans les fichiers journaux système, d'erreurs ou d'événements.

Si nécessaire, vous pouvez redéfinir le nombre maximum de connexions prises en charge par le proxy dans l'onglet **Configurer > Networking (Mise en réseau) > Connection Management (Gestion des connexions) > Throttling (Limitation)**, ou modifiez la valeur de la variable *proxy.config.net.connections_throttle* dans le fichier **records.config**. N'augmentez pas la limite de connexions tant que le système n'a pas suffisamment de mémoire pour gérer le nombre de connexions requis. Tout système dont la mémoire RAM est limitée doit avoir une limite de connexions inférieure à la valeur par défaut.

Important

Ne définissez pas cette variable sur une valeur inférieure à la valeur minimale de 100.

Symptômes du manque de mémoire

En cas de charge très lourde, le noyau Linux peut manquer de mémoire RAM. Cette condition peut ralentir les performances et provoquer divers problèmes système. Le manque de mémoire RAM peut se faire sentir même si le système dispose d'une grande quantité d'espace d'échange disponible.

Les symptômes d'une insuffisance extrême de mémoire comprennent les messages suivants dans les fichiers journaux système (**/var/log/messages**) :

```
WARNING (AVERTISSEMENT) : errno 105 is ENOBUFS (low on
kernel memory), consider a memory upgrade
kernel: eth0: can't fill rx buffer (force 0)!
kernel: recvmsg bug: copied E01BA916 seq E01BAB22
```

Vous pouvez éventuellement configurer Content Gateway pour qu'il suspende l'analyse du trafic lorsque le système vient à manquer de mémoire. Dans Content Gateway Manager, ouvrez l'onglet **Configurer > Networking (Mise en réseau) > Connection Management (Gestion des connexions) > Low Memory Mode (Mode mémoire insuffisante)**. Voir *Gestion des connexions*, page 320.

Expiration des connexions au serveur d'origine

Certains serveurs d'origine ont besoin de plus de 30 secondes pour publier des requêtes HTTP, ce qui provoque des expirations de leurs connexions au proxy. Pour prévenir de telles expirations des connexions, dans Content Gateway Manager, ouvrez l'onglet **Configurer > Protocoles > HTTP > Timeouts (Expirations)** et, dans la section **Active Timeout (Expiration active)**, changez la valeur de **Origin Server Response (Réponse du serveur d'origine)** pour la définir sur 60 secondes ou plus.

Dysfonctionnement des serveurs Web IBM avec Content Gateway

Les serveurs Web IBM ne prennent pas en charge le protocole TLS (Transport Layer Security). Pour qu'ils fonctionnent avec Content Gateway, vous devez modifier la valeur d'une variable de configuration.

1. Ouvrez le fichier **records.config** situé dans **/opt/WCG/config**.
2. Modifiez la variable suivante :

Variable	Description
`proxy.config.ssl.TLSv1`	Définissez cette variable sur 0 (zéro).

3. Enregistrez et fermez le fichier.
4. Dans le répertoire **bin** de Content Gateway (**/opt/WCG/bin)**, exécutez la commande `content_line -x` pour appliquer vos modifications.

Content Gateway ne démarre pas (ou ne s'arrête pas).

Content Gateway démarre automatiquement après son installation. Si vous devez l'arrêter, la méthode conseillée consiste à utiliser les commandes `./WCGAdmin start` et `./WCGAdmin stop`.

Pour démarrer ou arrêter Content Gateway :

1. Devenez utilisateur racine :

   ```
   su
   ```

2. Accédez au répertoire **bin** de Content Gateway (**/opt/WCG/bin**).
3. Démarrez le proxy :

   ```
   ./WCGAdmin start
   ```

   Arrêtez le proxy :

   ```
   ./WCGAdmin stop
   ```

Glossaire

Alternatives

Différentes versions du même objet Web. Certains serveurs d'origine répondent aux requêtes correspondant à la même URL par divers objets. Le contenu de ces objets peut varier, selon si le serveur fournit un contenu différent selon les langues, cible les différents navigateurs par des styles de présentation différents ou envoie différents contenus selon les heures de la journée.

Accès fructueux au cache

Objet présent dans le cache et qui peut être envoyé directement au client

Accès infructueux au cache

Objet absent dans le cache, ou il est présent mais n'est plus valide. Dans les deux cas, le proxy doit récupérer l'objet auprès du **Serveur d'origine**.

ARM

Adaptive Redirection Module. Ce module prend en charge la mise en cache du proxy transparent lors de laquelle le module ARM redirige le trafic intercepté des clients entre un serveur d'origine et Content Gateway. Avant que le trafic soit redirigé par le module ARM, il est intercepté par un **Commutateur de Niveau 4** ou un routeur.

Basculement IP virtuel

Option disponible pour les serveurs Content Gateway mis en cluster. Content Gateway conserve un pool d'adresses IP virtuelles qu'il affecte aux nœuds du cluster. Si un nœud tombe en panne, les autres masquent cette défaillance et prennent le relais.

Cache

Stocke des copies des objets fréquemment demandés à proximité des utilisateurs et les leur envoie à la demande. Voir également **Magasin d'objets**.

Cache enfant

Cache inférieur dans une **Hiérarchie de caches** dont Content Gateway est un parent. Voir également **Cache parent**.

Cache parent

Cache supérieur dans une **Hiérarchie de caches**, auquel le proxy peut envoyer des requêtes

CGI

Common Gateway Interface. Ensemble de règles qui décrivent la communication entre un serveur d'origine et un autre élément logiciel (un *programme CGI*) installé dans le même ordinateur.

cgi-bin

Nom du répertoire le plus utilisé dans un serveur d'origine. Les programmes **CGI** y sont stockés.

Cluster

Groupe de nœuds Content Gateway qui partage des informations de configuration et peut agir en tant que grand cache unique virtuel

Commutateur de Niveau 4

Commutateur Ethernet qui peut contrôler le flux du trafic réseau à l'aide des règles de Niveau 4 (L4). Il peut intercepter les paquets des protocoles client désirés et les diriger vers un proxy pour un traitement transparent.

Content Gateway Manager

Interface de Content Gateway sur navigateur, composée d'une série de pages Web qui vous permettent de surveiller les performances du système et de modifier ses paramètres de configuration

content_cop

Processus Content Gateway qui surveille le fonctionnement des processus **content_gateway** et **content_manager** en envoyant régulièrement des requêtes de pulsation pour récupérer des pages Web synthétiques

content_gateway

Processus Content Gateway qui est le moteur de traitement du cache du produit Content Gateway. `content_gateway` est chargé d'accepter les connexions, de traiter les requêtes et de fournir les documents demandés à partir du **Cache** ou du **Serveur d'origine**.

content_manager

Processus Content Gateway et dispositif de contrôle et de commande. `content_manager` est chargé de lancer, surveiller et reconfigurer le processus **content_gateway**. Il est également responsable de l'interface utilisateur d'administration, du port d'auto-configuration du proxy, de l'interface des statistiques, de l'administration du cluster et du **Basculement IP virtuel**.

Cookie

Élément d'informations envoyé à un navigateur Web par un serveur d'origine. Le logiciel du navigateur enregistre ces informations et les renvoie au serveur à chaque nouvelle requête du navigateur. Les cookies permettent aux serveurs d'origine de garder la trace des utilisateurs.

DNS

Système de noms de domaine (Domain Name Service). Content Gateway comprend un résolveur DNS asynchrone rapide qui simplifie les conversions de noms d'hôte en adresses IP.

FAI

Fournisseur d'accès Internet. Entreprise qui fournit l'accès à Internet.

Fichier PAC

Fichier d'auto-configuration du proxy. Définition de fonction JavaScript appelée par un navigateur pour déterminer le traitement des requêtes.

Format de journalisation Netscape

Format standard de la journalisation des accès. Il vous permet d'analyser les fichiers journaux de l'accès à Content Gateway avec des scripts d'analyse des journaux prêts à l'emploi. Voir également **Format de journalisation Squid**.

Format de journalisation Squid

Format standard de la journalisation des accès. Il vous permet d'analyser les fichiers journaux d'événements de Content Gateway avec des scripts d'analyse des journaux prêts à l'emploi. Voir également **Format de journalisation Netscape**.

FTP

File Transfer Protocol (Protocole de transfert de fichiers). Protocole basé sur TCP/IP pour la fiabilité des transferts de fichiers.

Gestion de la mise en cluster

Option de Content Gateway dans laquelle tous les nœuds d'un cluster partagent automatiquement les mêmes informations de configuration

Hiérarchie de caches

Niveaux de caches qui communiquent entre eux. Toutes les hiérarchies de caches reconnaissent les concepts de **Cache parent** et **Cache enfant**.

HTTP

Hypertext Transfer Protocol. Protocole client/serveur sur lequel repose le World Wide Web.

HTTPS

Hypertext Transfer Protocol Secure. Utilisation du protocole HTTP avec SSL pour fournir une forme de communication cryptée sur le World Wide Web.

IP

Internet Protocol. Protocole de couche inférieure, placé sous TCP/IP et chargé des transmissions de bout-en-bout et du contrôle de la fragmentation des paquets.

JavaScript

Langage de script conçu pour permettre aux pages Web d'interagir avec leurs visiteurs. Parmi ces interactions, citons les actions en réponse aux mouvements ou aux clics de la souris et la validation des données saisies dans les formulaires.

Magasin d'objets

Base de données haut débit et personnalisée, dans laquelle Content Gateway stocke tous les objets mis en cache

Mise en cache de proxy explicite

Option de configuration de Content Gateway, dans laquelle le logiciel client (généralement un navigateur) doit être configuré spécialement pour envoyer les requêtes Web au proxy Content Gateway

Mise en cache du proxy transparent

Option de configuration qui permet à Content Gateway d'intercepter les requêtes Internet et d'y répondre sans que les utilisateurs n'aient besoin de reconfigurer les paramètres de leur navigateur. Pour ce faire, il intercepte le trafic destiné à un serveur d'origine et le redirige via le cache du proxy.

Mise en cache du serveur proxy Web

Serveur proxy Web avec stockage de cache local qui lui permet de satisfaire les requêtes des clients localement à l'aide d'une copie mise en cache de la précédente réponse du serveur d'origine

Mode Configuration

L'un des deux modes de **Content Gateway Manager**. Il vous permet de configurer le système Content Gateway. Voir également **Mode Surveillance**.

Mode Surveillance

L'un des deux modes de **Content Gateway Manager**. Le mode Surveillance vous permet d'afficher des statistiques sur les performances de Content Gateway et sur le trafic Web. Voir également **Mode Configuration**.

MRTG

Multi Router Traffic Grapher. Outil graphique fourni avec Content Gateway qui crée les graphiques qui vous permettent de surveiller les performances de Content Gateway.

Routeur

Périphérique qui gère la connexion entre plusieurs réseaux. Les routeurs examinent les adresses de destination des paquets qui les traversent et décident de leur itinéraire.

Serveur d'origine

Serveur Web qui contient la copie originale des informations demandées

Serveur proxy

Voir **Serveur proxy Web**.

Serveur proxy Web

Serveur proxy qui transmet les requêtes des clients à leur **Serveur d'origine**. Il peut refuser des requêtes en fonction des règles de filtrage ou des restrictions de sécurité.

Serveur Web

Ordinateur qui fournit des services World Wide Web sur Internet. Voir également **Serveur d'origine**.

SOCKS

Protocole de proxy de niveau circuit qui fournit un mécanisme de mise en tunnel aux protocoles qui ne conviennent pas aux proxy

SSL

Secure Sockets Layer. Protocole qui permet de crypter et d'authentifier les communications à travers Internet. Utilisé essentiellement pour les communications entre les serveurs d'origine et les navigateurs Web.

syslog

Utilitaire de journalisation du système UNIX

TCP

Transmission Control Protocol. Protocole Internet standard de la couche de transport. TCP fournit des communications fiables de bout-en-bout à l'aide de données séquencées envoyées par IP.

URL

Uniform Resource Locator. Adresse qui définit l'itinéraire d'accès à un fichier sur le Web ou un autre dispositif Internet.

WCCP

Web Cache Control Protocol. Protocole utilisé par les routeurs Cisco IOS pour rediriger le trafic pendant la mise en cache du proxy transparent.

WPAD

Web Proxy Auto-Discovery. Protocole qui permet aux clients de localiser automatiquement un proxy Web, afin de bénéficier des avantages d'un proxy sans configuration explicite des clients.

ANNEXE J

Copyrights

AUTRES PARTIES DISTRIBUENT LE PROGRAMME « EN L'ÉTAT », SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER. VOUS ASSUMEZ LA TOTALITÉ DES RISQUES LIÉS À LA QUALITÉ ET AUX PERFORMANCES DU PROGRAMME. EN CAS DE DÉFAILLANCE DU PROGRAMME, VOUS ASSUMEZ LE COUT DE TOUTES LES OPÉRATIONS DE MAINTENANCE, DE RÉPARATION OU DE CORRECTION.

Netscape Directory SDK 4.0 pour C

Netscape Directory SDK 4.0 pour C est disponible sans frais de licence dans le cadre des termes et conditions du Contrat de licence d'utilisateur final Netscape ONE SDK.

Chacun des Composants est fourni « EN L'ÉTAT », sans garantie d'aucune sorte, incluant, sans limitation, les garanties de qualité marchande et d'adéquation à un usage particulier et d'absence de contre-façon. La totalité des risques liés à la qualité et aux performances des Composants vous incombent. En cas de dysfonctionnement ou d'imprécision des Composants, suivant le cas, vous, et non Netscape ou ses fournisseurs, assumez la totalité des frais de maintenance et de réparation. Par ailleurs, les mécanismes de sécurité éventuellement implémentés par les Composants présentent des limitations inhérentes, et vous devez déterminer que chacun des Composants répond correctement à vos besoins. Cette exclusion de garantie constitue un élément essentiel du présent contrat. CERTAINES JURIDICTIONS N'AUTORISANT PAS LES EXCLUSIONS DE GARANTIE IMPLICITE, IL SE PEUT QUE CETTE EXCLUSION NE VOUS CONCERNE PAS ET QUE VOUS BÉNÉFICIEZ D'AUTRES DROITS, QUI VARIENT SELON LES JURIDICTIONS.

Tcl 8.3

Le logiciel Tcl est protégé par les droits d'auteur de Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, et d'autres tiers. Les termes suivants s'appliquent à tous les fichiers associés au logiciel, sauf indication contraire explicite dans les fichiers individuels. Par le présent document, les auteurs autorisent toute personne à utiliser, copier, modifier, distribuer et concéder sous licence ce logiciel et la documentation qui l'accompagne, pour quelque fin que ce soit, sous réserve que les avertissements relatifs aux droits d'auteur apparaissent dans toutes les copies et que cet avertissement figure textuellement dans toutes les distributions. Aucun accord écrit, ni frais de licence ou de droits d'auteur n'est requis pour les utilisations autorisées. Les modifications apportées à ce logiciel peuvent être protégées par leurs auteurs et différer des conditions de licence décrites dans le présent document, à condition que ces nouvelles conditions soient clairement indiquées dans la première page de chaque fichier concerné.

LES AUTEURS OU LES DISTRIBUTEURS NE POURRONT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES DIRECTS, INDIRECTS, SPÉCIAUX ET ACCESSOIRES, NI D'AUCUN DOMMAGE QUEL QU'IL SOIT RÉSULTANT DE L'UTILISATION DE CE LOGICIEL, DE SA DOCUMENTATION OU DE SES DÉRIVÉS, ET CE, MÊME SI LES AUTEURS ONT ÉTÉ INFORMÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. LES AUTEURS ET LES DISTRIBUTEURS DÉCLINENT EXPRESSEMENT TOUTE GARANTIE, Y COMPRIS, SANS LIMITATION AUCUNE, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON. CE LOGICIEL EST FOURNI « EN L'ÉTAT », ET LES AUTEURS ET LES DISTRIBUTEURS NE SONT EN RIEN TENUS D'ASSURER LA MAINTENANCE OU DE FOURNIR UN SUPPORT, DES MISES A JOUR, DES AMÉLIORATIONS OU DES MODIFICATIONS.

libdb

LIBDB Copyright © 1991, 1993 The Regents of the University of California. Tous droits réservés.
Ce produit comprend un logiciel édité par l'Université de Californie, Berkeley et ses contributeurs.

CE LOGICIEL EST FOURNI « EN L'ÉTAT » PAR 'THE REGENTS' ET LES CONTRIBUTEURS ET TOUTE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS, SANS LIMITATION AUCUNE, TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE. 'THE REGENTS' OU LES CONTRIBUTEURS NE POURRONT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES DIRECTS, INDIRECTS, SPÉCIAUX OU EXEMPLAIRES, NI D'AUCUN DOMMAGE QUEL QU'IL SOIT (Y COMPRIS LES DOMMAGES CAUSÉS PAR LA PERTE D'USAGE, LA PERTE DE DONNÉES OU DE BÉNÉFICES OU L'INTERRUPTION D'EXPLOITATION), CAUSÉS D'UNE MANIÈRE OU D'UNE AUTRE, QUE CETTE RESPONSABILITÉ SOIT DE NATURE CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) RÉSULTANT DE, OU LIÉS D'UNE QUELCONQUE MANIÈRE À L'UTILISATION DE CE LOGICIEL, ET CE MÊME SI 'THE REGENTS' OU LES CONTRIBUTEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

INN

Copyright © 1991, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001 The Internet Software Consortium and Rich Salz. Ce code provient d'un logiciel d'Internet Software Consortium by Rich Salz. Vous êtes autorisé(e) à redistribuer et à utiliser le code source et les formes binaires, avec ou sans modification, pour autant que les conditions suivantes soient respectées : 1. La redistribution du code source doit faire mention des droits d'auteur ci-dessus, de cette liste de conditions et de l'avis de non-responsabilité suivant. 2. La redistribution sous forme binaire doit faire mention des droits d'auteur ci-dessus, de cette liste de conditions et de l'avis de non-responsabilité suivant dans la documentation et/ou tout autre matériel accompagnant la distribution. 3. Tout support publicitaire mentionnant les fonctions ou l'utilisation de ce logiciel doit porter la mention suivante : Ce produit comprend un logiciel édité par Internet Software Consortium et ses contributeurs. 4. Toute utilisation du nom de Internet Software Consortium ou des noms de ses contributeurs en vue de soutenir ou de promouvoir les produits dérivés de ce logiciel sans autorisation écrite et expresse au préalable est interdite.

CE LOGICIEL EST FOURNI « EN L'ÉTAT » PAR INTERNET SOFTWARE CONSORTIUM ET SES CONTRIBUTEURS ET TOUTE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS, SANS LIMITATION AUCUNE, TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE. INTERNET SOFTWARE CONSORTIUM OU SES CONTRIBUTEURS NE POURRONT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX OU EXEMPLAIRES, NI D'AUCUN DOMMAGE QUEL QU'IL SOIT (Y COMPRIS LES DOMMAGES CAUSÉS PAR LA FOURNITURE DE SERVICES OU DE BIENS DE SUBSTITUTION, LA PERTE D'USAGE, LA PERTE DE DONNÉES OU DE BÉNÉFICES OU L'INTERRUPTION D'EXPLOITATION), CAUSÉS D'UNE MANIÈRE OU D'UNE AUTRE, QUE CETTE RESPONSABILITÉ SOIT DE NATURE CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) RÉSULTANT DE, OU LIÉS D'UNE QUELCONQUE MANIÈRE À L'UTILISATION DE CE LOGICIEL, ET MÊME SI LES PROPRIÉTAIRES DES DROITS D'AUTEUR ET LES CONTRIBUTEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

MRTG

Multi Router Traffic Grapher (MRTG) est librement diffusable et utilisable selon les termes de la Licence Publique Générale GNU. Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

LE PROGRAMME ÉTANT CONCÉDÉ SOUS LICENCE GRATUITE, IL NE BÉNÉFICIE PAS D'UNE GARANTIE, DANS LES LIMITES AUTORISÉES PAR LES LOIS EN VIGUEUR. SAUF INDICATION CONTRAIRE PAR ÉCRIT, LES DÉTENTEURS DES DROITS D'AUTEUR ET LES AUTRES PARTIES DISTRIBUENT LE PROGRAMME « EN L'ÉTAT », SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER. VOUS ASSUMEZ LA TOTALITÉ DES RISQUES LIÉS À LA QUALITÉ ET AUX PERFORMANCES DU PROGRAMME. EN CAS DE DÉFAILLANCE DU PROGRAMME, VOUS ASSUMEZ LE COUT DE TOUTES LES OPÉRATIONS DE MAINTENANCE, DE RÉPARATION OU DE CORRECTION.

Libregx

Copyright © 1992, 1993, 1994, 1997 Henry Spencer. Tous droits réservés. Ce logiciel n'est pas protégé par une licence d'American Telephone and Telegraph Company ou de The Regents of the University of California.

libmagic

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Logiciel écrit par Ian F. Darwin et d'autres ; maintenance assurée par Christos Zoulas.

Ce logiciel n'est pas soumis aux dispositions concernant les exportations du Département du commerce des États-Unis et peut être exporté vers tout autre pays ou planète.

Vous êtes autorisé(e) à redistribuer et à utiliser le code source et les formes binaires, avec ou sans modification, pour autant que les conditions suivantes soient satisfaites :

1. La redistribution du code source doit faire mention, au tout début du fichier et sans aucune modification, des droits d'auteur ci-dessus, de cette liste de conditions et de l'avis de non-responsabilité suivant.

2. La redistribution sous forme binaire doit faire mention des droits d'auteur ci-dessus, de cette liste de conditions et de l'avis de non-responsabilité suivant dans la documentation et/ou tout autre matériel accompagnant la distribution.

CE LOGICIEL EST FOURNI « EN L'ÉTAT » PAR L'AUTEUR ET LES CONTRIBUTEURS ET TOUTE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER EST EXCLUE. L'AUTEUR OU LES CONTRIBUTEURS NE POURRONT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX OU EXEMPLAIRES, NI D'AUCUN DOMMAGE QUEL QU'IL SOIT (Y COMPRIS LES DOMMAGES CAUSÉS PAR LA FOURNITURE DE SERVICES OU DE BIENS DE SUBSTITUTION, LA PERTE D'USAGE, LA PERTE DE DONNÉES OU DE BÉNÉFICES OU L'INTERRUPTION D'EXPLOITATION), CAUSÉS D'UNE MANIÈRE OU D'UNE AUTRE, QUE CETTE RESPONSABILITÉ SOIT DE NATURE CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) RÉSULTANT DE, OU LIÉS D'UNE QUELCONQUE MANIÈRE À L'UTILISATION DE CE LOGICIEL, ET CE MÊME SI L'AUTEUR OU LES CONTRIBUTEURS ONT ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

S

T

U

V

W

X