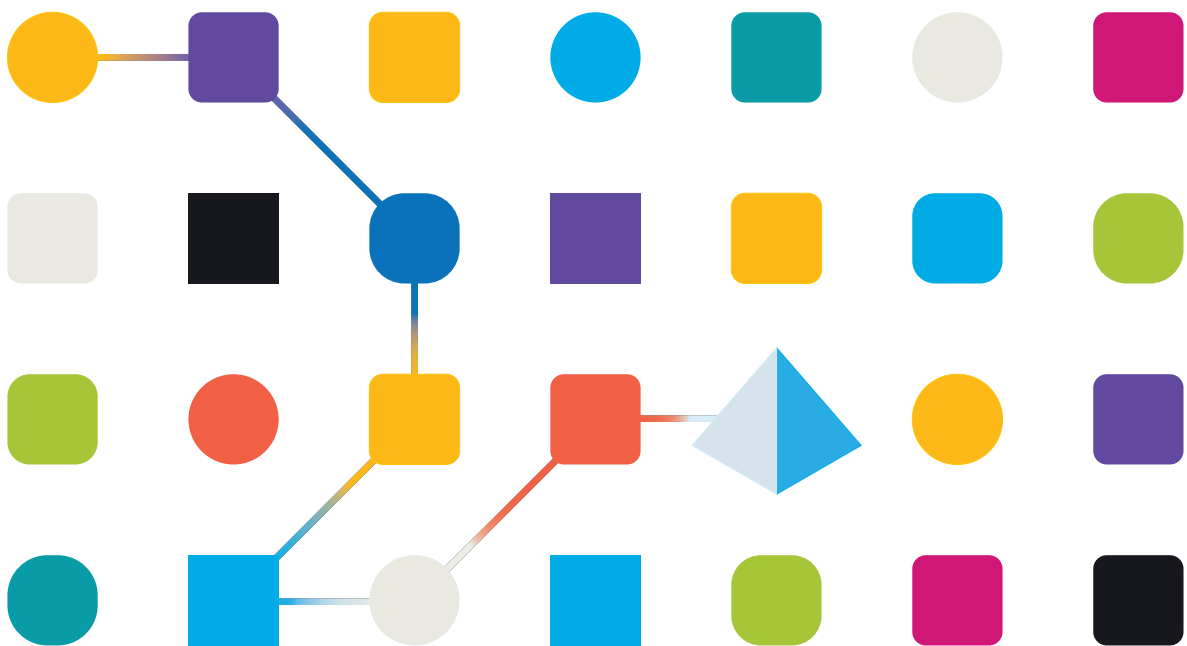


blueprism[®]

Hub and Interact 4.6

Guide de configuration haute disponibilité

Révision des documents : 3.0



Marques déposées et droits d'auteur

Les informations contenues dans ce document sont les informations propriétaires et confidentielles de Blue Prism Limited et ne doivent pas être divulguées à un tiers sans le consentement écrit d'un représentant autorisé de Blue Prism. Aucune partie de ce document ne peut être reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie, sans la permission écrite de Blue Prism Limited.

© 2023 Blue Prism Limited

« Blue Prism », le logo « Blue Prism » et l'appareil Prism sont des marques commerciales ou des marques déposées de Blue Prism Limited et ses filiales. Tous droits réservés.

Toutes les marques sont reconnues et utilisées au profit de leurs propriétaires respectifs.

Blue Prism n'est pas responsable du contenu des sites web externes mentionnés dans ce document.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.

Enregistré en Angleterre : numéro d'enregistrement 4260035. Tél. : +44 370 879 3000. Web :

www.blueprism.com

Contenu


| | |
|---|-----------|
| Configuration haute disponibilité | 4 |
| Public visé | 4 |
| Prérequis | 5 |
| Cluster RabbitMQ | 5 |
| Groupe de haute disponibilité SQL | 5 |
| Équilibreur de charge | 6 |
| Serveurs Web | 6 |
| Logiciel et scripts Blue Prism | 6 |
| Exemple d'infrastructure | 7 |
| Configuration de haute disponibilité avec HAProxy | 7 |
| Configuration de haute disponibilité avec ARR IIS et HAProxy | 8 |
| Configuration de haute disponibilité avec Application Gateway | 9 |
| Équilibreur de charge HAProxy – Exemple de configuration | 10 |
| Exemple de script d'équilibreur de charge (HAProxy) | 10 |
| Installation et configuration initiales | 14 |
| Installer Blue Prism Hub | 14 |
| Installer Blue Prism Interact | 14 |
| Configurer votre installation | 15 |
| Solution scriptée | 16 |
| Informations importantes | 16 |
| Script Functions.ps1 | 17 |
| Script Prepare.ps1 | 18 |
| Script Setup.ps1 | 21 |
| Tester votre environnement de haute disponibilité | 23 |
| Logging | 25 |

Configuration haute disponibilité


La haute disponibilité garantit la disponibilité permanente des systèmes grâce à l'utilisation de plusieurs serveurs. La configuration de plusieurs serveurs fournit une résilience intégrée. Si un serveur échoue, la disponibilité ne sera pas perdue.


Blue Prism fournit une solution scriptée pour répliquer votre Blue Prism® Hub et votre serveur Web Blue Prism® Interact à des hôtes de serveur Web supplémentaires.

Ce guide offre des conseils sur la manière de préparer les hôtes de serveur Web pour la configuration de haute disponibilité, à l'aide de scripts fournis par Blue Prism. Ces informations sont fournies à titre de conseils de haut niveau uniquement. Il est recommandé de suivre les meilleures pratiques standard de l'industrie et de rechercher les recommandations d'un professionnel expérimenté.

 Si vous utilisez un environnement de haute disponibilité avec plusieurs nœuds, Hub et Interact peuvent actuellement prendre en charge jusqu'à 250 requêtes simultanées adressées au serveur. Par exemple, il peut prendre en charge 250 utilisateurs, tous cliquant sur **Soumettre** sur un formulaire en l'espace d'une seconde. De nombreux autres utilisateurs peuvent se trouver simultanément sur le système et afficher ou saisir des informations sans adresse de requête au serveur (comme la saisie dans un champ de texte). Blue Prism vise à augmenter cette limite dans les versions futures.

Avant d'entreprendre un déploiement de haute disponibilité, vous devez vérifier auprès de votre service informatique que l'infrastructure du réseau peut prendre en charge le déploiement envisagé.

 Pour voir le processus d'installation et de configuration de haute disponibilité, regardez notre [vidéo d'installation de la haute disponibilité de Blue Prism Hub et d'Interact](#).

 L'utilisation de l'authentification Active Directory avec la configuration haute disponibilité n'est pas prise en charge.

Public visé

Ce guide est destiné aux professionnels de l'informatique compétents dans les domaines suivants :

- Configuration des hôtes du serveur Web
- Utilisation de scripts PowerShell

Prérequis

Ce guide couvre uniquement la configuration du logiciel Blue Prism dans une configuration de haute disponibilité. Il ne couvre pas les détails de la configuration des produits tiers requis.

Avant de configurer Hub et, éventuellement, Interact, vous aurez besoin de :

- **Cluster RabbitMQ** : installé et configuré avec trois (ou plus) hôtes.
- **Groupe de haute disponibilité SQL** : installé et configuré avec deux à trois hôtes.
- **Équilibreur de charge** : installé et configuré avec un à deux hôtes.
- **Serveurs Web** : installés avec le logiciel prérequis prêt à installer Blue Prism Hub et Blue Prism Interact.
- **Logiciel et scripts Blue Prism** : les installateurs et scripts pour configurer votre environnement de haute disponibilité Blue Prism.

Cluster RabbitMQ

Il est recommandé d'utiliser au moins trois serveurs RabbitMQ dans votre cluster RabbitMQ avec des files d'attente miroir. Les serveurs doivent tous exécuter les mêmes versions de RabbitMQ et d'Erlang. Pour plus d'informations sur les versions requises, voir [Serveur de l'agent de messages](#).

Des informations sur la création d'un cluster sont disponibles sur le site Web de RabbitMQ : <https://www.rabbitmq.com/clustering.html>.

Groupe de haute disponibilité SQL

Il est recommandé d'utiliser au moins deux serveurs SQL dans un groupe de disponibilité AlwaysOn. Si vous utilisez Azure, un équilibreur de charge Azure est requis.


Si Blue Prism Hub et/ou Blue Prism Interact est/sont installé(s) dans une configuration standard (serveur Web unique), les assistants d'installation créent les bases de données. Cependant, pour la configuration de haute disponibilité, vous devez créer les bases de données requises manuellement avant d'installer le logiciel, ainsi que des bases de données supplémentaires qui sont utilisées comme caches pour les principaux services. Les bases de données requises sont les suivantes :

- AuditDB
- AuthenticationServerDB
- EmailServiceDB
- FileServiceDB
- HubDB
- LicenseManagerDB
- NotificationCenterDB
- AuthenticationServerCache
- HubCache

Si vous installez également Interact, vous aurez besoin des bases de données supplémentaires suivantes :

- IadaDB
- InteractDB
- InteractCache

Pour plus d'informations sur les groupes de disponibilité AlwaysOn, consultez la documentation Microsoft : <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver15>

 Vous devez travailler avec vos administrateurs de base de données pour créer les bases de données et les ajouter au groupe de disponibilité AlwaysOn. Il est probable qu'ils aient un processus scripté et votre entreprise peut nécessiter des réglages de configuration supplémentaires.

Équilibreur de charge

Vous aurez besoin d'un équilibreur de charge pour distribuer les tâches aux serveurs dans l'environnement de haute disponibilité. Vous devriez utiliser l'équilibreur de charge le mieux adapté à votre entreprise. La transparence IP doit être définie sur l'équilibreur de charge afin de stocker l'adresse IP appropriée dans les événements d'audit.

Ce guide utilise HAProxy comme exemple d'équilibreur de charge dans la configuration de haute disponibilité. Pour plus d'informations sur cette configuration, voir [Exemple d'infrastructure sur la page suivante](#) et [Équilibreur de charge HAProxy – Exemple de configuration sur la page 10](#).

Serveurs Web


Vous devrez préparer les hôtes du serveur Web à utiliser dans la configuration de haute disponibilité. Vous aurez besoin d'un serveur Web pour l'installation et la configuration initiales de Hub et/ou d'Interact, et d'hôtes de serveur Web supplémentaires sur lesquels dupliquer la configuration.

Consultez le [guide d'installation de Hub](#) et le [guide d'installation d'Interact](#) pour connaître la configuration matérielle et logicielle requise des serveurs.

Pour préparer les hôtes :

- Installez IIS sur chaque hôte. Voir [Installer IIS](#) pour en savoir plus.
- Installez Microsoft .NET Core Runtime (3.1.11 ou versions ultérieures) et Microsoft Windows Desktop Runtime (3.1.11 ou versions ultérieures) sur chaque hôte. Les hôtes supplémentaires doivent utiliser la même version que sur le serveur Web initial. Pour plus d'informations sur l'installation, voir [Installer les composants .Net Core](#).

Consultez le [guide d'installation de Hub](#) pour plus d'informations sur le téléchargement du logiciel.

 Avant d'installer le logiciel, vous devez décider si vous souhaitez utiliser l'authentification Windows ou l'authentification SQL. Si vous utilisez l'authentification Windows, vous devez vous assurer que vos comptes de service sont configurés pour accéder aux pools d'applications et aux certificats appropriés. Vous devez le faire après avoir installé votre serveur Web initial, mais avant d'exécuter l'un des scripts HA. Voir [Installer Hub à l'aide de l'authentification Windows](#) et [Installer Interact à l'aide de l'authentification Windows](#) pour en savoir plus.

Logiciel et scripts Blue Prism

Vous devrez télécharger ce qui suit à partir du [Portail Blue Prism](#) :

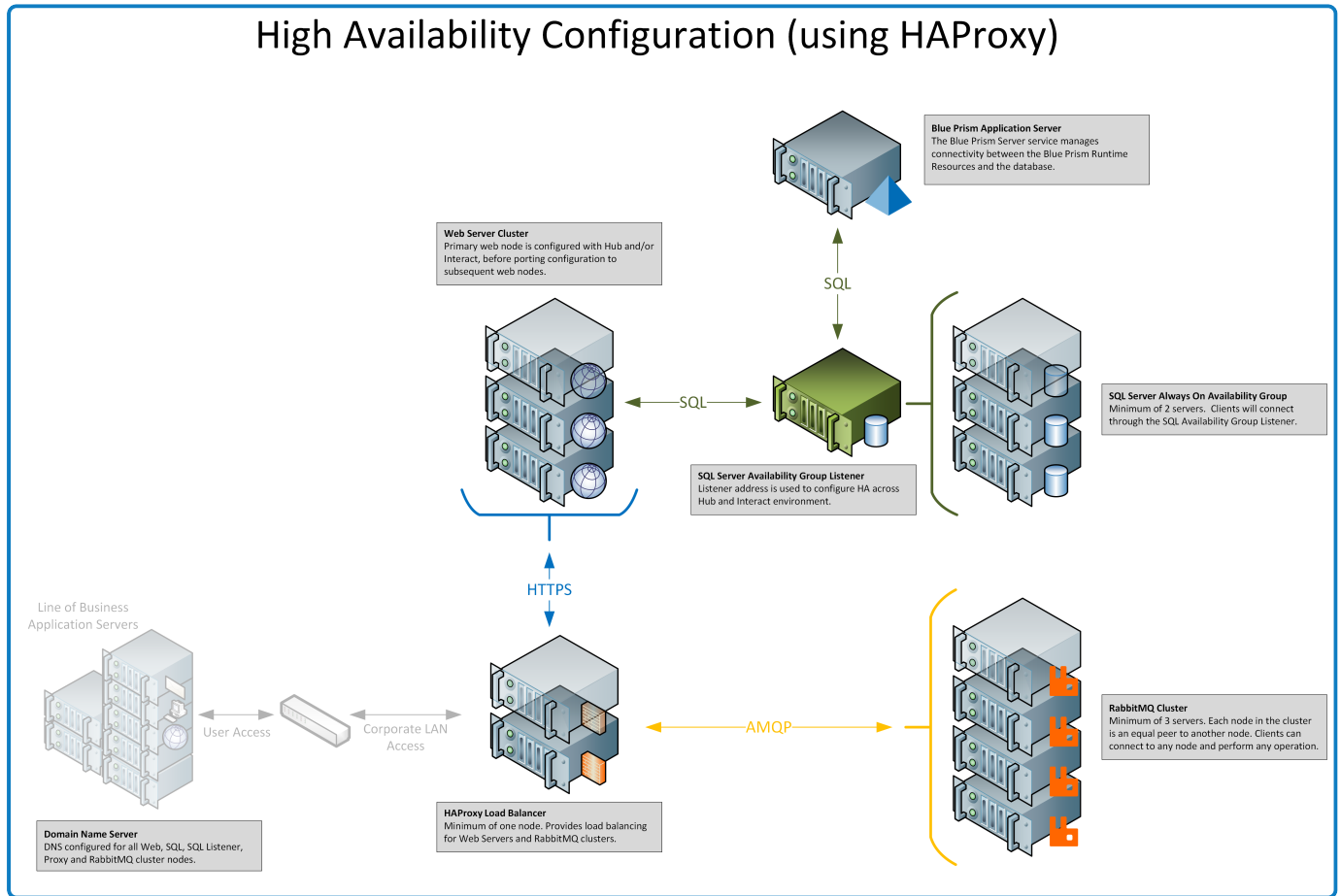
- Assistant d'installation de Blue Prism Hub
- Assistant d'installation de Blue Prism Interact
- Scripts de haute disponibilité
- Outil de protection des données Blue Prism

Exemple d'infrastructure

Les diagrammes suivants illustrent un exemple de configuration d'infrastructure pour les déploiements de haute disponibilité :

- Utilisation de HAProxy : cette configuration est utilisée comme exemple dans ce guide.
- Utilisation d'ARR IIS et de HAProxy
- Utilisation d'Application Gateway

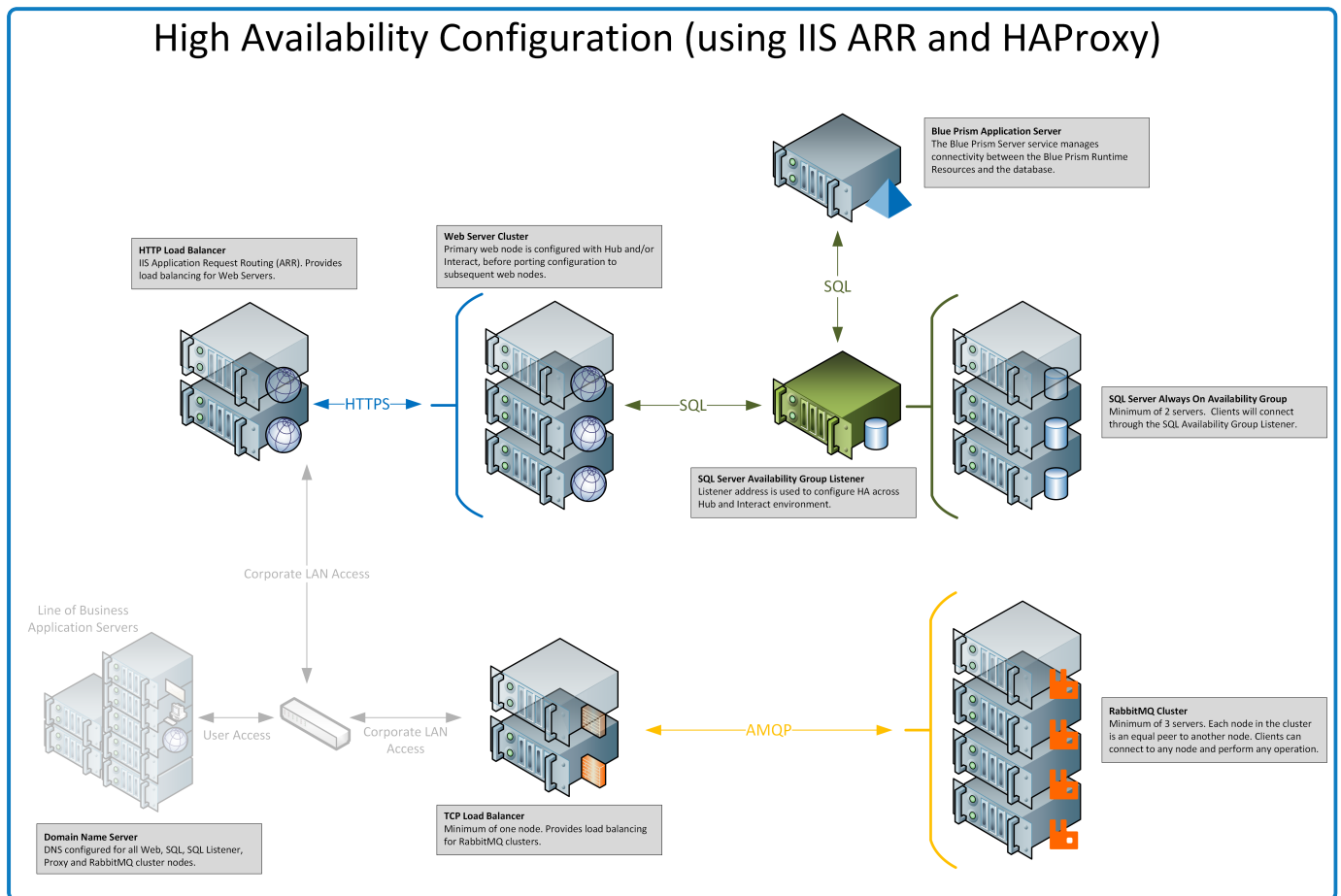
Configuration de haute disponibilité avec HAProxy



Les informations contenues dans ce guide utilisent cette configuration comme exemple.

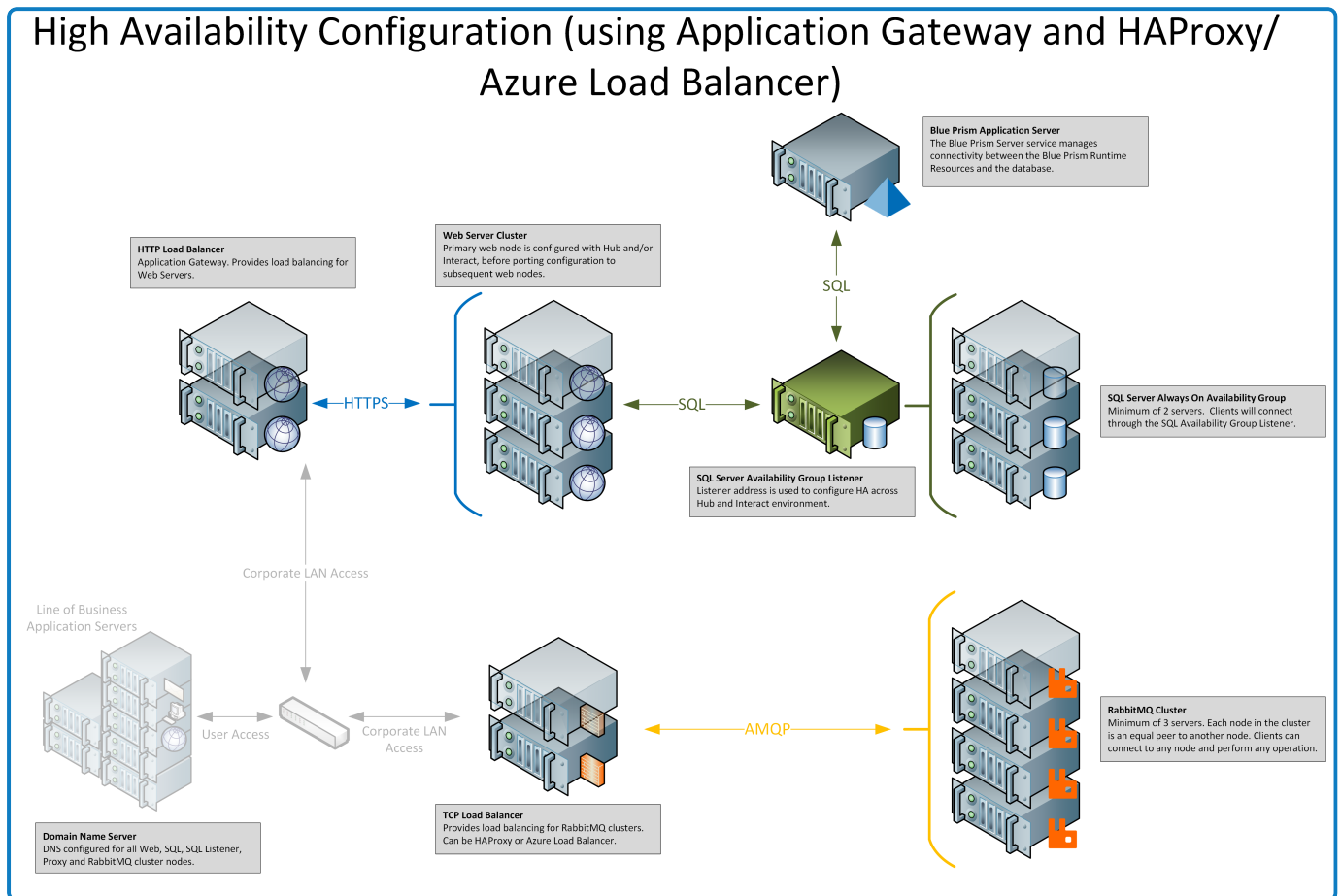
Configuration de haute disponibilité avec ARR IIS et HAProxy

High Availability Configuration (using IIS ARR and HAProxy)



Configuration de haute disponibilité avec Application Gateway

High Availability Configuration (using Application Gateway and HAProxy/ Azure Load Balancer)



Équilibreur de charge HAProxy – Exemple de configuration

Vous devriez utiliser l'équilibreur de charge le mieux adapté à votre organisation. Les informations ci-dessous fournissent un exemple de configuration pour un équilibreur de charge HAProxy (v2.4).

Dans cet exemple, Blue Prism a utilisé HAProxy v2.4 sur une machine Linux (spécification minimale : Ubuntu 20.04 avec 1 processeur virtuel et 2 Go de RAM).

Exemple de script d'équilibreur de charge (HAProxy)

Les exemples suivants ont recours à l'équilibreur de charge HAProxy (v2.4), qui utilise le fichier `/etc/haproxy/haproxy.cfg`.

Exemple de structure de script de base

```
global
    # global settings here

defaults
    # defaults here

frontend
    # a frontend that accepts requests from clients

backend
    # servers that fulfill the requests
```

Où :

- Les réglages sous l'en-tête `global` définissent les configurations de sécurité et de performance à l'échelle du processus qui affectent HAProxy à un niveau faible.
- L'utilisation d'une section `defaults` réduit la duplication. Les réglages s'appliquent à toutes les sections `frontend` et `backend` qui viennent après. Vous pouvez remplacer les réglages dans les sections qui suivent.
- Lorsque vous placez HAProxy en tant que proxy inverse devant vos serveurs principaux, une section `frontend` définit les adresses IP et les ports auxquels les clients peuvent se connecter.
- Une section `backend` définit un groupe de serveurs qui seront équilibrés en charge et affectés pour gérer les requêtes. Vous pouvez ajouter un libellé à chaque `backend`, par exemple « `web_servers` ».

Exemple de configuration



Consultez la version en ligne de l'exemple ci-dessous pour connaître le formatage correct.

```
#Example of HAPROXY config
#ANMQP loadbalancer for 3 nodes with IP-addresses 10.30.0.10,10.30.0.20,10.30.0.30
#HTTPS loadbalancer without SSL termination for 2 nodes with IP-addresses 10.30.0.50,10.30.0.60
#statistics is available at https://haproxyname.yourdomainname.com:10001/stats with adminname:adminpassword credits
global
    log /dev/log      local0
    log /dev/log      local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

    # Default SSL material locations
    ca-base /etc/ssl/certs
    crt-base /etc/ssl/private

    # See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0.3&config=intermediate
    ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDSA-AES128-GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-
    RSA-AES256-GCM-SHA384:ECDSA-CHACHA20-POLY1305:ECDSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-
    SHA384
```

```
ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets
```

defaults

```
log global
mode http
option httplog
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000
errorfile 400 /etc/haproxy/errors/400.http
errorfile 403 /etc/haproxy/errors/403.http
errorfile 408 /etc/haproxy/errors/408.http
errorfile 500 /etc/haproxy/errors/500.http
errorfile 502 /etc/haproxy/errors/502.http
errorfile 503 /etc/haproxy/errors/503.http
errorfile 504 /etc/haproxy/errors/504.http
```

frontend stats

```
bind *:10001 ssl crt /etc/haproxy/cert/yourdomainname.pem
mode http
stats enable
stats hide-version
stats refresh 10s
stats show-node
stats auth adminname:adminpassword
stats uri /stats
```

frontend main_frontend

```
bind *:443 ssl crt /etc/haproxy/cert/yourdomainname.pem
acl ims_acl hdr(host) -i ims.yourdomainname.com
acl hub_acl hdr(host) -i hub.yourdomainname.com
acl interact_acl hdr(host) -i interact.yourdomainname.com
acl audit_acl hdr(host) -i audit.yourdomainname.com
acl emailqueue_acl hdr(host) -i emailqueue.yourdomainname.com
acl fileserver_acl hdr(host) -i fileserver.yourdomainname.com
acl iada_acl hdr(host) -i iada.yourdomainname.com
acl interactremoteapi_acl hdr(host) -i interactremoteapi.yourdomainname.com
acl licensemanager_acl hdr(host) -i licensemanager.yourdomainname.com
acl notificationcenter_acl hdr(host) -i notificationcenter.yourdomainname.com
acl signalr_acl hdr(host) -i signalr.yourdomainname.com
use_backend ims_backend if ims_acl
use_backend hub_backend if hub_acl
use_backend interact_backend if interact_acl
use_backend audit_backend if audit_acl
use_backend emailqueue_backend if emailqueue_acl
use_backend fileserver_backend if fileserver_acl
use_backend iada_backend if iada_acl
use_backend interactremoteapi_backend if interactremoteapi_acl
use_backend licensemanager_backend if licensemanager_acl
use_backend notificationcenter_backend if notificationcenter_acl
use_backend signalr_backend if signalr_acl
```

frontend amqp_frontend

```
bind *:5672
mode tcp
option tcplog
use_backend amqp_backend
```

backend amqp_backend

```
mode tcp
balance roundrobin
server rabbit1 10.30.0.10:5672 check inter 5s
server rabbit2 10.30.0.20:5672 check inter 5s
server rabbit3 10.30.0.30:5672 check inter 5s
```

backend ims_backend

```
balance roundrobin
option httpchk
http-check send meth GET uri /health ver HTTP/1.1 hdr host ims.yourdomainname.com
http-check expect string Healthy
server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
```

backend hub_backend

```
balance roundrobin
option httpchk
http-check send meth GET uri /health ver HTTP/1.1 hdr host hub.yourdomainname.com
http-check expect string Healthy
server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
```

```
backend interact_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host interact.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend audit_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host audit.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend emailqueue_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host emailqueue.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend fileserver_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host fileserver.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend iada_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host iada.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend interactremoteapi_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host interactremoteapi.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend licensemanager_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host licensemanager.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend notificationcenter_backend
  balance roundrobin
  option httpchk
  http-check send meth GET uri /health ver HTTP/1.1 hdr host notificationcenter.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s

backend signalr_backend
  balance roundrobin
  option httpchk
  cookie SERVERID insert indirect nocache
  http-check send meth GET uri /health ver HTTP/1.1 hdr host signalr.yourdomainname.com
  http-check expect string Healthy
  server web1 10.30.0.50:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s cookie web1
  server web2 10.30.0.60:443 ssl ca-file /etc/haproxy/cert/root.ca check inter 5s cookie web2
```


Où :

- L'équilibreur de charge utilise des sections **frontend** distinctes pour chaque service, pour le cluster RabbitMQ et pour une page avec des statistiques.
- Pour activer la prise en charge SSL, HAProxy doit avoir des certificats dans le dossier **cert** situé dans **/etc/haproxy/cert/**.

- HAProxy envoie des requêtes à la page « /health » à intervalles de cinq secondes et attend la réponse « Healthy ».
- Le service SignalR utilise des sessions permanentes (les clients se fixent à un serveur unique).

Installation et configuration initiales


Avant d'exécuter les [scripts de haute disponibilité Blue Prism](#), vous devez installer et configurer un serveur Web initial avec Hub et, si nécessaire, Interact. Ce serveur Web sera ensuite utilisé pour répliquer la configuration aux serveurs Web supplémentaires dans votre configuration de haute disponibilité.

 L'utilisation de l'authentification Active Directory avec la configuration haute disponibilité n'est pas prise en charge.

Installer Blue Prism Hub

Avant d'utiliser les scripts, vous devez installer Hub sur l'un des serveurs Web, en suivant le [processus d'installation standard](#) avec les principales différences suivantes :

- Sur l'écran Prérequis 2 – RabbitMQ de l'assistant d'installation de Hub, dans le champ **Nom du serveur**, saisissez l'adresse de l'équilibreur de charge utilisé dans le cluster et non un nœud RabbitMQ individuel.

 N'utilisez pas les identifiants de compte invité RabbitMQ par défaut. Vous devez utiliser les identifiants pour un compte que vous avez créé dans RabbitMQ pour Hub.

- Sur les différents écrans de connexion SQL de l'assistant d'installation de Hub, dans le champ **Veillez sélectionner SQL Server.**, fournissez les détails pour l'auditeur de groupe de disponibilité et non un serveur SQL individuel. Assurez-vous également que les informations du champ **Nom de la base de données** correspondent au nom de base de données approprié que vous avez créé manuellement dans [Prérequis sur la page 5](#).
- Sur les différents écrans de configuration IIS de l'assistant d'installation de Hub, dans le champ **Nom d'hôte**, saisissez le nom d'hôte que vous avez spécifié dans la configuration de votre équilibreur de charge et sélectionnez le certificat approprié.

Si vous utilisez l'authentification Windows, vous devez vous assurer que vos comptes de service sont configurés pour accéder aux pools d'applications et aux certificats appropriés. Voir [Installer Hub à l'aide de l'authentification Windows](#) pour en savoir plus.

Installer Blue Prism Interact

Si Interact est requis, vous devez installer Interact avant d'utiliser les scripts, en suivant le [processus d'installation standard](#) avec les principales différences suivantes :

- Sur les différents écrans de connexion SQL de l'assistant d'installation d'Interact, dans le champ **Veillez sélectionner SQL Server.**, fournissez les détails pour l'auditeur de groupe de disponibilité et non un serveur SQL individuel. Assurez-vous également que les informations du champ **Nom de la base de données** correspondent au nom de base de données approprié que vous avez créé manuellement dans [Prérequis sur la page 5](#).
- Sur les différents écrans de configuration IIS de l'assistant d'installation d'Interact, dans le champ **Nom d'hôte**, saisissez le nom d'hôte que vous avez spécifié dans la configuration de votre équilibreur de charge et sélectionnez le certificat approprié.

Si vous utilisez l'authentification Windows, vous devez vous assurer que vos comptes de service sont configurés pour accéder aux pools d'applications et aux certificats appropriés. Voir [Installer Interact à l'aide de l'authentification Windows](#) pour en savoir plus.

Configurer votre installation

1. Configurez votre installation pour la première fois de manière standard. Voir [Configuration initiale de Hub](#) et [Installer le plug-in Interact](#).



Lors de la configuration des connexions de base de données, vous devez saisir les détails pour l'auditeur de groupe de disponibilité.

2. Installez et concédez sous licence tous les autres plug-ins utilisés par votre organisation, tels qu'Automation Lifecycle Management (ALM).
3. Une fois la configuration de l'environnement terminée, déconnectez-vous de Hub.


Solution scriptée

Une fois la [configuration du serveur Web initial](#) terminée, les scripts suivants peuvent être utilisés pour préparer l'hôte initial du serveur Web contenant Hub et Interact pour une haute disponibilité, et pour dupliquer cette configuration sur de nouveaux hôtes de serveur Web dans votre configuration de haute disponibilité.

Il existe trois scripts PowerShell qui doivent être exécutés dans l'ordre suivant :


| | Script | Description |
|----|-------------------------------|--|
| 1. | functions.ps1 | Un script contenant des fonctions PowerShell externes (utilisées par les deux autres scripts). |
| 2. | prepare.ps1 | Un script pour la préparation de l'hôte initial du serveur Web. |
| 3. | setup.ps1 | Un script pour configurer un hôte de serveur Web supplémentaire. |

Copiez ces scripts et l'outil de protection des données Blue Prism dans un dossier sur l'hôte du serveur Web initial, par exemple, C:\Scripts.

 Exécutez toujours PowerShell en tant qu'administrateur.


Informations importantes

- Lorsque vous transmettez des chaînes de connexion en tant que paramètres du script `prepare.ps1`, vous devez spécifier l'auditeur du groupe de disponibilité.
- Lorsque vous utilisez la méthode DNS recommandée, chaque nom d'hôte d'application doit pointer vers l'adresse IP privée de l'équilibreur de charge.

 Si DNS n'est pas disponible et que des fichiers hôtes sont utilisés, vous devrez mettre à jour le fichier **Hosts** sur chaque hôte de serveur Web.

- Après l'installation de Blue Prism Hub/Interact, l'option **Nécessite l'indication du nom du serveur** est activée par défaut dans les réglages de liaison Web pour chaque site sur le serveur Web initial. Cette option doit être :

- Désactivée : si vous avez plusieurs sites Web de sous-domaine qui partagent le même domaine et que vous utilisez un certificat générique ou un certificat unique pour tous les sous-domaines.

 Il s'agit de la configuration la plus courante de l'environnement Hub et Interact.

- Activée : si vous avez plusieurs sites Web de sous-domaine qui ne sont pas rattachés au même domaine, et un certificat différent pour chaque domaine.
- Activée : pour les sites Web de sous-domaine pertinents si vous avez plusieurs sous-domaines, dont certains sont rattachés au même domaine, et dont d'autres n'y sont pas rattachés.

Script Functions.ps1

Ce script stocke toutes les fonctions PowerShell utilisées par les scripts prepare.ps1 et setup.ps1.

Fonctions PowerShell

Le script functions.ps1 contient les fonctions PowerShell suivantes :

| Fonction PowerShell | Description |
|------------------------------|---|
| Convert-Guid | Convertit le GUID dans l'ID pour les chemins de registre où les informations d'installation Blue Prism Hub/Interact sont stockées. |
| Install-Dependencies | Simplifie l'installation des modules PowerShell et sélectionne le fournisseur d'ensemble logiciel. |
| Install-WinFeature | Installe les fonctionnalités Windows. |
| New-Site | Crée un site IIS et un pool d'applications, génère ou importe des certificats et définit des options de pool d'applications étendues. |
| New-HostedService | Crée des services Windows. |
| New-Password | Génère un mot de passe aléatoire avec des conditions prédéfinies. |
| Remove-HostedService | Supprime les services Windows. |
| Remove-Site | Supprime le site IIS et le pool d'applications. |
| Set-CertificatePrivateKeyAcl | Définit les permissions pour les clés privées de certificats installés pour les utilisateurs et les groupes. |
| Set-FolderPermissions | Définit les permissions pour les dossiers et les fichiers. |
| Set-Logging | Définit le niveau de logging pour les scripts. |


Exécuter le script Functions


Le script Functions.ps1 est appelé par le script Prepare.ps1 et n'a pas besoin d'être exécuté indépendamment. Voir [Script Prepare.ps1 sur la page suivante](#) pour plus d'informations sur l'exécution de ce script.

Script Prepare.ps1

Le script prepare.ps1 effectue toutes les préparations sur l'hôte initial du serveur Web où se trouvent les applications, telles qu'Authentication Server, Hub et Interact.

Le script prepare.ps1 doit d'abord être exécuté sur l'hôte du serveur Web initial (où Hub et Interact ont été installés à partir de l'assistant d'installation Blue Prism).

 Vous aurez également besoin de l'outil de protection des données Blue Prism dans votre dossier C:\Scripts. Pour plus d'informations sur cet outil, voir [Outil de protection des données Blue Prism](#).

 Le script prepare.ps1 génère des fichiers qui seront utilisés pour créer les serveurs Web supplémentaires. Le répertoire de sortie a une taille d'environ 800 Mo. Assurez-vous d'avoir au moins 1 Go d'espace disque libre avant d'exécuter ce script.

Fonctionnalités

Le script prepare.ps1 offre les fonctionnalités suivantes :

- Recueille des données à partir du registre et crée des fichiers de registre.
- Exporte les certificats.
- Prépare les applications et les services.
- Effectue les migrations de base de données.
- Modifie les propriétés dans le fichier appsettings.json.
- Comprime les dossiers racine des applications et des services.
- Génère le fichier variable.json et le remplit avec des données.

Paramètres

Le script prepare.ps1 contient les paramètres suivants :

| Paramètre | Description |
|----------------------------------|--|
| -HubCacheConnectionString | Spécifie la chaîne de connexion à la base de données Distributed Cache de Blue Prism Hub. Cela nécessite les détails de l'auditeur de groupe de disponibilité et le nom de la base de données que vous avez créée manuellement : HubCache. |
| -AuthServerCacheConnectionString | Spécifie la chaîne de connexion à la base de données Distributed Cache de Blue Prism Authentication Server. Cela nécessite les détails de l'auditeur de groupe de disponibilité et le nom de la base de données que vous avez créée manuellement : AuthenticationServerCache. |

| Paramètre | Description |
|--------------------------------|--|
| -InteractCacheConnectionString | Spécifie la chaîne de connexion à la base de données Cache de Blue Prism Interact. Cela nécessite les détails de l'auditeur de groupe de disponibilité et le nom de la base de données que vous avez créée manuellement : InteractCache. Ce paramètre doit être inclus si vous incluez également le paramètre -IncludeInteract . Cela n'est pas obligatoire si vous préparez uniquement Hub pour une haute disponibilité. |
| -DataProtectorPath | Spécifie le chemin d'accès complet à l'exécutable de l'outil de protection des données Blue Prism. |
| -IncludeInteract | Indique que vous devez rassembler les données et les fichiers de Blue Prism Interact à copier sur d'autres hôtes de serveur Web. Il s'agit d'un paramètre facultatif. Si ce paramètre n'est pas inclus, seul Hub sera affecté par le script. |

Exécuter le script Prepare

 Assurez-vous d'avoir au moins 1 Go d'espace disque libre avant d'exécuter ce script.

1. Sur l'hôte du serveur Web initial, exécutez PowerShell en tant qu'administrateur et modifiez le répertoire dans le dossier où les scripts sont stockés, par exemple :

```
cd C:\Scripts
```

2. Exécutez le script Prepare : vous devez spécifier les détails des paramètres répertoriés dans [Paramètres sur la page précédente](#). Voici quelques exemples de scripts :

Si vous avez à la fois Blue Prism Hub et Blue Prism Interact installés et que vous utilisez l'authentification SQL :

```
.\prepare.ps1 `
-HubCacheConnectionString 'Server=aglistener.domain.local;Database=HubCache;User
Id=sqladmin;Password=StR0nGP@ssw0rD;MultiSubnetFailover=True;' `
-AuthServerCacheConnectionString 'Server=aglistener.domain.local;Database=AuthenticationServerCache;User
Id=sqladmin;Password=StR0nGP@ssw0rD;MultiSubnetFailover=True;' `
-InteractCacheConnectionString 'Server=aglistener.domain.local;Database=InteractCache;User
Id=sqladmin;Password=StR0nGP@ssw0rD;MultiSubnetFailover=True;' `
-DataProtectorPath '.\BluePrismDataProtector.Console.exe' `
-IncludeInteract
```

Si vous n'avez installé que Blue Prism Hub et que vous utilisez l'authentification SQL :

```
.\prepare.ps1 `
-HubCacheConnectionString 'Server=aglistener.domain.local;Database=HubCache;User
Id=sqladmin;Password=StR0nGP@ssw0rD;MultiSubnetFailover=True;' `
-AuthServerCacheConnectionString 'Server=aglistener.domain.local;Database=AuthenticationServerCache;User
Id=sqladmin;Password=StR0nGP@ssw0rD;MultiSubnetFailover=True;' `
-DataProtectorPath '.\BluePrismDataProtector.Console.exe'
```

Si vous avez à la fois Blue Prism Hub et Blue Prism Interact installés et que vous utilisez l'authentification Windows :

```
.\prepare.ps1 `
-HubCacheConnectionString 'Server=aglistener.domain.local;Database=HubCache;Integrated
Security=True;MultiSubnetFailover=True;' `
-AuthServerCacheConnectionString 'Server=aglistener.domain.local;Database=AuthenticationServerCache;Integrated
Security=True;MultiSubnetFailover=True;' `
-InteractCacheConnectionString 'Server=aglistener.domain.local;Database=InteractCache;Integrated
Security=True;MultiSubnetFailover=True;' `
-DataProtectorPath '.\BluePrismDataProtector.Console.exe' `
-IncludeInteract
```

Si vous n'avez installé que Blue Prism Hub et que vous utilisez l'authentification Windows :

```
.\prepare.ps1 `
-HubCacheConnectionString 'Server=aglistener.domain.local;Database=HubCache;Integrated
Security=True;MultiSubnetFailover=True;' `
-AuthServerCacheConnectionString 'Server=aglistener.domain.local;Database=AuthenticationServerCache;Integrated
Security=True;MultiSubnetFailover=True;' `
-DataProtectorPath '.\BluePrismDataProtector.Console.exe'
```

Après avoir exécuté le script prepare.ps1, vous aurez :

- Un dossier Fichiers avec du contenu d'application compressé, des certificats et des fichiers de registre est désormais stocké dans le dossier Scripts.
 - Un fichier variables.json dans le dossier Scripts avec toutes les valeurs nécessaires pour chaque script.
3. Copiez l'intégralité du dossier Scripts sur l'hôte initial du serveur Web sur chaque hôte de serveur Web supplémentaire en utilisant la même structure de répertoire, par exemple, C:\Scripts.
- Voir [Script Setup.ps1 sur la page suivante](#) pour l'étape suivante.


Script Setup.ps1

Le script setup.ps1 effectue la configuration des applications préparées par le script prepare.ps1.

Le script setup.ps1 doit être exécuté sur chaque hôte de serveur Web supplémentaire qui sera dans votre configuration de haute disponibilité. Les hôtes du serveur Web doivent être configurés avec le logiciel prérequis, comme détaillé dans [Prérequis sur la page 5](#).

Après avoir exécuté le script setup.ps1, vous aurez :

- importé des certificats et des fichiers de registre.
- installé toutes les fonctionnalités et tous les rôles Windows nécessaires.
- créé et configuré toutes les applications et tous les services à partir de l'hôte du serveur Web initial.

 Le script setup.ps1 ne doit être exécuté qu'après avoir terminé les étapes requises pour [Script Prepare.ps1 sur la page 18](#).

Fonctionnalités

Le script setup.ps1 fournit les fonctionnalités suivantes :


- Importe les fichiers de registre.
- Importe les certificats.
- Définit les permissions pour les clés privées de certificat.
- Installe les fonctionnalités et rôles Windows.
- Crée une structure de dossiers et extrait le contenu des applications.
- Crée des sites IIS pour toutes les applications précédemment exportées.
- Crée des services Windows pour tous les services précédemment exportés.

Paramètres

Le script setup.ps1 contient les paramètres suivants :

| Paramètre | Description |
|-----------|--|
| -Force | Force la recréation de tous les sites et services. |

Exécuter le script Setup

 Avant d'exécuter le script, assurez-vous d'avoir copié C:\Scripts du serveur Web initial vers celui-ci. Vous devez également vous assurer que vous disposez d'au moins 1 Go d'espace disque libre.

1. Si vous ne l'avez pas déjà fait, copiez le dossier contenant les scripts et les fichiers (C:\Scripts) du serveur Web initial vers ce serveur Web.
2. Exécutez PowerShell en tant qu'administrateur et modifiez le répertoire pour le dossier dans lequel les scripts et les fichiers ont été copiés, par exemple :


```
cd C:\Scripts
```

3. Exécutez le script Setup : vous n'avez pas besoin de spécifier de paramètres supplémentaires, par exemple :

```
.\setup.ps1
```

Le script prend un certain temps à s'exécuter, car il construit le serveur Web.

4. Répétez ce processus sur tous les serveurs Web supplémentaires qui doivent être configurés.

 Si vous avez rencontré une erreur lors de l'exécution du script setup.ps1, vous pouvez l'exécuter à nouveau à l'aide du paramètre -Force :

```
.\setup.ps1 -Force
```

Tester votre environnement de haute disponibilité

Une fois que vous avez terminé la configuration de votre environnement de haute disponibilité, vous devez tester qu'il fonctionne comme prévu en cas de défaillance.

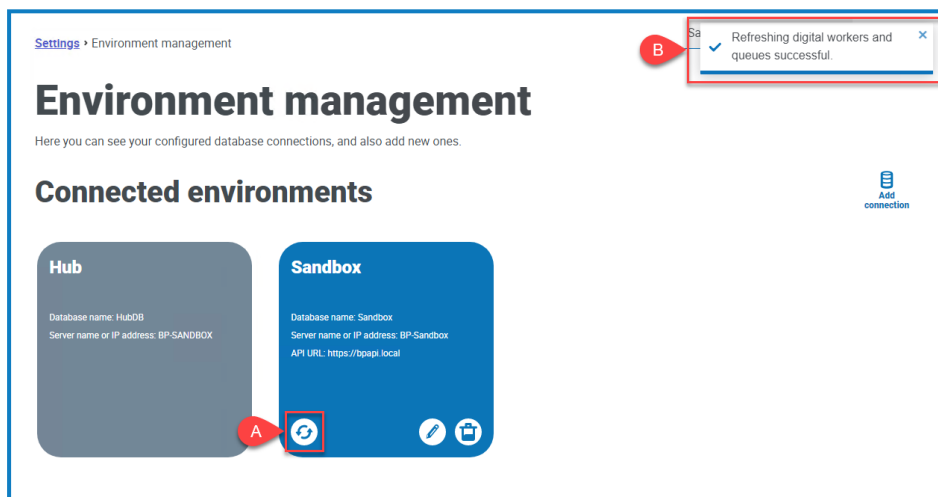
Pour ce faire :

1. Vérifiez que l'environnement de haute disponibilité fonctionne initialement comme prévu :
 - a. Connectez-vous à Blue Prism Hub en tant qu'administrateur Hub, cliquez sur l'icône de profil en forme de prisme, puis sur **Gestion des environnements** sur la page Réglages.

La page Gestion des environnements s'affiche.

- b. Cliquez sur l'icône Actualiser (A) sur la dalle de la base de données Blue Prism pour mettre à jour les files d'attente et les informations dans l'environnement Hub.

Le message *Actualisation des travailleurs numériques et des files d'attente réussie* s'affiche (B).



Laissez cette fenêtre du navigateur Web ouverte tout au long de ce processus de test.

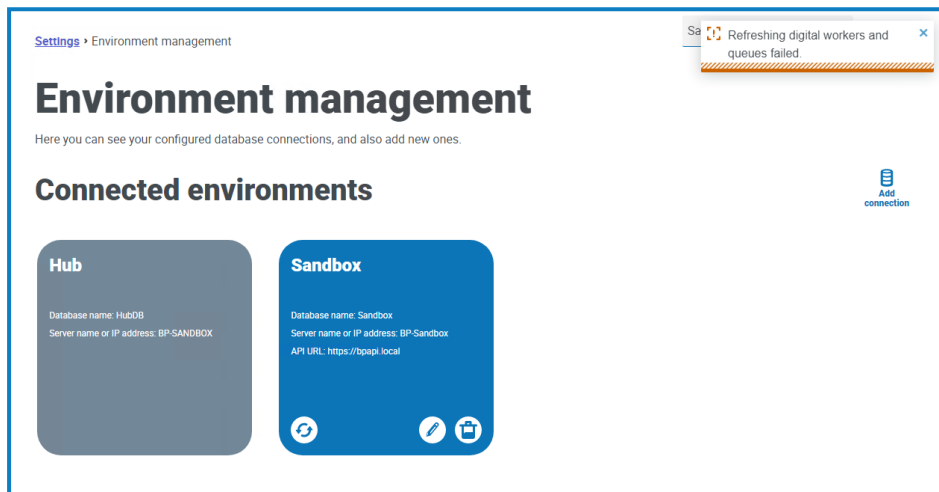
2. Simuler une défaillance de serveur :
 - a. Sur l'un des serveurs Web supplémentaires du cluster, ouvrez le gestionnaire Internet Information Services (IIS) et arrêtez le serveur. Cela simule une défaillance du serveur.
 - b. Revenez à la fenêtre de votre navigateur Web avec la page du gestionnaire d'environnement Hub affichée et cliquez à nouveau sur l'icône Actualiser.

Il peut y avoir un délai légèrement plus long pour actualiser les informations, car la communication est rétablie, avant que le message *Actualisation des travailleurs numériques et des files d'attente réussie* ne s'affiche.

3. Simuler un redémarrage de serveur et une défaillance de serveur différente :

- a. Dans le gestionnaire Internet Information Services (IIS), démarrez le serveur Web qui a été arrêté à l'étape 2a.
- b. Sur le serveur Web initial (le premier serveur) dans le cluster, ouvrez le gestionnaire Internet Information Services (IIS) et arrêtez le serveur.
- c. Revenez à la fenêtre de votre navigateur Web avec la page du gestionnaire d'environnement Hub affichée et cliquez à nouveau sur l'icône Actualiser.

Un message d'échec de l'actualisation s'affiche. La défaillance est due à un retard dans l'équilibrage de charge après la commutation des serveurs.



- d. Attendez quelques secondes, puis cliquez à nouveau sur l'icône Actualiser.

Le message Actualisation réussie s'affiche. Si vous voyez toujours le message d'échec de l'actualisation, répétez cette étape.

4. Terminer le test :

- a. Dans le gestionnaire Internet Information Services (IIS), démarrez le serveur Web qui a été arrêté à l'étape 3b.

Logging

Les fichiers log sont créés suite à l'exécution de ces scripts. Les fichiers log sont créés au format suivant :

<DISQUE DU SYSTÈME>\<NOM D'HÔTE DU SERVEUR>.log

par exemple : C:\webserver.log.