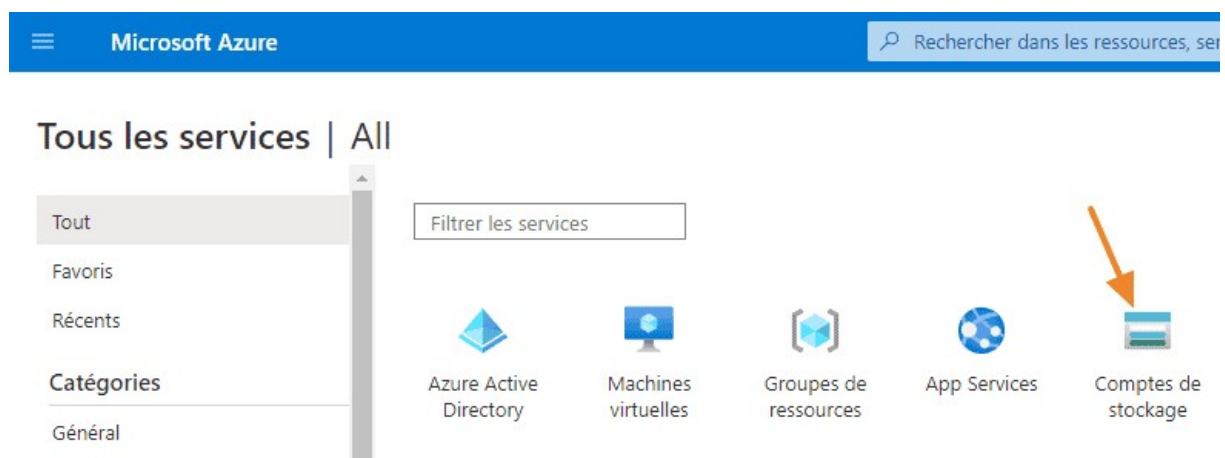


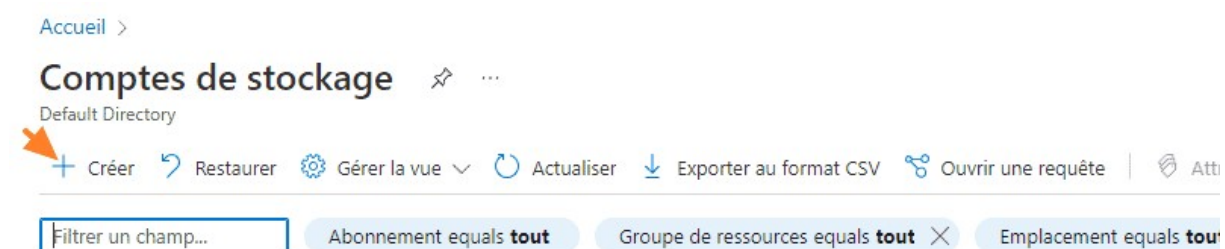
TPs et Labs Azure Mardi

Azure Files : Création d'un partage SMB dans Azure

Pour accéder à la fonctionnalité "**Partage de fichiers**" d'Azure, il est nécessaire de disposer d'un compte de stockage. À partir du portail Azure, il faut rechercher le service "**Comptes de stockage**" pour créer un compte.




Le bouton "**Créer**" sert à lancer l'assistant de création d'un compte de stockage.





Ensuite, il faut nommer ce compte de stockage (sans espace ni caractères spéciaux, avec des minuscules et des chiffres), choisir la région, ainsi que les options liées aux performances. Il est à noter qu'il est possible de créer un partage avec une capacité maximale de 5 To ou de 100 To. Pour être en mesure de choisir 100 To, le partage doit être redondant en local uniquement (LRS), car si l'on prend l'option géo-redondant, on est limité à 5 To par partage, ce qui est déjà intéressant.

Détails du projet

Sélectionnez l'abonnement dans lequel créer le compte de stockage. Choisissez un groupe de ressources nouveau ou existant pour organiser et gérer votre compte de stockage avec d'autres ressources.



Abonnement * 



Groupe de ressources *  (Nouveau) IT-Connect_Partage 

[Créer nouveau](#)

Détails de l'instance

Si vous devez créer un type de compte de stockage hérité, cliquez sur [ici](#).



Nom du compte de stockage ⓘ *  partageazurefiles 

Région ⓘ *  (Europe) France Central 

Performances ⓘ *

☒ Standard: Recommandé pour la plupart des scénarios (compte universel v2)

☐ Premium: Recommandé pour les scénarios nécessitant une faible latence.

Redondance ⓘ *  Stockage géoredondant (GRS) 

☒ Proposez l'accès en lecture sur les données en cas d'indisponibilité régionale.

Vérifier + créer

< Précédent

Suivant : Avancé >

Les options liées au réseau permettent de limiter les accès à ce partage : est-ce qu'il doit être accessible publiquement (avec authentification, bien sûr), ou uniquement à partir de certains réseaux.

Créer un compte de stockage ...

Informations de base

Avancé

Réseau

Protection des données

Chiffrement

Étiquettes


Vérifier + créer

Connectivité réseau

Vous pouvez vous connecter à votre compte de stockage de manière publique, via des adresses IP publiques ou des points de terminaison de service, ou en mode privé à l'aide d'un point de terminaison privé.

Accès réseau *

- ☒ Activez l'accès public à partir de tous les réseaux
- ☐ Activer l'accès public à partir de réseaux virtuels et d'adresses IP sélectionnés
- ☐ Désactivez l'accès public et utilisez l'accès privé

 L'activation de l'accès public à partir de tous les réseaux peut rendre cette ressource disponible publiquement. À moins que l'accès public ne soit requis, nous vous recommandons d'utiliser un type d'accès plus restreint. [En savoir plus](#)

Routage réseau

Déterminez la façon dont votre trafic est routé entre sa source et son point de terminaison Azure. Le routage réseau Microsoft est recommandé pour la plupart des clients.

Préférence de routage ⓘ *

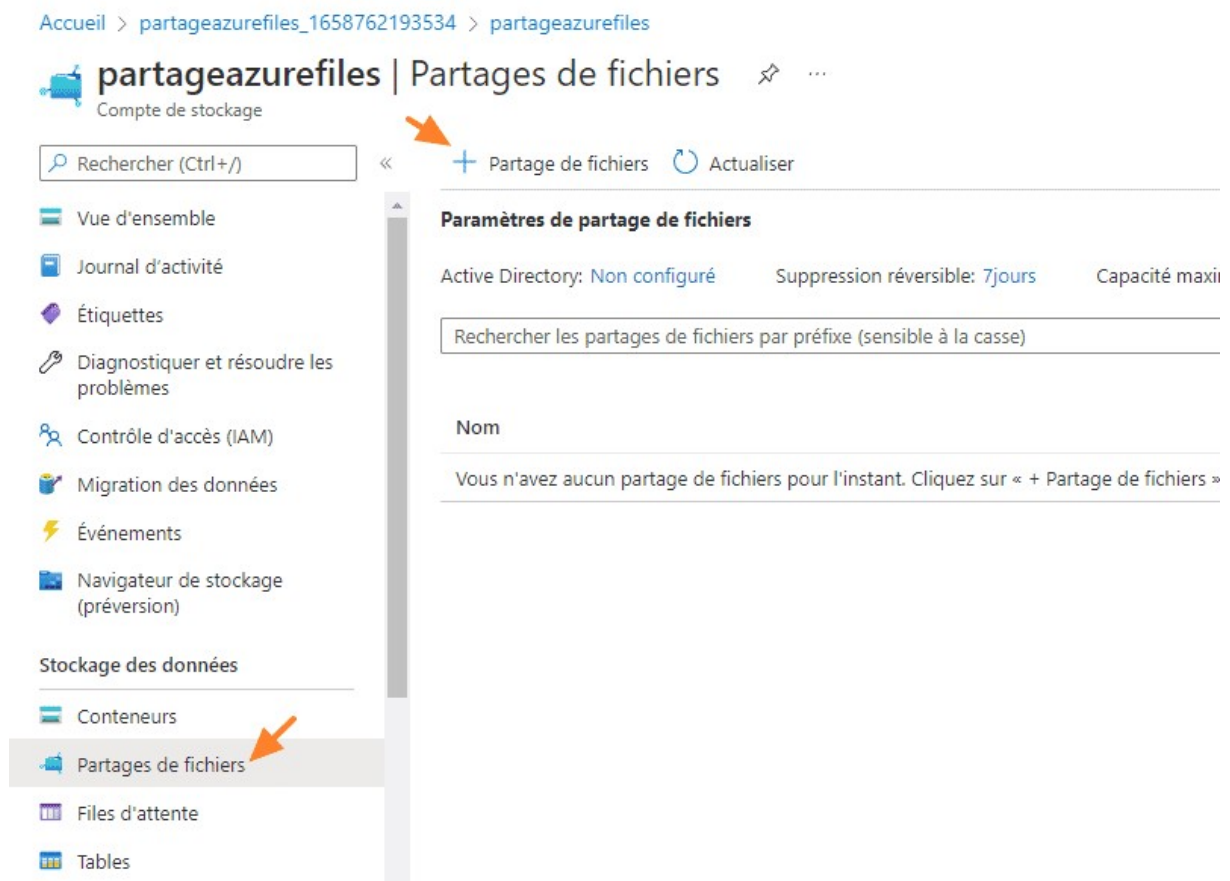
- ☒ Routage réseau Microsoft
- ☐ Routage Internet

Vous pouvez également parcourir les autres options des différents onglets, avant d'arriver à l'étape finale : le clic sur le bouton "**Créer**". Parfois, ce bouton reste grisé une ou deux minutes, le temps de la validation de la configuration (c'est indiqué en haut de la page).



III. Créer un partage Azure Files

Dès que la ressource Azure est créée, nous pouvons y accéder afin de poursuivre la configuration. Une fois dans la ressource, cliquez à gauche sur "**Partages de fichiers**" puis sur le bouton "**Partage de fichiers**" pour créer un nouveau partage.



Ce partage doit être configuré. Cela consiste à attribuer un nom, comme ici "**partage**" tout simplement. Le champ "**Niveau**" est important, car **il détermine le niveau de performances de l'espace de stockage, ce qui impactera le coût directement**. Ici, on est clairement sur la notion de stockage chaud / froid. Selon ce que vous souhaitez faire avec ce partage, il peut être intéressant financièrement de commencer sur un niveau et de le changer par la suite.

Voici ce que précise Microsoft : "*Les coûts de transaction sont plus élevés sur les niveaux plus froids. Il est souvent plus économique de commencer votre partage au niveau Transaction optimisée si vous prévoyez de migrer un plus grand nombre de fichiers. Une fois la migration effectuée, vous pouvez définir le partage sur un niveau plus froid.*"

Le mode "**Transaction optimisée**" est un mode équilibré, qui n'est pas le plus performant (il y a le mode "**Premium**"), mais qui peut suffire pour le stockage des données d'une application. Pour une utilisation plus intensive ou une synchronisation avec Azure File Sync, il faut partir sur le mode "**Chaud**".

Une fois les différents champs renseignés, cliquez sur "**Créer**".

Nouveau partage de fichiers ✕

Nom * ✓


partage


Niveau ⓘ

Transaction optimisée ▼


Performances

Nombre maximal d'e/s par seconde ⓘ	1000
Débit de sortie ⓘ	60 Mio/s
Débit d'entrée ⓘ	60 Mio/s
Capacité maximale	5 Tio
Grands partages de fichiers	Disabled

 Vous pouvez améliorer les performances et la capacité maximale de partage en activant des partages de fichiers importants pour ce compte de stockage. [En savoir plus](#)

 Pour utiliser le protocole SMB avec ce partage, vérifiez si vous pouvez communiquer via le port 445. Ces scripts pour [Clients Windows](#) et [Clients Linux](#) peuvent vous aider. Découvrez comment [contourner les problèmes liés au port 445](#).

Le nouveau partage vient s'ajouter à la liste des partages associés à ce compte de stockage. Vous remarquerez l'option "**Sécurité: Compatibilité maximale**" qui permet de choisir les versions du SMB autorisées, les types d'authentification, etc... Le mode "**Sécurité maximale**" utilise uniquement les versions et algorithmes les plus sécurisés : je vous le recommande si votre environnement le prend en charge. Vous pouvez aussi créer un mode personnalisé : ces options sont modifiables à tout moment.

 Sécurité: Compatibilité maximale

Modifié


25/07/2022 17:19:29

Sécurité ✕


Paramètres du protocole

Azure Files expose des paramètres qui vous permettent d'activer/désactiver le protocole SMB pour être plus compatible ou plus sécurisé, en fonction des exigences de votre organisation. La restriction de ces paramètres peut empêcher certains clients de se connecter. [En savoir plus](#)

Profil

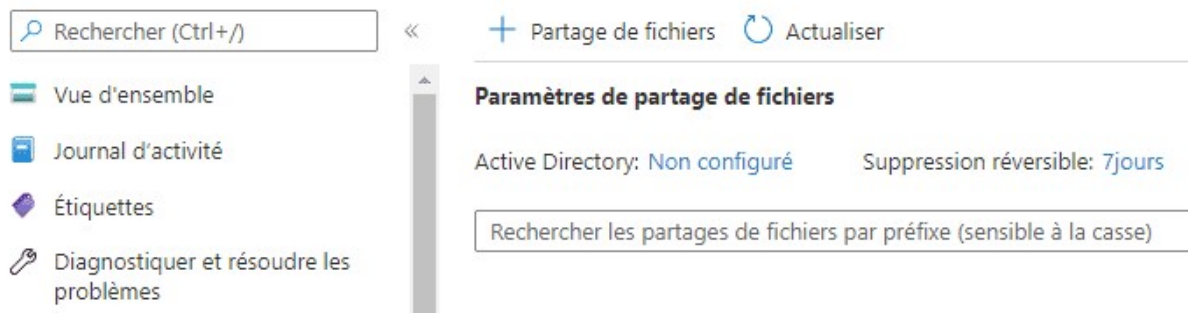
Sécurité maximale ▼ 

Versions du protocole SMB <ul style="list-style-type: none"> <input type="checkbox"/> SMB 2.1 <input type="checkbox"/> SMB 3.0 <input checked="" type="checkbox"/> SMB 3.1.1 	Chiffrement du canal SMB <ul style="list-style-type: none"> <input type="checkbox"/> Aucun <input type="checkbox"/> AES-128-CCM <input type="checkbox"/> AES-128-GCM <input checked="" type="checkbox"/> AES-256-GCM
Mécanismes d'authentification <ul style="list-style-type: none"> <input type="checkbox"/> NTLM v2 <input checked="" type="checkbox"/> Kerberos 	Chiffrement du ticket Kerberos <ul style="list-style-type: none"> <input type="checkbox"/> RC4-HMAC <input checked="" type="checkbox"/> AES-256

 Pour plus d'informations sur la prise en charge des paramètres de protocole dans les clients SMB, consultez [SMB sur Windows](#) et [SMB sur Linux](#).

D'autres options sont disponibles pour les partages, dont l'authentification basée sur l'Active Directory (on-premise) ou Azure Active Directory Domain Services. Cela permet d'avoir une **authentification par utilisateur sur le partage**.

Par ailleurs, l'option "**Suppression réversible**" définie à 7 jours indique que l'on peut **recupérer un fichier jusqu'à 7 jours après sa suppression**. Cette option peut être désactivée ou l'on peut changer la valeur : de 1 à 365 jours. Là encore, c'est aussi une question de coût.



IV. Monter le partage Azure Files sur Windows

Notre partage est prêt, nous pouvons le **monter sur une machine client sous Windows**, voire même sous Linux ou macOS en utilisant la procédure adaptée à chaque système. Comme je le disais précédemment, on peut s'appuyer sur l'authentification Active Directory si elle est configurée (pour un AD local, cela implique d'utiliser [Azure AD Connect](#)) ou sur une authentification intégrée à Azure via l'option "**Clé du compte de stockage**".

En fait, il faut **choisir la lettre de lecteur à associer au lecteur réseau**, la méthode d'authentification et copier le bout de code PowerShell indiqué dans la fenêtre. Ce bout de code intègre l'adresse du partage, mais aussi le nom d'utilisateur (*localhost\partageazurefiles*) et le mot de passe - très long - associé à ce compte.

e quota

Connecter

partage

⚠ L'option « Transfert sécurisé obligatoire » est activée sur le compte de stockage. Les clients SMB qui se connectent à ce partage doivent prendre en charge le protocole SMB version 3 ou ultérieure pour pouvoir répondre aux conditions de chiffrement. Cliquez ici pour en savoir plus.

Windows Linux macOS

Pour vous connecter à ce partage de fichiers Azure à partir de Windows, choisissez une des méthodes d'authentification suivantes et exécutez les commandes PowerShell à partir d'un terminal PowerShell normal (sans élévation de privilèges) :

Lettre de lecteur

P

Méthode d'authentification

- ☐ Active Directory
- ☒ Clé du compte de stockage

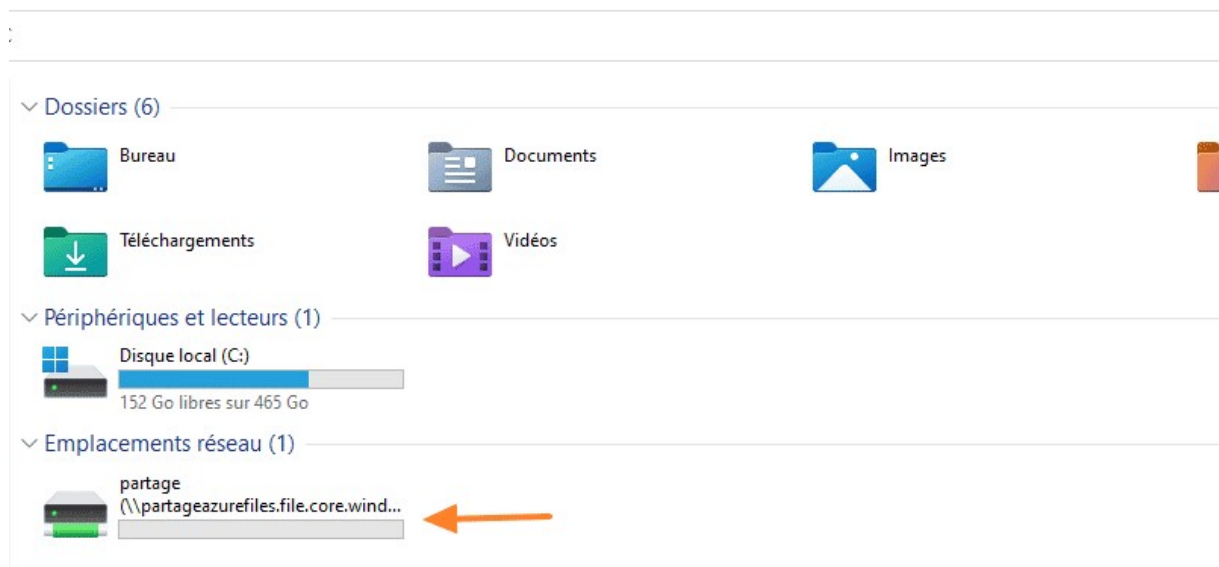
i Une connexion à un partage à l'aide de la clé de compte de stockage n'est appropriée que pour un accès administrateur. Un montage du partage de fichiers Azure avec l'identité Active Directory de l'utilisateur est préférable. [En savoir plus](#)

```
$connectTestResult = Test-NetConnection -ComputerName  
partageazurefiles.file.core.windows.net -Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Enregistrer le mot de passe pour rendre le lecteur persistant au redémarrage  
    cmd.exe /C "cmdkey /add:"partageazurefiles.file.core.windows.net"  
/user:"localhost\partageazurefiles"  
/pass:"zqKdO31S4xbboB29tQRxjEC9qgOE87ElHxxquWx/KsqQCLv+pJNaNm4iyk8O"
```

Après avoir collé ce bout de code dans une console PowerShell, j'obtiens le résultat suivant qui laisse penser le partage s'est monté correctement.

```
Windows PowerShell  
Copyright (C) Microsoft Corporation. Tous droits réservés.  
  
Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows  
  
PS C:\Users\Florian> $connectTestResult = Test-NetConnection -ComputerName partageazurefiles.file.core.windows.net -Port  
445  
PS C:\Users\Florian> if ($connectTestResult.TcpTestSucceeded) {  
>> # Enregistrer le mot de passe pour rendre le lecteur persistant au redémarrage  
>> cmd.exe /C "cmdkey /add:"partageazurefiles.file.core.windows.net" /user:"localhost\partageazurefiles" /pass:'  
"zqKdO31S4xbboB29tQRxjEC9qgOE87ElHxxquWx/KsqQCLv+pJNaNm4iyk8O"  
>> # Monter le lecteur  
>> New-PSDrive -Name P -PSProvider FileSystem -Root "\\partageazurefiles.file.core.windows.net\partage" -Persist  
>> } else {  
>> Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organizatio  
n or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a di  
fferent port."  
>> }  
  
CMDKEY: les informations d'identification ont été ajoutées correctement.  
  
Name          Used (GB)  Free (GB) Provider      Root                                          CurrentLocation  
-----  
P              0,00      5120,00 FileSystem     \\partageazurefiles.file.core.wi...  
  
PS C:\Users\Florian> |
```

Nous pouvons le vérifier à partir de l'Explorateur de fichiers de Windows, comme ceci :



Il est à noter que si l'on crée des dossiers ou que l'on dépose des fichiers dans ce partage, ils sont directement envoyés sur Azure. Ces données sont visibles sur l'interface d'Azure. En fait, vous pouvez créer ou supprimer un dossier à partir d'Azure pour structurer le partage, ou le faire directement à partir du poste client, mais aussi charger des fichiers.

Périphériques et lecteurs

- OS (C:)
- DATA (D:)
- Nouveau nom (E:)
- backup (G:)
- data03 (Q:)
- VHDX (X:)

Emplacements réseau

- Wireshark-win64-3.4.8.exe
- data (\\storage1974.file.core.windows.net) (Z:)

Utilisation d'Azure Bastion pour se connecter à ses VM

Nous allons apprendre à mettre en place un Bastion dans Azure de manière à bénéficier d'un accès sécurisé à une ou plusieurs machines virtuelles Azure. Cet accès sécurisé est possible sur les serveurs Windows et Linux, aussi bien en RDP qu'en SSH.

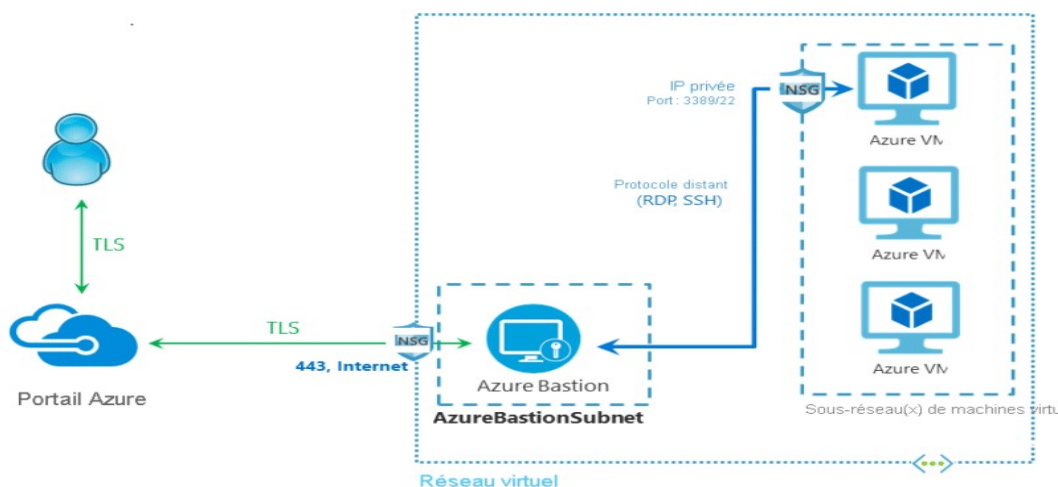
la mise en place d'un bastion est intéressante à partir du moment où l'on a des machines virtuelles dans Azure, et que l'on souhaite avoir un accès sécurisé sans avoir une adresse IP publique sur les VMs. Ici, l'adresse IP publique est hébergée par le Bastion, et ce dernier contrôle les connexions aux machines virtuelles.

Pour se connecter à des machines virtuelles Azure, il y a plusieurs solutions qui dépendent aussi de votre infrastructure : hybride entre du Cloud et du on-premise ? Full Cloud ? Etc... Parmi les possibilités pour se connecter à ses VMs Azure, il y a l'attribution d'une adresse IP publique sur chaque VM (avec les risques que cela comporte) ou encore la mise en place d'un VPN site-à-site (ou ExpressRoute) entre son infrastructure locale et l'infrastructure Azure. Néanmoins, ce n'est pas recommandé d'attribuer une adresse IP publique sur chacune de vos VMs, car elles se retrouvent directement exposées. La surface d'attaque est étendue de manière dangereuse et il est plus difficile de gérer les accès (chaque configuration étant indépendante, les connexions journalisées indépendamment, etc.).

Grâce à la solution Azure Bastion, pleinement intégrée à Azure sous la forme d'un service PaaS et développée par Microsoft, notre Bastion servira de point d'entrée unique pour accéder à nos machines virtuelles. Toutes les connexions à destination des machines virtuelles associées au Bastion seront gérées par ce même Bastion, qui au passage, assure une protection contre les différentes attaques.

La connexion aux machines virtuelles Windows et Linux est effectuée au travers des protocoles RDP et SSH, sans avoir besoin d'utiliser un logiciel spécifique sur son ordinateur : un navigateur compatible HTML5 suffit, ainsi qu'un accès au portail Azure.

Ci-dessous, le schéma de principe mis en ligne par Microsoft.



Pour mettre en place Azure Bastion, il y a deux licences (SKUs) différentes : "De base" et "Standard". La version standard est plus évoluée, car elle intègre quelques fonctionnalités supplémentaires. De ce fait, elle est également plus coûteuse que la version "De base" avec un coût horaire qui est plus élevé. Ci-dessous, un tableau comparatif des fonctionnalités, ce qui pourra évoluer dans le temps.

Références (SKU)

Azure Bastion présente deux références SKU disponibles : de base et standard. Pour plus d'informations, notamment sur la mise à niveau d'une référence SKU, consultez l'article [Paramètres de configuration](#).

La table suivante présente les fonctionnalités et les références SKU correspondantes.

Fonctionnalité	Référence SKU De base	Référence SKU standard
Se connecter pour cibler les machines virtuelles dans les réseaux virtuels appairés	Oui	Oui
Accéder aux clés privées des machines virtuelles Linux dans Azure Key Vault (AKV)	Oui	Oui
Se connecter à une machine virtuelle Linux avec SSH	Oui	Oui
Se connecter à une machine virtuelle Windows avec RDP	Oui	Oui
Sortie audio de la machine virtuelle	Oui	Oui
Mise à l'échelle de l'hôte	Non disponible	Oui
Spécifier le port d'entrée personnalisé	Non disponible	Oui
Se connecter à une machine virtuelle Linux avec RDP	Non disponible	Oui
Se connecter à une machine virtuelle Windows avec SSH	Non disponible	Oui
Charger ou télécharger des fichiers	Non disponible	Oui
Désactiver le copier/coller (clients web)	Non disponible	Oui

Le coût d'Azure Bastion dépend du type de SKU retenu. Il y a un coût à l'heure (à partir de 0,198€ par heure), auquel il faut ajouter la consommation en termes de "Transfert de données sortantes" tout en sachant que chaque mois les 5 premiers Go sont offerts. Il faut avoir conscience que le Bastion est très intéressant en matière de sécurité, mais qu'il y a un coût à l'usage qui n'est pas négligeable.

Azure Bastion - Tarifs

La présentation étant faite, passons à la configuration d'Azure Bastion. Finalement, ce service intégré à Azure reprend le principe du bastion en matière de sécurité informatique.

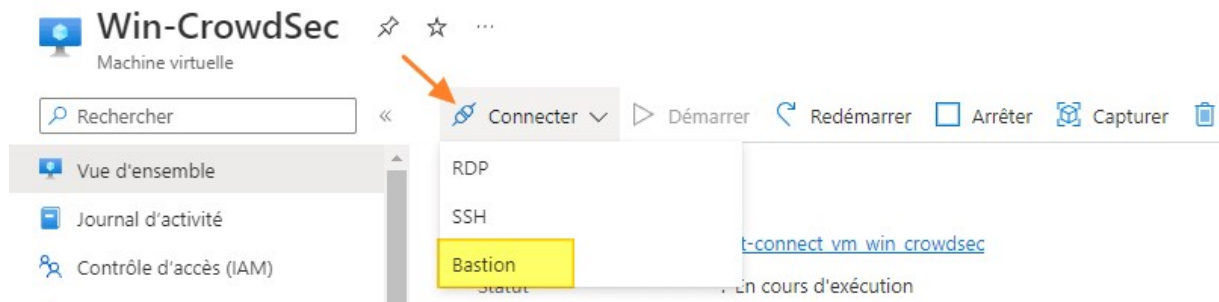
III. Configuration d'Azure Bastion

Pour créer un Bastion à partir du portail Azure, il y a deux possibilités : le configurer au sein d'une machine virtuelle, ou le configurer à partir de la section "Bastions" du portail Azure.

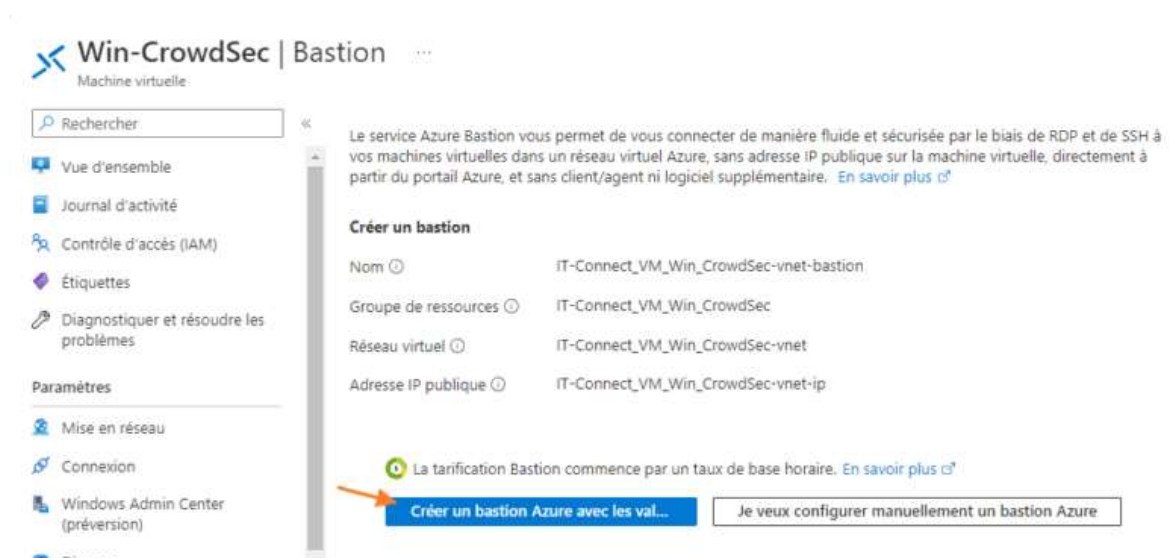
A. Configurer un accès bastion pour une VM

Prenons le cas où l'on souhaite activer un bastion uniquement pour accéder à une seule VM. Cela s'effectue en quelques clics : on sélectionne la VM dans le portail Azure, puis dans "Vue d'ensemble", on clique sur "Connecter" puis on sélectionne "Bastion".

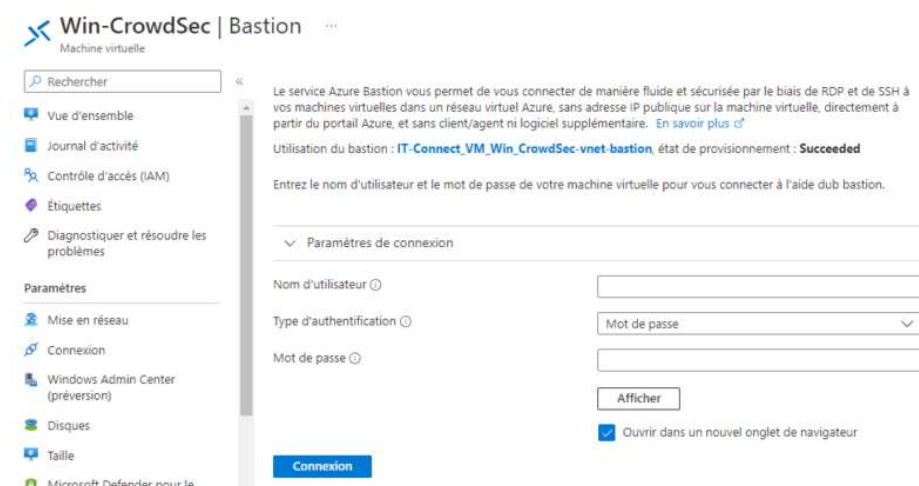
Azure - Bastion pour une VM



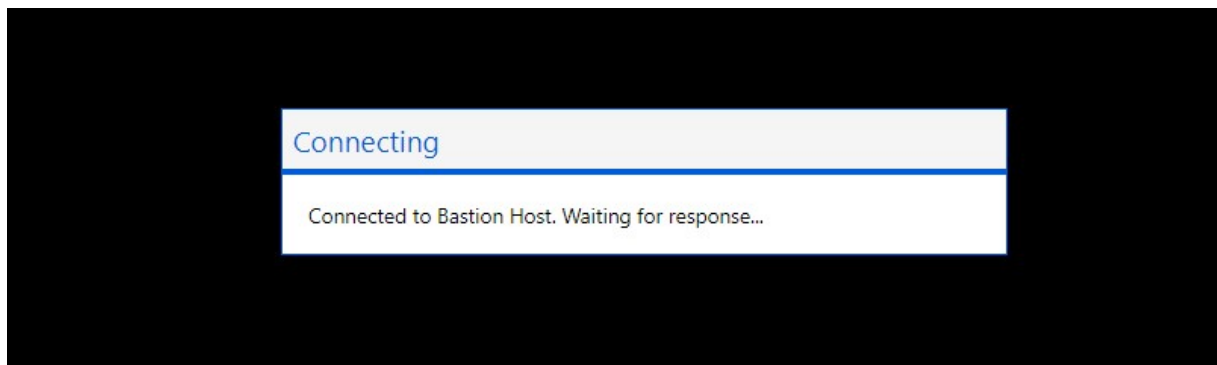
Ici, on a le choix entre créer un bastion avec la configuration par défaut (ce qui va générer un réseau virtuel, un groupe de ressources, etc...) ou avec une configuration manuelle (ce que l'on verra dans un second temps). La création du Bastion en mode automatique, c'est-à-dire avec les valeurs par défaut, prend environ 10 minutes dès lors que l'on a appuyé sur le bouton "Créer un bastion avec les valeurs par défaut". Avec la configuration manuelle, il faudra compter un peu de temps supplémentaire afin de définir les différents paramètres.



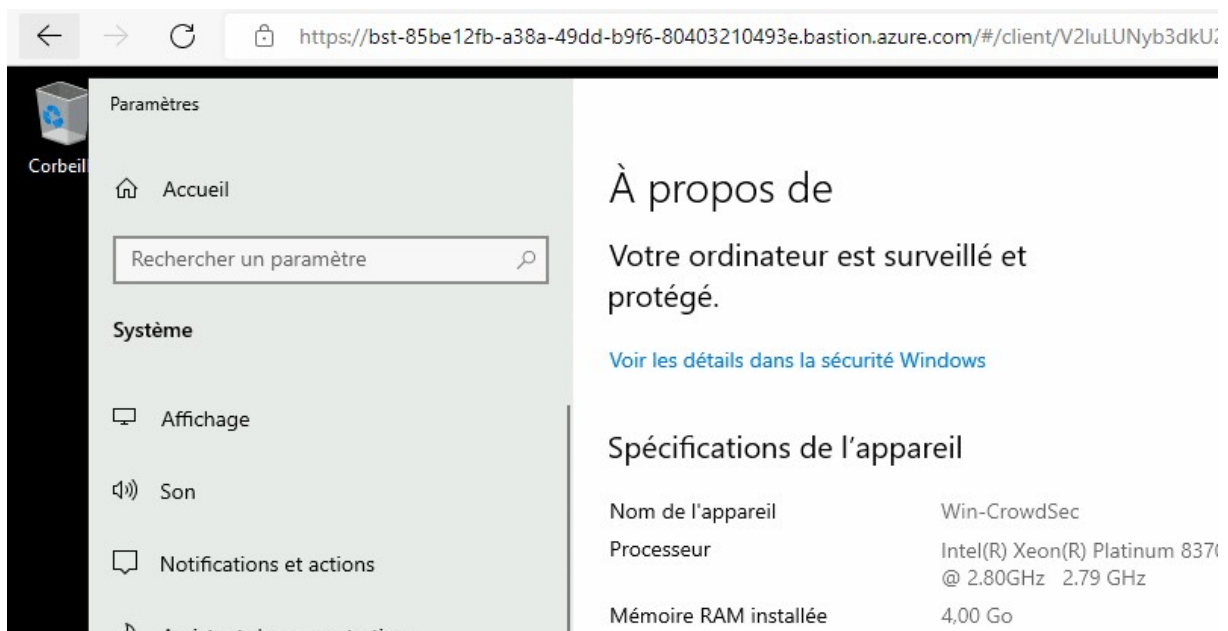
Dès que la création est finie, il faut accéder à la section "Bastion" dans la VM pour laquelle la fonctionnalité est activée. Ainsi, on peut voir que l'on bastion est bien provisionné (état "Succeeded") et on peut s'authentifier à l'aide d'un compte sur cette VM (soit avec un mot de passe, soit à partir d'informations stockées dans Azure Key Vault).



Ensuite, on clique sur "Connexion" et la connexion à la VM s'ouvre dans un nouvel onglet. La première fois, il sera utile d'activer les pop-up : un message s'affiche dans le navigateur pour vous le demander.



Au bout de quelques secondes, me voilà connecté sur ma VM en RDP par l'intermédiaire de mon Bastion ! J'accède à ma VM de façon sécurisée, à distance, à partir de n'importe quel ordinateur simplement à l'aide d'une connexion au portail Azure et d'un navigateur récent !

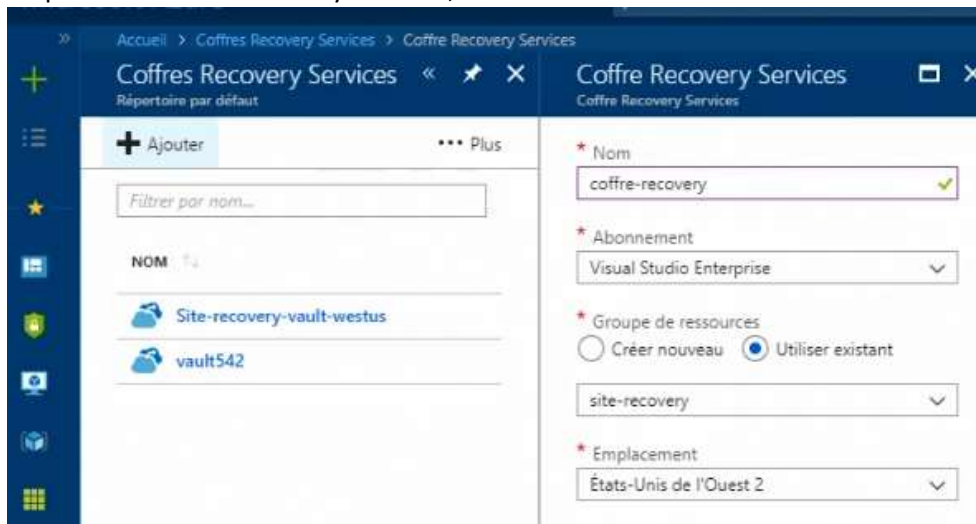


Mise en œuvre d'un PRA pour une VM



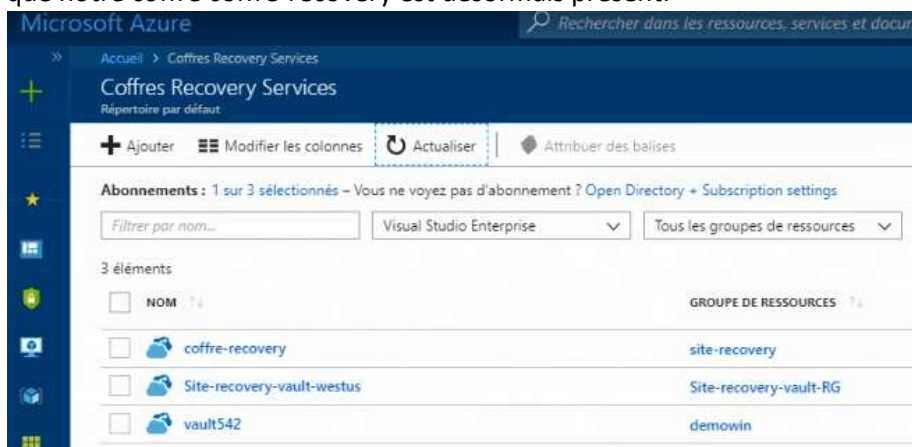
Azur Site Recovery vous permet de créer des plans de reprise d'activité après un sinistre. Ce service vous permet de créer des plans de reprise d'activité entre vos régions Azure, ou encore entre votre réseau d'entreprise et Azure. Dans cette exemple, nous allons créer un plan de reprise d'activité entre nos régions Azure, et ce pour une machine virtuelle. Pour cela, je vous invite à vous connecter sur le portail Azure, puis à aller dans Tous les services et saisir coffre.

Cliquez sur Coffres Recovery Services,

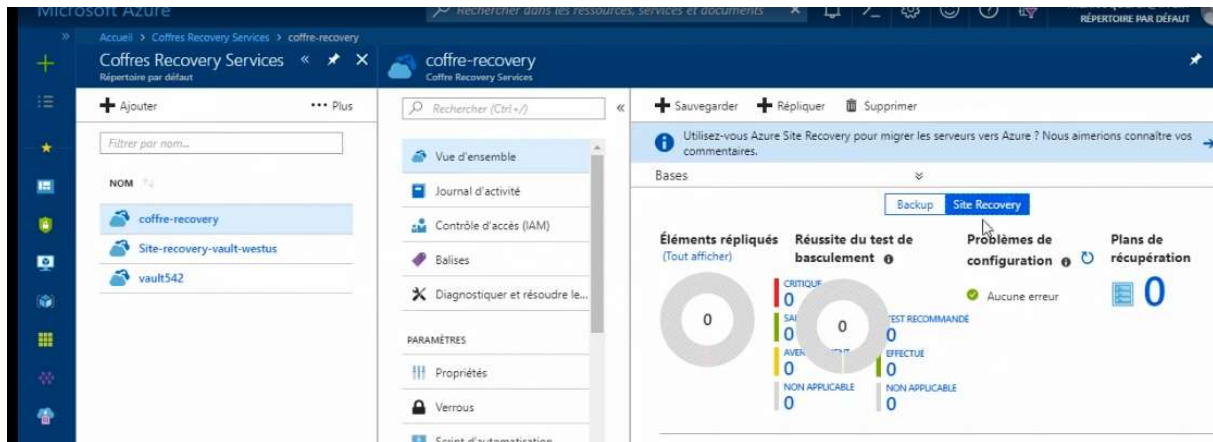


puis je vous invite

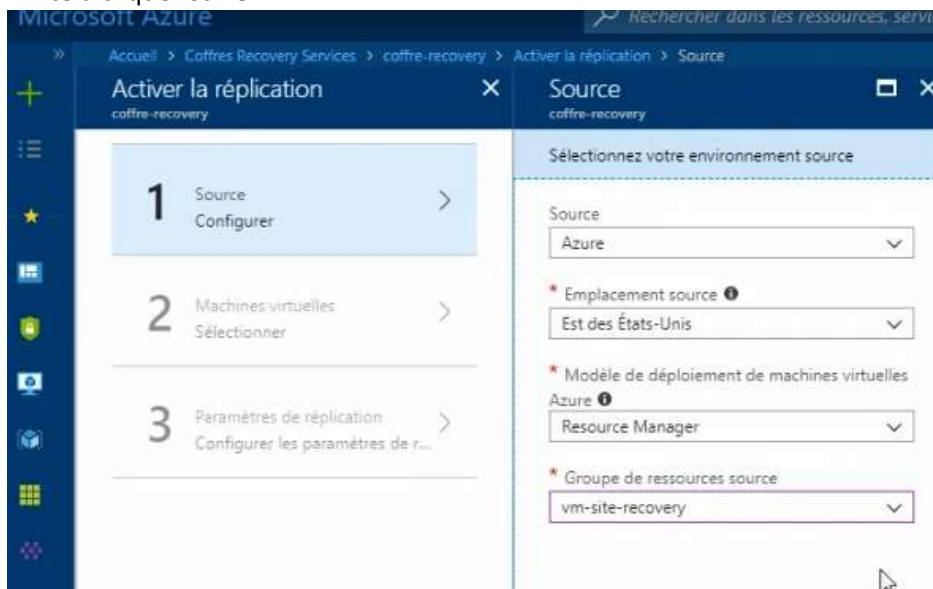
à cliquer sur Ajouter. Nous allons donner un nom à notre coffre, dans cet exemple coffre-recovery. Nous sélectionnons notre abonnement, dans cet exemple Visual Studio Enterprise, nous sélectionnons un groupe de ressources. Dans notre scénario, nous utilisons un groupe de ressources existant, à savoir site-recovery. L'emplacement est États-Unis de l'ouest 2. Puis je vous invite à cliquer sur Créer. Le déploiement est actuellement en cours. Nous avons enfin la confirmation que le déploiement a réussi. Je vous invite désormais à cliquer sur Actualiser et nous pouvons voir ensemble que notre coffre coffre-recovery est désormais présent.



Activer la réplication d'une machine virtuelle

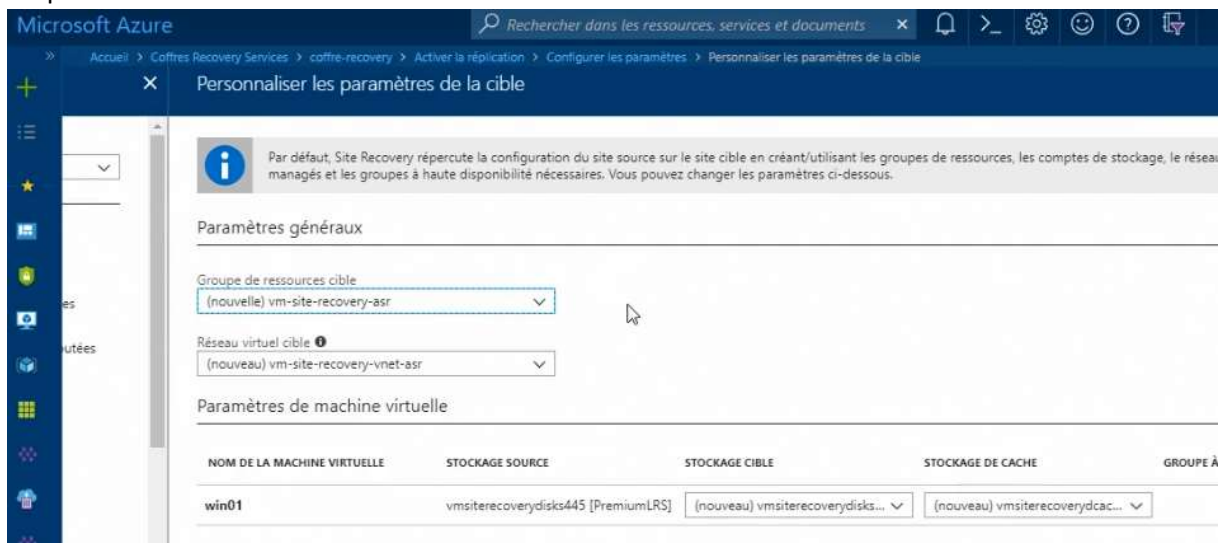


L'activation de la réplication d'une machine virtuelle pour le service Azure Site Recovery. Pour cela, je vous propose de vous connecter sur le portail Azure, puis d'aller dans le service coffre Recovery Services et cliquer sur votre coffre. Dans mon exemple il s'agit du coffre se nommant coffre-recovery. Puis je vous invite à cliquer sur Site Recovery et sur Répliquer. Nous allons alors sélectionner notre environnement Source, à savoir dans notre exemple Azure, l'emplacement source. Il est important de comprendre que l'emplacement source correspond à là où se trouve votre machine virtuelle, dans notre exemple, Est des États-Unis. Puis je vous invite à sélectionner le modèle de déploiement de machines virtuelles Azure. Je vous recommande toujours d'utiliser Resource Manager. Enfin nous allons sélectionner un groupe de ressources. Dans notre exemple, il s'agit du groupe vm-site-recovery, c'est dans ce groupe de ressources que se trouve notre machine virtuelle. Puis je vous invite à cliquer sur OK.

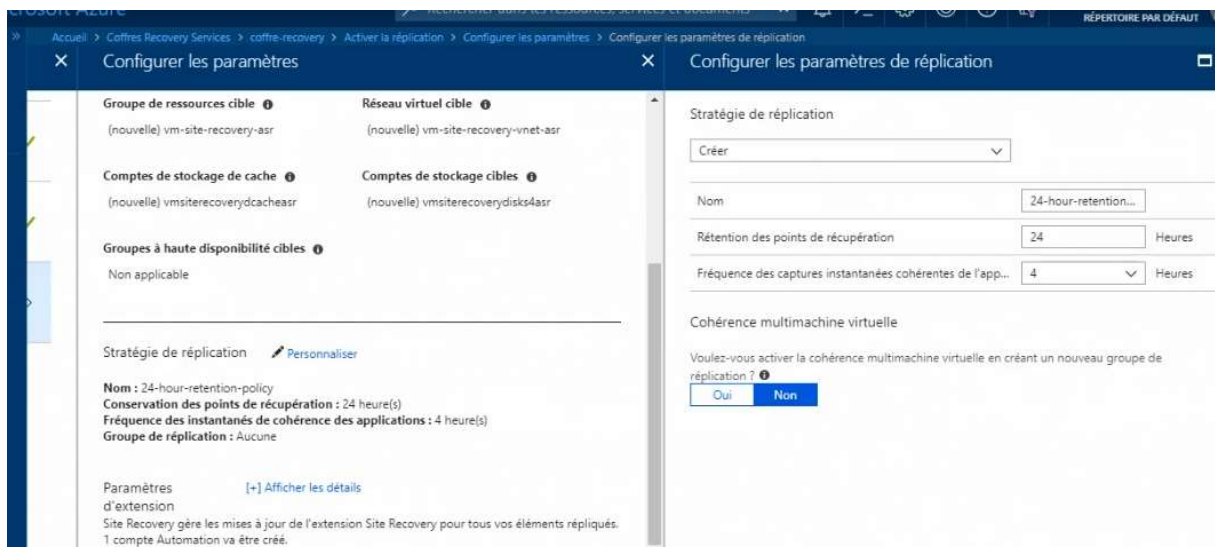


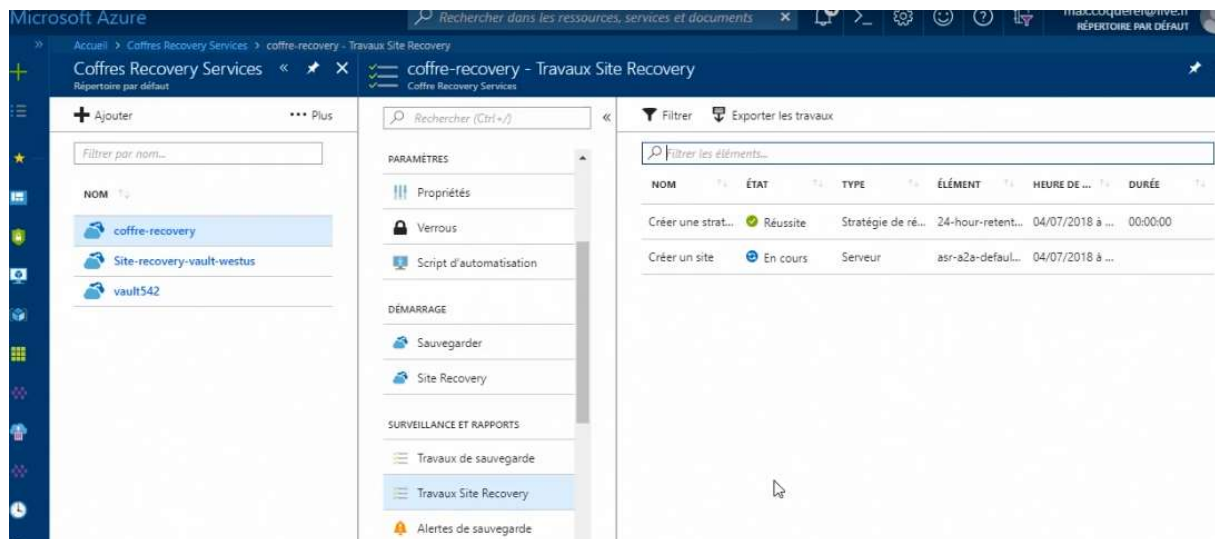
Nous allons sélectionner notre machine virtuelle, à savoir la machine win01. Puis je vous invite à cliquer sur OK. Nous allons pouvoir sélectionner l'emplacement cible, à savoir dans notre exemple, États-Unis de l'Ouest 2. Si vous le souhaitez, vous pouvez personnaliser le groupe de ressources, le réseau, le stockage et les groupes à haute disponibilité en cliquant sur Personnaliser. Nous pouvons voir par exemple le groupe de ressources cible vm-site-recovery-asr. Dans ce scénario, nous laissons

l'ensemble des paramètres par défaut. Ainsi je vous invite à cliquer sur OK. Si nous le souhaitons, nous pouvons également personnaliser la stratégie de réplication en cliquant sur Personnaliser. Dans ce scénario nous laissons l'ensemble des paramètres par défaut, puis je vous invite à cliquer sur OK. Enfin je vous invite à cliquer sur Créer les ressources cibles. L'initialisation du déploiement est en cours, sa soumission également, le déploiement est en cours. Le déploiement a réussi, un service principal est en train de se créer. Nous avons la confirmation que le service principal a été correctement créé. Nous pouvons désormais cliquer sur Activer la réplication. L'activation de la réplication pour la machine est en cours. Nous pouvons également voir l'ensemble des travaux en cliquant sur Travaux Site Recovery et nous pouvons voir les travaux qui sont actuellement en cours d'exécution. Dans cet exemple, nous pouvons voir que créer une stratégie s'est déroulé avec succès et que nous sommes actuellement en train de créer un site.

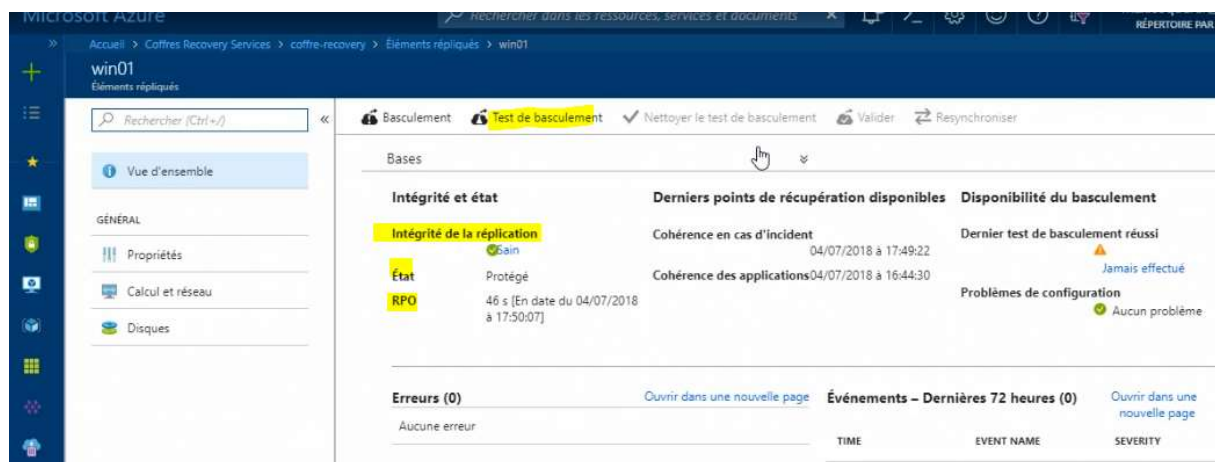


Nous pouvons en voir ensemble la progression. Pour conclure, dans cette vidéo nous avons activé la réplication d'une machine virtuelle pour le service Azure Site Recovery.





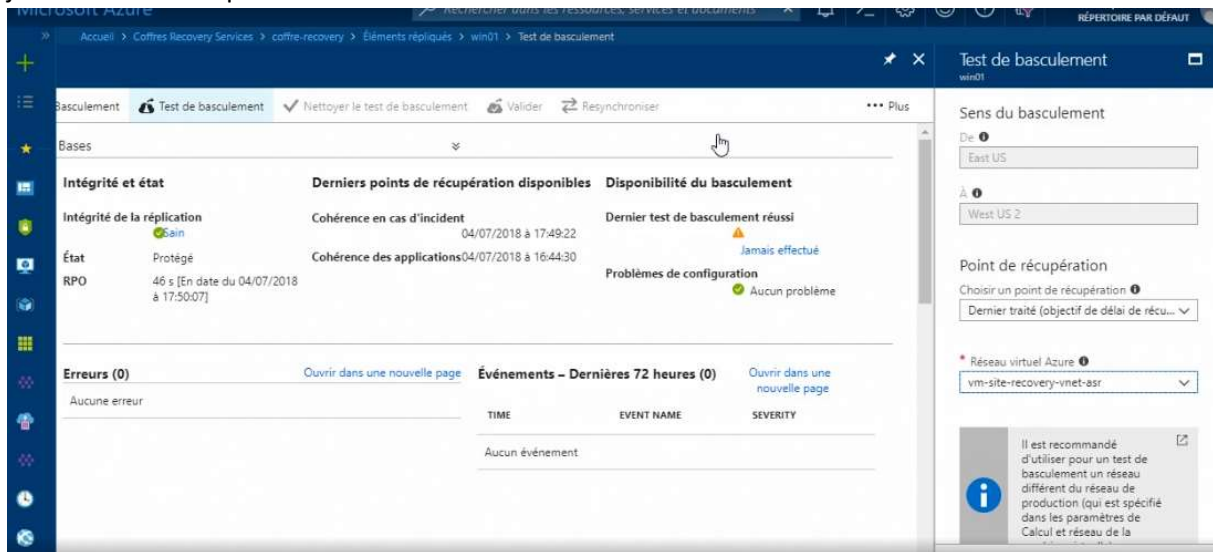
Effectuer un test de bascule



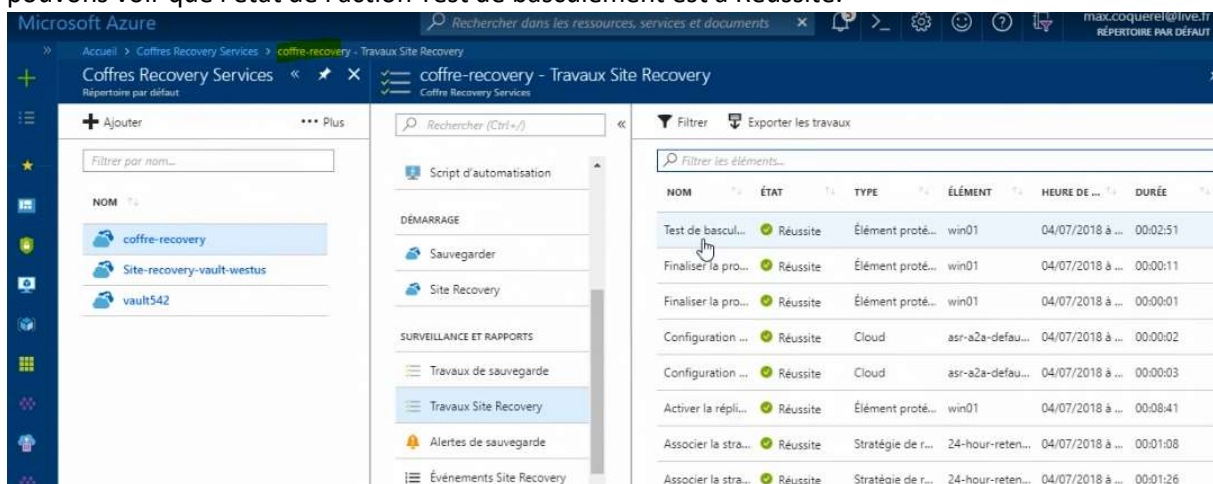
La sélection de lignes de transcription dans cette section vous redirigera vers l'horodatage de la vidéo

Dans cette vidéo, nous allons voir ensemble comment effectuer un test de bascule. Nous pouvons constater que nous avons l'ensemble de nos travaux qui se sont correctement exécutés, je vous invite donc à retourner dans la vue d'ensemble. Comme nous pouvons le voir, notre machine virtuelle a un statut sain. Nous pouvons cliquer dessus. Nous constatons qu'il s'agit bien de la machine win01, la machine que nous avons répliquée précédemment. Je vous invite donc à cliquer dessus. Nous avons désormais la confirmation de l'intégrité de la réplication, donc nous pouvons voir le statut Sain. Nous pouvons voir l'état de la machine Protégé et le RPO qui est de 46s actuellement. Avant de faire un basculement de la machine, je vous propose de faire un test de basculement. Pour cela, je vous invite à cliquer sur Test de basculement. Sens du basculement, East US vers West US, donc Côte Est des États-Unis vers la Côte Ouest des États-Unis. Le point de récupération sera le

dernier point traité et je vous invite ainsi à sélectionner le réseau virtuel Azure, dans notre exemple vm-site-recovery-vnet-asr. Il s'agit du réseau virtuel de destination se trouvant sur la Côte Ouest. Puis je vous invite à cliquer sur OK.



Nous pouvons voir que le démarrage du test de basculement est en cours. Nous pouvons constater que l'état est à l'initialisation du test de basculement. Notre test de basculement s'est déroulé avec succès, pour cela je vous invite à cliquer sur coffre-recovery, puis sur Travaux Site Recovery. Nous pouvons voir que l'état de l'action Test de basculement est à Réussite.



Je vous invite à retourner sur la vue d'ensemble, puis à cliquer sur Sain et sur win01. Nous pouvons voir que l'état est actuellement en attente du nettoyage du test de basculement. Pour cela, je vous invite à cliquer sur Nettoyer le test de basculement. Vous pouvez, si vous le souhaitez, saisir une remarque. Sinon je vous invite à cocher la case Le test est terminé. Supprimez la ou les machines virtuelles du test de basculement. Puis je vous invite à cliquer sur OK. Le démarrage de la tâche de suppression est en cours. Pendant le nettoyage du test de basculement, je vous invite à consulter le graphique ci-dessous. Nous pouvons voir notre machine virtuelle qui s'est fait répliquer entre la Côte Est et la Côte Ouest des États-Unis.

Microsoft Azure

Rechercher dans les ressources, services et documents

Accueil > Coffres Recovery Services > coffre-recovery > Éléments répliqués > win01 > Nettoyage du test de basculement

Basculement Test de basculement **✓ Nettoyer le test de basculement** Valider Resynchroniser

Bases

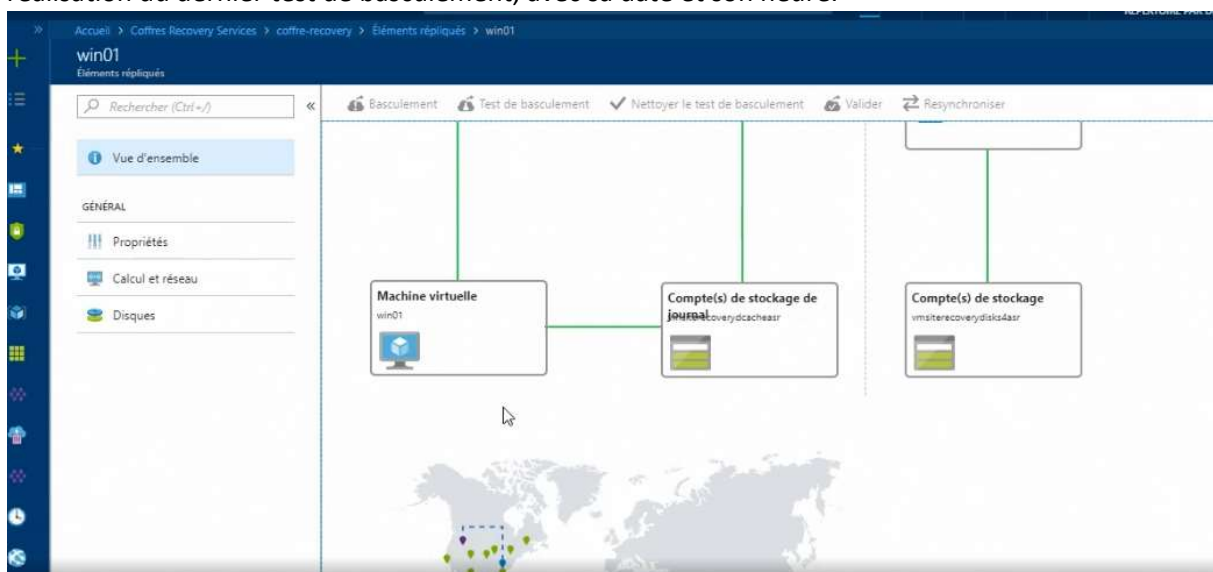
Intégrité et état	Derniers points de récupération disponibles	Disponibilité du basculement
Intégrité de la réplication ✓ Sain	Cohérence en cas d'incident 04/07/2018 à 17:54:22	Dernier test de basculement réussi
État Nettoyage du basculement de test en attente	Cohérence des applications 04/07/2018 à 16:44:30	Problèmes de configuration ✓ Aucun problème
RPO 27 s [En date du 04/07/2018 à 17:59:49]		

Erreurs (0) [Ouvrir dans une nouvelle page](#) Événements – Dernières 72 heures (0) [Ouvrir dans une nouvelle page](#)

Aucune erreur

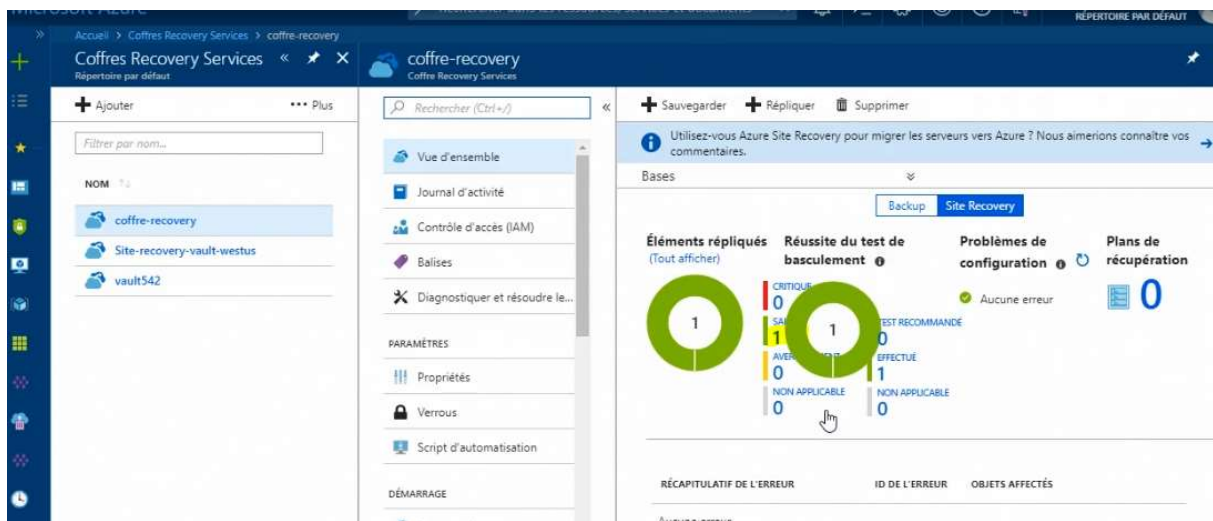
TIME	EVENT NAME	SEVERITY
Aucun événement		

La tâche de suppression a désormais eu lieu avec succès. Nous pouvons ainsi constater ensemble la réalisation du dernier test de basculement, avec sa date et son heure.

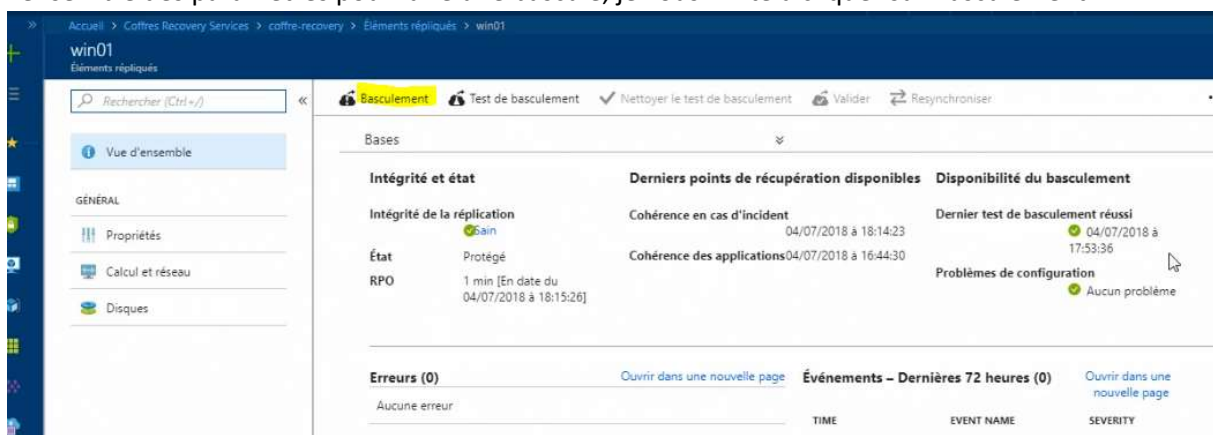


Nous sommes désormais prêts à faire un test de basculement.

Réaliser une bascule



Dans cette vidéo, je vais vous présenter comment faire une bascule avec Azure Site Recovery. Pour cela, je vous donne rendez-vous sur le portail Azure, puis sur Tous les services. Je vous invite à saisir coffre, à cliquer sur Coffres Recovery Services. Sélectionnez votre coffre, dans notre exemple il s'agit du coffre coffre-recovery. Puis je vous invite à cliquer sur l'élément qui est sain, à savoir dans notre cas win01. Comme nous pouvons le constater, un test de bascule a été réalisé au préalable, il est vraiment important de réaliser un test de bascule avant de faire votre basculement. Nous avons l'ensemble des paramètres pour faire une bascule, je vous invite à cliquer sur Basculement.



Nous pouvons voir ensemble le sens du basculement, à savoir de East US vers West US 2. Plus concrètement, de la Côte Est à la Côte Ouest des États-Unis. Nous prenons le dernier point de récupération traité et nous cochons Arrêter la machine avant de commencer le basculement. Puis nous cliquons sur OK. Le basculement est alors en cours. Nous pouvons constater dans l'état que le basculement a été lancé.

Accueil > Coffres Recovery Services > coffre-recovery > Éléments répliqués > win01

win01
Éléments répliqués

Rechercher (Ctrl+J)

Vue d'ensemble

GÉNÉRAL

- Propriétés
- Calcul et réseau
- Disques

Bases

Intégrité et état	Derniers points de récupération disponibles	Disponibilité du basculement
Intégrité de la réplication ✓ Sain	Cohérence en cas d'incident 04/07/2018 à 18:19:23	Dernier test de basculement réussi -
État exécution du basculement	Cohérence des applications 04/07/2018 à 16:44:30	Problèmes de configuration ✓ Aucun problème
RPO -		

Erreurs (0) [Ouvrir dans une nouvelle page](#)

Aucune erreur

Événements – Dernières 72 heures (0) [Ouvrir dans une nouvelle page](#)

TIME	EVENT NAME	SEVERITY
Aucun événement		

Nous avons désormais la confirmation que notre basculement s'est déroulé avec succès, nous pouvons voir ceci dans l'état Basculement terminé. Une fois notre bascule réalisée, je vous invite à cliquer sur Valider notre bascule. Après validation, on ne pourra plus modifier le point de récupération de la machine virtuelle. Je vous invite à cliquer sur OK. Comme nous pouvons le constater, la validation du basculement est actuellement en cours. La validation du basculement s'est déroulée avec succès.