Editions ENI

Hyper-V et System Center Virtual Machine Manager

Services de virtualisation de Windows Server 2016

Collection
Expert IT

Extrait

Chapitre 6
Gestion de la haute disponibilité Hyper-V

1. Introduction

Depuis plusieurs années les équipes IT ont été confrontées à la mise en œuvre de solutions de haute disponibilité pour garantir un fonctionnement constant des services les plus sensibles 24h/24, 7j/7, 365 j/an. Ces solutions ont généralement toujours été proches du matériel et du système d'exploitation assurant le support des applications et de l'infrastructure. Cependant, aujourd'hui, la mise en œuvre de plates-formes de virtualisation rend encore plus dramatique et significative la perte d'une machine unique dont le rôle est de supporter un nombre de plus en plus important de machines virtuelles.

En effet, les plates-formes de virtualisation permettent de réduire le coût total de possession et aussi d'améliorer la qualité des services offerts (déploiement de nouveaux serveurs instantanés, optimisation des ressources matérielles, etc.) mais malheureusement, elles introduisent un problème majeur : le risque d'une défaillance au niveau de la machine hôte de virtualisation elle-même.

Ainsi, un dysfonctionnement provoquant l'arrêt brutal d'une machine hôte assurant le fonctionnement d'une dizaine voire de plusieurs centaines de machines virtuelles sera un événement catastrophique aux conséquences multiples ! Pour répondre à cette problématique et ainsi aux enjeux des entreprises, Hyper-V a été conçu pour assurer une haute disponibilité des machines virtuelles.

Plusieurs alternatives sont envisageables :

– La mise en cluster de la machine hôte.

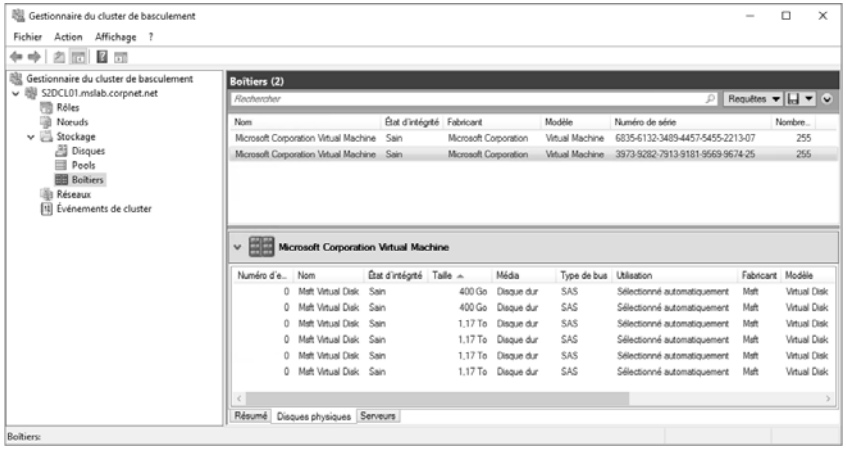
– La mise en cluster des machines virtuelles hébergées par N machines hôtes.

– L'utilisation des fonctionnalités de haute disponibilité intégrées aux applications telles que, par exemple, Microsoft Exchange Server ou Microsoft SQL Server.
– L'ajout de solutions tierces.

1.1 Virtualisation Hyper-V et Clustering avec Windows Server 2016

Définition d'un cluster Windows

Un cluster de basculement – en anglais Failover Clustering – est un groupe de machines indépendantes travaillant conjointement pour accroître la disponibilité et l'extensibilité des ressources configurées au sein dudit cluster. Appelées « Rôles » avec les clusters fonctionnant sous Windows Server 2012 R2 et Windows Server 2016, ces ressources apparaissaient sous la rubrique « Applications et services » sur les clusters fonctionnant sous Windows Server 2008 R2. Du côté de l'administration, la console MMC Gestionnaire du cluster de basculement permet de gérer un seul ou de multiples clusters en affichant chaque cluster, chacun des nœuds de chaque cluster ainsi que les ressources réseau et les ressources de stockage associées de type SAN et de type convergé et hyperconvergé avec Storage Spaces Direct. La figure ci-dessous illustre la gestion du stockage hyperconvergé S2D.



Console du Cluster et Stockage Storage Spaces Direct

Au-delà de ces composants élémentaires et centraux, des services tels que les services de fichiers et d'impressions, ou des applications telles que SQL Server, Exchange Server ou le rôle Hyper-V sont gérés nativement par le clustering avec basculement de Windows Server. En cas de défaillance générale d'un ou plusieurs nœuds ou même d'une ou de plusieurs ressources mises en cluster, un ou d'autres nœuds prennent le relais pour fournir les services requis lors du processus de basculement des ressources – appelé en anglais Failover.

Le clustering avec basculement ne se contente pas non plus de réagir en cas de coupure franche mais il assure aussi une surveillance proactive afin de vérifier que les rôles fonctionnent correctement. Si tel n'est pas le cas, ils sont par défaut d'abord redémarrés sur le même nœud puis, si nécessaire, déplacés vers un autre nœud.

Les versions Standard et Datacenter de Windows Server 2016 et Nano Server étant rigoureusement identiques, elles permettent à chaque nœud devant supporter des machines virtuelles à l'aide du rôle Hyper-V de faire partie intégrante d'un cluster Windows Server 2016.

Pour rappel, notez que ces versions implémentent pour la première fois un mode de licence par cœurs et incluent des droits de virtualisation limités à deux machines virtuelles pour l'édition Standard, ou illimités pour l'édition Datacenter. Pour plus d'informations sur ces versions, reportez-vous au chapitre Implémentation et gestion d'Hyper-V, section À propos des technologies de virtualisation de serveurs - Technologie de virtualisation Hyper-V.

Rappel à propos des licences par cœurs Windows Server 2016 : désormais, dans l'objectif d'aligner les licences Windows Server avec la tarification des VM sur Azure – qui sont licenciées en nombre de cœurs – Windows Server 2016 utilise une tarification basée aussi sur ce principe. Tous les coeurs physiques d'un serveur sont donc soumis à licence pour un minimum de 16 cœurs, sachant que les licences de base – appelées en anglais Core Pack – sont vendues par pack de 2 cœurs. Ainsi, chaque serveur physique doit être équipé de 8 packs de 2 cœurs, sachant que le coût d'un pack est égal à un huitième du prix d'une licence pour 2 processeurs physiques Windows Server 2012 R2. Dans l'absolu, le coût de Windows Server 2016 est donc identique à celui de Windows Server 2012 R2 – quelle que soit l'édition – mais pourra être supérieur en fonction du nombre de cœurs présents dans les serveurs.

Du point de vue de l'administration, la configuration d'une machine virtuelle au sein du cluster signifie que l'administrateur peut rendre disponible auprès des autres nœuds du cluster les ressources nécessaires à ladite machine virtuelle. Cela comprend tant l'ensemble de ses paramètres de configuration que le ou les disque(s) virtuel(s) disponible(s) via le stockage partagé au sein du cluster via une connectivité SAN FC ou iSCSI, un partage SMB302 ou un stockage Storage Spaces Direct sous Windows Server 2016.

Sur la base de ces principes, chaque machine virtuelle peut être rendue « hautement disponible » grâce à la fonctionnalité Clustering avec basculement capable de prendre en charge le basculement et le redémarrage automatique de chaque machine virtuelle en cas de nécessité.

En plus de ces aspects haute disponibilité, la possibilité de déplacer une machine virtuelle vers un autre hôte Hyper-V avec ou sans son stockage associé – c'est-à-dire respectivement, Live Migration ou Live Storage Migration – permet de garantir une disponibilité maximum tout en permettant à l'administrateur de disposer de toute la souplesse nécessaire pour la maintenance matérielle et logicielle des machines hôtes.

Remarque

À propos des contraintes matérielles, qu'il s'agisse de vSphere ou d'Hyper-V, les fonctionnalités de haute disponibilité nécessitaient un stockage partagé de type SAN ou convergé via Storage Spaces Direct. Avec Windows Server 2016, et aussi vSphere 5.1 et ultérieur, il n'est plus obligatoire de disposer d'un stockage de type cluster. La migration à chaud du stockage des machines virtuelles peut être réalisée quel que soit le type de stockage, qu'il soit partagé, local ou convergé.

1.2 Profiter des services de virtualisation et des services de clustering Windows

Le principe consiste à déterminer quelle est la meilleure solution à implémenter pour mettre à disposition de l'application un environnement hautement disponible. Dans l'absolu, la bonne approche consiste à utiliser les fonctionnalités intégrées au sein des applications.

Par exemple, il n'est pas nécessaire d'implémenter de mécanisme supplémentaire pour les contrôleurs de domaine, les serveurs DNS, les espaces DFS-R ou les bases de données SQL Server. Tous ces services disposent de mécanismes de réplication intégrés qui les rendent hautement disponibles, pour peu qu'au minimum deux machines soient configurées. C'est par exemple le cas d'Exchange Server qui propose depuis de nombreuses années déjà ses fameux DAG (*Database Availability Group*) pour répliquer les bases de données de boîtes aux lettres sur de multiples serveurs – de type physiques ou en VM.

Toutes ces méthodes de secours peuvent être implémentées dans des environnements de machines virtuelles. De cette manière, en cas d'indisponibilité d'une machine virtuelle invitée ou de la machine hôte Hyper-V, une autre machine virtuelle fonctionnant sur un autre serveur de virtualisation Hyper-V pourra fournir les services et applications manquantes. De cette manière, la disponibilité des systèmes est assurée à deux niveaux, d'une part, grâce à la plate-forme de virtualisation et d'autre part, grâce aux fonctionnalités de haute disponibilité embarquées dans l'application.

1.3 À propos du Clustering avec basculement de Windows Server 2016

La fonctionnalité de Clustering avec basculement de Windows Server 2016 a fait l'objet de nombreuses améliorations sachant qu'une refonte totale avait déjà été réalisée avec Windows Server 2012 et 2012 R2.

Microsoft a encore une fois mis l'accent sur la simplicité d'utilisation et la mise en œuvre de fonctionnalités nouvelles. Les points suivants listent les avancées réalisées avec Windows Server 2012, suivent ensuite celles apportées par Windows Server 2012 R2 et Windows Server 2016.

– Capacité augmentée via le support de 64 nœuds par cluster. Dans le cas des configurations de type cluster Hyper-V, Microsoft supporte désormais 8000 machines virtuelles par cluster avec un maximum de 1000 machines virtuelles par nœud.
– Intégration Active Directory améliorée : les services de clustering de Windows Server 2012 R2 sont désormais capables de démarrer sans nécessiter une dépendance avec les services d'annuaire Active Directory. Cette amélioration est notable car elle offre une grande indépendance vis-à-vis de l'infrastructure pendant la phase de démarrage de chaque nœud du cluster. Comme cela était le cas avec les versions antérieures de Windows Server, les objets CNO (*Cluster Name Objects*) permettent aux clusters de disposer de leur identité propre au sein de l'Active Directory. Notez que par défaut, l'objet CNO représentant le cluster est créé dans la même unité d'organisation que le compte d'ordinateur du premier nœud du cluster permettant sa création.

Remarque

Windows Server 2012 R2 et Windows Server 2016 implémentent la réparation automatique des objets CNO en cas de suppression accidentelle.

L'assistant de création du cluster permet la déclaration du nom complet de l'objet CNO représentant le cluster pour spécifier l'emplacement de l'objet dans Active Directory.

– Configuration simplifiée du quorum : par défaut, les clusters Windows Server 2012 R2 et Windows Server 2016 choisissent automatiquement les paramètres de quorum adaptés à la configuration. Le quorum est désormais dit « dynamique » sachant que l'administrateur dispose en plus de la possibilité de manuellement empêcher tel ou tel nœud de participer au vote nécessaire à la détermination du quorum.

Remarque

Utilisation de la configuration par défaut : le mode de quorum dynamique détermine automatiquement le nombre de votants lequel change dynamiquement en fonction du nombre de nœuds participants. Les détails relatifs à la configuration du quorum au sein d'un environnement Windows Server 2012 R2 et Windows Server 2016 sont traités plus loin.

– Mise à jour automatique des nœuds : les clusters fonctionnant sous Windows Server 2012 R2 et Windows Server 2016 supportent la fonctionnalité Cluster-Aware Updating (CAU). Il s'agit d'une fonctionnalité de gestion des mises à jour automatique des nœuds membres d'un cluster tout en maintenant la haute disponibilité pendant la phase de mise à jour. Un processus de déplacement automatique libère chaque nœud puis repositionne les ressources après le redémarrage de celui-ci. Ce composant utilise l'agent Windows Update comme source des mises à jour.

- Administration plus performante des clusters : l'administration est réalisée via le nouveau Gestionnaire de serveur et aussi via la nouvelle console Gestionnaire du Cluster à basculement qui intègre des fonctions de recherche, de filtrage et la possibilité de créer des vues simplifiées. Ainsi, il est facile de réaliser des sélections multiples pour lancer via la console MMC des opérations en masse de type Live Migration, arrêt, redémarrage, sauvegarde de l'état, etc.
- Nouveaux assistants simplifiés pour réaliser les opérations de déplacement des machines virtuelles Hyper-V avec Live Migration, Live Storage Migration et Quick Migration.
- Configuration simplifiée du stockage et des volumes CSV (*Cluster Shared Volumes*).
- Support de la réplication sur site ou hors site des machines virtuelles via Hyper-V Replica. La fonctionnalité permet de facilement mettre en œuvre un DRP (*Disaster Recovery Plan*), grâce à la réplication des machines virtuelles les plus importantes entre différents systèmes de stockage, différents clusters Windows Server et différents centres de données.

  Gestion améliorée des rôles : l'administrateur peut configurer la priorité de démarrage et le placement des machines virtuelles pour allouer de façon plus efficace les ressources nécessaires via l'utilisation de trois classes de priorités : Haute, Moyenne (valeur par défaut) et Basse. Notez que l'option Pas de démarrage automatique permet de ne pas démarrer telle ou telle VM automatiquement au démarrage du cluster.

Nouvelles fonctionnalités apportées par Windows Server 2012 R2

Les nouvelles fonctionnalités des services de basculement de Windows Server 2012 R2 sont listées ci-dessous :

- Disque virtuel VHDX partagé pour les clusters de machines virtuelles invitées : avec Windows Server 2012, l'administrateur avait la possibilité de créer des clusters de machines virtuelles invitées via des ressources de stockage partagées de type SAN (iSCSI ou Virtual Fibre Channel). Bien que cela soit parfaitement suffisant dans la majorité des scénarios, ce type de configuration a l'inconvénient d'exposer le stockage existant au sein des machines virtuelles concernées, ce qui peut être un problème de sécurité dans les environnements de type Cloud. Windows Server 2012 R2 peut désormais « mettre en commun » un ou plusieurs disques virtuels VHDX entre plusieurs machines virtuelles. Ces disques virtuels apparaissent virtuellement comme des ressources disque partagées disponibles entre les différents nœuds du cluster de machines invitées. De cette manière, les fichiers de disques virtuels VHDX partagés offrent l'abstraction et toute la souplesse d'administration souhaitée. Nous verrons plus loin que Windows Server 2016 améliore grandement cette fonctionnalité.

Editions ENI

Windows Server 2016

Administration avancée

Collection
Expert IT

Extrait

Chapitre 5
Mise en place des services réseau d'entreprise

1. Introduction

Ce chapitre est consacré à la définition et la configuration des composants nécessaires au bon fonctionnement d'un réseau d'entreprise basé sur Windows Server 2016.

Les composants IP, DNS, DHCP, WINS, ainsi que la mise en place d'une autorité de certification (PKI) seront abordés. Comme cela était prévu, il n'est plus possible de configurer la quarantaine réseau à partir de Windows Server 2016.

2. Le choix de l'infrastructure réseau

La mise en place de toute architecture réseau passe par l'analyse des réseaux existants. Il est souvent difficile de modifier l'ensemble en une seule fois. La migration se fait donc souvent en implémentant un nouvel adressage réseau et une cohabitation avec les réseaux existants. La modification de l'adressage IP est souvent vue comme coûteuse, n'apportant que peu d'avantages supplémentaires.

C'est souvent lors du déplacement ou de la création d'un site qu'il est facile voire nécessaire de repenser l'adressage IP et de planifier un nouveau système.

Le changement d'un domaine DNS est encore plus compliqué, surtout lorsque ce domaine DNS sert de support à un domaine Active Directory. Dans ce cas, une migration représente une étude particulière qui sort du cadre de cette présentation.

2.1 Le choix de l'architecture réseau

Deux points précis sont à étudier à ce niveau :

– Le choix de la zone DNS.
– Le choix de la classe réseau.

2.1.1 La zone DNS

Deux aspects sont importants lors du choix de la zone DNS.

Le nom choisi pour la zone DNS doit correspondre à l'intégralité de l'entité (entreprise, groupe, etc.) que l'on souhaite gérer. Ce nom doit pouvoir être accepté par toutes les entités dépendantes qui vont se retrouver dans cette zone. Le problème est beaucoup plus politique que technique !

Si une entité n'entre pas dans ce cadre, cela veut dire qu'une zone DNS spécifique doit lui être affectée.

Si la zone DNS doit être utilisée sur Internet, le domaine DNS sera forcément public et enregistré, c'est-à-dire utilisant une extension reconnue de type **.fr**, **.com**, **.info**...

Pour un réseau interne, le domaine peut être public ou privé. Le choix le plus courant est alors d'utiliser un domaine DNS local avec une extension inconnue sur Internet. L'extension **.local** est très souvent utilisée sous la forme **masociete.local**. Le découpage entre ce qui est interne ou externe est plus facile à réaliser. Ce choix est maintenant à déconseiller, car les fournisseurs de certificats ont décidé, en accord avec les grands éditeurs, de ne plus distribuer à partir du 1er Janvier 2014 de certificats comportant des noms appartenant à des domaines DNS non vérifiables. Ceci a une conséquence directe pour la configuration de nombreux serveurs Exchange qui possèdent ce type de certificats. Mais, il est probable que certains serveurs web visibles à la fois en Intranet et en Internet utilisaient ce type de fonctionnalité.

En revanche, l'utilisation du même nom de domaine sur le réseau interne et sur Internet suppose des serveurs DNS différents pour ne rendre visible sur Internet que ce qu'il est souhaitable de montrer. Cela entraîne une double administration des zones DNS. Cette solution est plus complexe.

Pour les nouvelles installations, la préconisation sera :

– soit d'utiliser un domaine qui a une extension reconnue (et disponible à l'enregistrement) telle que **.org**, **.net**, **.info**.
– soit de définir un sous-domaine du domaine public déjà utilisé, sous la forme **ad.masociete.fr**.

Dans les deux cas, l'obtention d'un certificat public ne posera aucun problème.

2.1.2 La classe réseau

Pour tous les réseaux internes, le choix se portera évidemment toujours sur les classes réseaux privées. Si l'on ne peut pas toujours modifier l'intégralité des réseaux existants pour des raisons souvent historiques, on peut au moins créer tous les nouveaux réseaux en suivant cette règle.

La classe du réseau se choisit en fonction du nombre de machines présentes sur le réseau, du nombre de sites, etc. Un réseau de classe C (192.168.0.X) représente souvent un bon choix initial. Il est toujours possible de changer de classe, de réseau ou même surtout d'utiliser plusieurs réseaux en fonction des besoins.

L'usage de TCP/IP v6 n'est pas encore bien développé mais deviendra nécessaire dans les deux ou trois années qui suivent, principalement sur Internet. Sur le réseau local, il reste encore de nombreux logiciels qui ne sont pas compatibles, mais ceci devrait évoluer très rapidement ! Le réseau IPv6 est étudié dans le chapitre Les évolutions du réseau.

2.2 L'installation d'un serveur DHCP

Si le service DHCP permet de mettre en place rapidement le réseau choisi, il permet aussi de modifier rapidement et globalement une série de paramètres. Les entreprises n'utilisant aucun service DHCP sont maintenant très rares.

Parmi les nombreux composants de Windows Server 2016, le service DHCP est un rôle.

2.2.1 Définition

Le protocole DHCP (*Dynamic Host Configuration Protocol*) a pour but de fournir une adresse IP et un masque de sous-réseau à tout périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la configuration, d'autres paramètres tout aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser, des serveurs WINS et le suffixe de domaine pour ne citer que les principaux.

DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs.

2.2.2 L'installation

Comme pour tous les composants Windows, l'installation peut se faire graphiquement ou par commande PowerShell sans avoir besoin d'insérer le moindre média.

Installation via PowerShell :

```
Install-WindowsFeature DHCP
```

Remarque

Attention, le service sera démarré immédiatement et configuré en démarrage automatique ! En revanche, l'installation du composant DHCP par PowerShell n'installe que le service DHCP. Il faut lancer la commande indiquée ci-dessous pour installer l'outil d'administration.

```
Install-WindowsFeature RSAT-DHCP
```

Le service doit être démarré pour que DHCP soit accessible et configurable.

Pour que le service DHCP commence à distribuer des adresses, il est indispensable de configurer et d'activer une étendue.

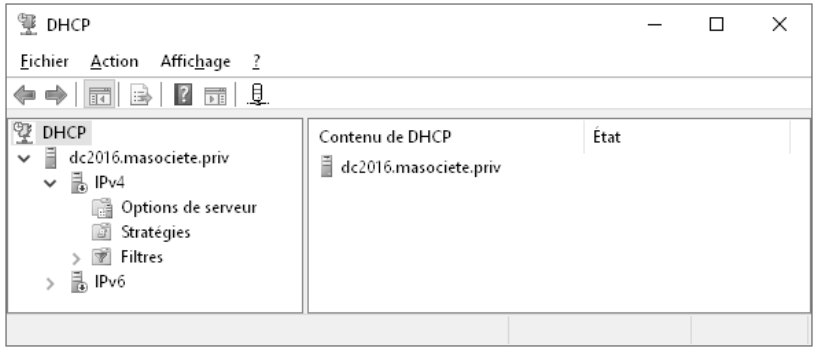
Attention, si le serveur qui héberge DHCP fait partie d'une forêt Active Directory, il doit en plus avoir été autorisé par des administrateurs membres du groupe **Administrateurs de l'entreprise** ou ayant reçu les droits d'administration DHCP.

Le service DHCP, comme les autres services réseau de référence (DNS, WINS), devrait toujours être installé sur des serveurs disposant d'adresses IP fixes.

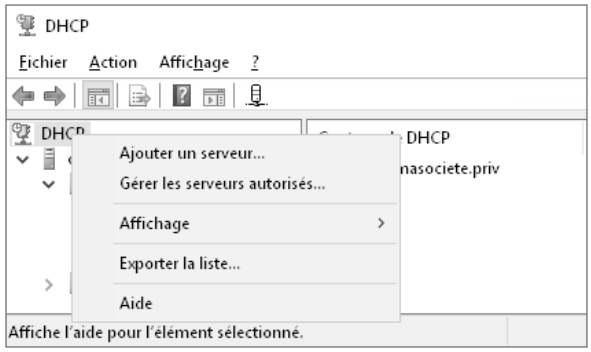
2.2.3 La configuration

La console d'administration DHCP se trouvera sur tout serveur où le rôle DHCP a été installé par l'interface graphique et sur tout serveur où le composant d'administration a été ajouté spécifiquement.

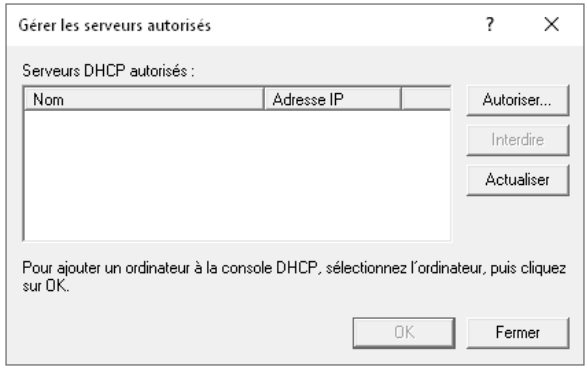
Si le serveur local héberge le rôle DHCP, le serveur apparaît automatiquement dans la console.



- Si le serveur n'héberge pas le rôle DHCP ou n'est pas celui souhaité, utilisez le bouton droit pour ajouter un serveur spécifique ou le sélectionner parmi les serveurs autorisés.



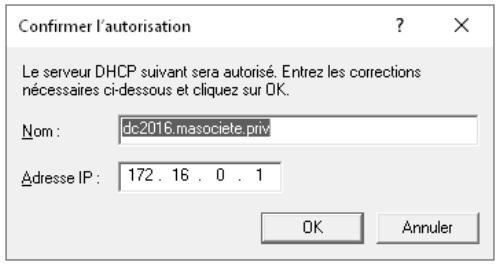
- Pour autoriser un serveur DHCP, utilisez l'option **Gérer les serveurs autorisés**.



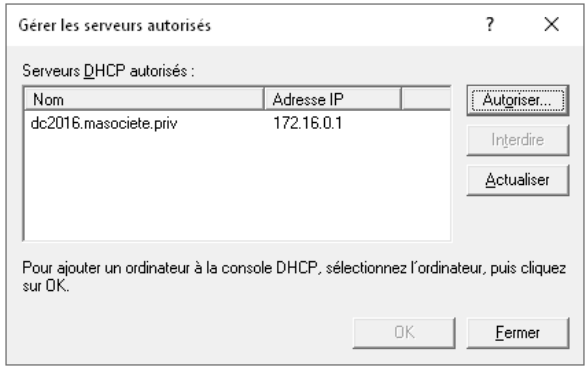
- Cliquez sur le bouton **Autoriser**, et saisissez le nom ou l'adresse IP.

Dans une forêt Active Directory, seuls les serveurs DHCP qui ont été autorisés par les administrateurs de l'entreprise ont le droit d'émettre des adresses IP à partir des étendues actives.

- Confirmez l'adresse et le nom proposés en cliquant sur le bouton **OK**.



Fermez la fenêtre des serveurs autorisés en cliquant sur **Fermer**.



Les serveurs autorisés apparaissent avec une flèche verte.