

Tout ce qu'il faut savoir sur le centre de données défini par logiciel

Rapport de synthèse d'Osterman Research

Publié en mai 2017



Osterman Research, Inc.

P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA

Tél. : +1 206 683 5683 • info@ostermanresearch.com

www.ostermanresearch.com • @mosterman

RAPPORT DE SYNTHÈSE

Le centre de données défini par logiciel (SDDC, Software-Defined Data Center) s'inscrit dans le cadre d'une approche globale visant l'optimisation des centres de données. En résumé, un SDDC peut être considéré comme un ensemble de ressources informatiques virtualisées alliées à un stockage et à une mise en réseau définis par logiciel. Au sein d'un SDDC, la sécurité est envisagée de manière globale. Ainsi, un SDDC procède à l'abstraction et à l'automatisation de tous les aspects du calcul, du stockage et de la mise en réseau qui prennent habituellement une forme physique, puis exploite cette abstraction et cette automatisation dans le but d'améliorer la sécurité.

En se fondant sur la virtualisation, un SDDC combine le réseau défini par logiciel (SDN, Software-Defined Networking) et le stockage défini par logiciel (SDS, Software-Defined Storage). En pratique, il s'agit d'un moyen pragmatique de mettre en place un centre de données virtualisé, par exemple un cloud privé ou hybride. En effet, la plupart des fournisseurs de clouds publics à grande échelle recourent d'une manière ou d'une autre au principe de fonctionnement des SDDC, ce qui leur permet de réduire leurs coûts.

Il ressort de nos recherches que la vaste majorité des serveurs actuels sont déjà virtualisés. Par ailleurs, environ la moitié des entreprises prévoient de transformer leurs centres de données en SDDC ou l'ont déjà fait. Parmi celles qui prévoient une transition dans ce sens, la plupart envisagent de l'implémenter dans un délai de deux ans.

POURQUOI UN SDDC ?

Nos études montrent que la plupart des entreprises adoptent le modèle du SDDC dans le but d'améliorer les performances des opérations, la sécurité constituant elle aussi un critère de première importance. D'autres facteurs d'adoption courants sont la réduction des coûts, la simplification de l'environnement et l'amélioration du contrôle. Les trois motivations principales sont illustrées ci-dessous :

Raisons justifiant l'adoption d'un SDDC



Source : Osterman Research, Inc.

AVANTAGES DU SDDC POUR L'ACTIVITÉ

Un SDDC offre de nombreux avantages importants pour l'activité d'une entreprise :

- **Opérations plus rapides et productivité accrue du personnel informatique**
De par sa nature logicielle, un SDDC est plus facile à configurer, à reconfigurer et à sécuriser (moyennant les outils appropriés). Les opérations informatiques en deviennent plus réceptives aux modifications et plus efficaces. En outre, le SDDC permet d'effectuer des mises à jour de service fréquentes et de bâtir et décommissionner rapidement des environnements de test.
- **Sécurité renforcée**
Un SDDC permet de centraliser le contrôle et la gestion des composants virtualisés du centre de données et les rend plus visibles vis-à-vis des opérations

informatiques. La centralisation et la visibilité sont deux caractéristiques inhérentes à la nature logicielle des SDDC, et sont essentielles pour une sécurité cohérente et rigoureuse. Dans les centres de données traditionnels, les règles sont distribuées et appliquées sur une série d'équipements et dépendent de topologies physiques fragiles. Au contraire, dans un SDDC, des stratégies mises en œuvre de manière cohérente agissent sur les caractéristiques logiques et abstraites de la *charge de travail* et de ses données, et non sur des caractéristiques physiques variables, condamnées à devenir obsolètes.

- **Plus grande fiabilité**

Les opérations informatiques traditionnelles sont par nature sujettes aux erreurs, même lorsque l'administrateur emploie une console de gestion centralisée. L'automatisation des opérations au sein d'un SDDC limite les erreurs et la lassitude née de la répétition des tâches, ce qui renforce la sécurité et réduit les temps d'arrêt *non programmés*.

- **Utilisation optimisée du matériel**

La virtualisation intensifie l'utilisation du matériel, permettant ainsi aux entreprises de mieux rentabiliser leurs dépenses d'investissement. Elle permet par exemple à plusieurs charges de travail de partager des ressources de calcul et de stockage définies par logiciel. De plus, le SDDC unifie les fonctions réseau traditionnellement isolées, de même que les rôles des baies de stockage.

- **Interopérabilité du cloud**

Les SDDC permettent aux entreprises de profiter des avantages inhérents des clouds hybrides sans les obliger à se cantonner à un fournisseur ou à une technologie spécifique. Par leur association, l'automatisation, l'abstraction, la visibilité et le contrôle renforcent la cohérence de l'environnement. Il devient dès lors nettement plus facile de placer des charges de travail dans des clouds publics ou privés qu'avec la virtualisation seule.

UNE SÉCURITÉ RENFORCÉE GRÂCE AU SDDC

En ce qui concerne la sécurité dans les environnements SDDC, divers éléments importants sont à prendre en compte :

- L'adoption d'un SDDC ne change en rien la nature des menaces pour la sécurité, pas plus que les compétences nécessaires pour évaluer ces menaces et les risques associés. Toutefois, le SDDC ne confine plus la sécurité à un point physique du réseau : la plate-forme de virtualisation effectue l'abstraction des fonctions réseau et de sécurité et les sépare de la plate-forme matérielle sous-jacente.
- L'un des avantages majeurs du SDDC en termes de sécurité est que la plate-forme de virtualisation peut superviser tous les comportements des charges de travail qu'elle gère : non seulement au sein d'une machine virtuelle donnée, mais *entre* les différentes VM, ce qui permet à la plate-forme de virtualisation et aux logiciels de sécurité de surveiller le comportement *en contexte*.
- Remonter les fonctions intelligentes d'un niveau permet aux logiciels de sécurité d'être plus près des charges de travail, ce qui améliore fortement la visibilité de ces logiciels sur les données au repos et en transit.
- Cette proximité vis-à-vis des charges de travail permet aux logiciels de sécurité d'assurer une protection plus efficace contre les attaques par déni de service, les tentatives malveillantes d'outrepasser les limites de la machine virtuelle, les violations de contrôle d'accès par zone géographique et divers autres problèmes.
- Un SDDC autorise l'inspection des menaces potentielles sur la base d'informations comportementales rarement disponibles dans un centre de données conventionnel. Il facilite la connexion à des réseaux de cyberveille externes et l'exécution d'investigations numériques en temps réel des menaces potentielles au sein d'un environnement virtuel « jetable ».

EN CONCLUSION

Un SDDC peut améliorer de façon significative le niveau de sécurité d'une entreprise ; réduire ses coûts informatiques, ses coûts de fonctionnement et ses dépenses d'investissement ; renforcer la fiabilité générale du réseau et des applications ; et assurer une plus grande flexibilité dès lors que les entreprises migrent vers des clouds publics, privés ou hybrides.