

NE MISEZ PAS VOTRE AVENIR SUR LES SERVICES RÉSEAU D'HIER

La modernisation, l'automatisation
et la sécurité reposent sur un DDI de
niveau entreprise

TABLE DES MATIÈRES

INTRODUCTION	3
LES SERVICES DE RÉSEAU ESSENTIELS ASSURENT VOTRE SURVIE NUMÉRIQUE	5
LES SERVICES RÉSEAU HÉRITÉS NE PEUVENT TOUT SIMPLEMENT PAS RÉPONDRE AUX BESOINS ACTUELS	6
LE STATU QUO NUIT AUX ENTREPRISES	7
POURQUOI UN DDI DE NIVEAU ENTREPRISE EST LA PREMIÈRE ÉTAPE DE LA MODERNISATION IT	8
LE DDI DE NIVEAU ENTREPRISE EST LA BASE D'UNE INFRASTRUCTURE IT MODERNE	9
LA SUITE DE PRODUITS INFOBLOX UNIVERSAL DDI™ OFFRE DES SERVICES RÉSEAU ESSENTIELS DE NIVEAU ENTREPRISE INÉGALÉS	11
INFOBLOX UNIVERSAL DDI REPOSE SUR CES PILIERS DE LA MODERNISATION	14
INFOBLOX UNIVERSAL DDI : CONÇU POUR L'AVENIR	15

LES COÛTS CACHÉS DES SERVICES RÉSEAU ESSENTIELS DISPARATES

Dans l'entreprise hyperconnectée d'aujourd'hui, le DNS, le DHCP et la gestion des adresses IP (DDI) ne sont pas de simples services en arrière-plan — ils constituent la base des opérations numériques sécurisées et évolutives. Pourtant, de nombreuses entreprises continuent de s'appuyer sur des infrastructures vieillissantes et fragmentées, convaincues que cela reste « suffisant ».

Ce qu'on oublie souvent, c'est que les solutions obsolètes coûtent cher, non seulement en argent, mais aussi en temps d'arrêt, en exposition aux risques et en perte de productivité. Selon des recherches récentes*, les organisations utilisant un DDI non adapté aux exigences d'entreprise sont nettement plus vulnérables aux perturbations opérationnelles, connaissent des délais de récupération plus longs après des pannes, font face à des taux d'échec plus élevés lors des audits et subissent des coûts plus importants.



* 9 pièges liés à l'absence de DDI de qualité professionnelle, Enterprise Strategy Group, février 2025

**À MESURE QUE
LES DEMANDES
AUGMENTENT
DANS LES
SERVICES
D'IDENTITÉ, DE
CLOUD ET DE
PÉRIPHÉRIE, LE
DDI DE NIVEAU
ENTREPRISE
N'EST PAS
QU'UNE
SIMPLE MISE À
NIVEAU, C'EST
UN IMPÉRATIF
POUR LA
MODERNISATION.**

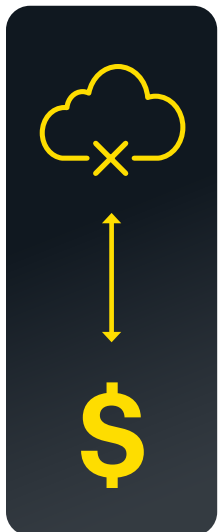
**SI LE DNS D'UNE
ENTREPRISE
TOMBE EN
PANNE, LE
MONDE
MODERNE
S'ARRÊTE :
PLUS DE
TRANSACTIONS,
PLUS DE
VOLS, PLUS
D'ÉLECTRICITÉ.
TOUT SE FIGE.**

PRINCIPAUX DÉFIS LIÉS AUX DNS, DHCP ET IPAM TRADITIONNELS ET CLOISONNÉS :

- ❗ **Panne imprévue**
- ❗ **Manque de visibilité et de contrôle**
- ❗ **Perte de productivité**
- ❗ **Coûts plus élevés**
- ❗ **Problèmes de mise à l'échelle**
- ❗ **Points de défaillance uniques**
- ❗ **Vulnérabilités de sécurité plus importantes**

LES SERVICES RÉSEAU ESSENTIELS ASSURENT VOTRE SURVIE NUMÉRIQUE

Votre organisation peut moderniser ses applications et son cloud, mais sans un DNS et DHCP de niveau entreprise, toute la base est en danger. Presque toutes les applications modernes, des systèmes de planification des ressources d'entreprise (ERP) aux plateformes d'identification, s'appuient sur le DNS comme point d'entrée numérique. Un seul champ d'application DHCP mal configuré peut empêcher des départements entiers d'accéder au réseau.



LE VÉRITABLE COÛT DES INTERRUPTIONS

Les défaillances de DNS et DHCP ne sont plus de simples problèmes informatiques, elles représentent aujourd'hui des risques majeurs pour les organisations. Le coût moyen d'une panne de réseau peut atteindre jusqu'à 9 000 \$ par minute* pour les grandes entreprises, et ce chiffre explose lorsque les incidents affectent les systèmes orientés client ou les processus critiques.

CAS CONCRET :

Un détaillant mondial, s'appuyant sur une infrastructure vieillissante de Microsoft DNS a rencontré un problème de synchronisation qui a perturbé les systèmes de point de vente (POS) dans plus de 100 magasins pendant trois heures.

» PERTE DE CHIFFRE D'AFFAIRES ESTIMÉE ? 7,5 MILLIONS DE DOLLARS.
LA CONFIANCE DES CLIENTS ? ENCORE PLUS DIFFICILE À RÉTABLIR.

**LES DÉFAILLANCES
DE DNS ET DHCP
PEUVENT
PROVOQUER DES
PANNES RÉSEAU
MÉDIATISÉES
ET ATTIRER
L'ATTENTION
DU CONSEIL
D'ADMINISTRATION.**

* Le véritable coût des interruptions, Forbes, David Flower, Forbes Technology Council, 10 avril 2024

**LA
TRANSFORMATION
NUMÉRIQUE SANS
UN DDI DE NIVEAU
ENTREPRISE
EST COMME
CONSTRUIRE
UN GRATTE-CIEL
SUR DES SABLES
MOUVANTS.**

LES SERVICES RÉSEAU HÉRITÉS NE PEUVENT PAS RÉPONDRE AUX BESOINS ACTUELS

Les entreprises ne peuvent pas se permettre de parier sur des outils DNS et DHCP obsolètes, surtout à mesure que la transformation numérique s'accélère. Ce qui fonctionnait il y a dix ans ne suffit tout plus aux besoins d'aujourd'hui.

RISQUE OPÉRATIONNEL

Les systèmes existants reposent souvent sur des interdépendances fragiles, entre DNS, DHCP et Microsoft Active Directory, tous déployés sur le même serveur Windows. Et, comme mentionné précédemment, un seul point de défaillance peut déclencher des pannes en cascade.

INEFFICACITÉS FINANCIÈRES

La prise en charge des infrastructures héritées nécessite souvent des effectifs dédiés pour la maintenance, les correctifs et le dépannage. Ajoutez à cela des cycles de renouvellement matériel coûteux, et votre courbe de coûts DDI devient incontrôlable.

VISIBILITÉ FRAGMENTÉE

La plupart des déploiements DDI existants ne disposent pas d'une vue consolidée, en temps réel et faisant autorité, de l'utilisation des adresses IP ou de l'état des actifs dans les environnements hybrides et multicloud. Cette visibilité réduite entraîne des retards dans l'identification et l'isolement des endpoints compromis, un suivi et un rapprochement manuels des adresses IP dans des feuilles de calcul, des difficultés à faire respecter la conformité et les pistes d'audit, ainsi que des conflits et des chevauchements d'adresses IP.

GOULOTS D'ÉTRANGLEMENT DE L'INNOVATION

Les systèmes DDI hérités ralentissent l'automatisation, limitent les intégrations et obligent les équipes DevOps à s'appuyer sur des tickets manuels ou des scripts obsolètes.

DANS L'ENSEMBLE, LES OUTILS HÉRITÉS NE PEUVENT PAS SUIVRE

Des fonctionnalités telles que les retards de synchronisation DNS, l'absence de corbeille et un contrôle d'accès basé sur les rôles (RBAC) limité font que les systèmes hérités ne sont pas fiables à grande échelle. Pire encore, nombre d'entre eux nécessitent une console de gestion par serveur, ce qui crée des silos opérationnels et augmente les risques de modifications de la configuration.

LE STATU QUO NUIT AUX ENTREPRISES

Les services essentiels de réseau cloisonnés posent de nombreux défis aux gestionnaires de réseau, de cloud et de sécurité, et offrent davantage d'opportunités aux acteurs malveillants. Quel que soit le secteur dans lequel vous opérez, si vous continuez à développer votre avenir numérique avec des services de réseau dépassés, vous vous exposez à des risques majeurs.

Comment un ransomware a paralysé les soins aux patients

- Un gang de ransomware a visé un système hospitalier majeur
- Les services DNS/DHCP et d'annuaire partageaient le même serveur, ce qui bloque l'accès au moment où le dépannage est le plus urgent
- Le téléchargement par un seul employé a conduit à la compromission de serveurs critiques
- Les opérations de santé se sont effondrées : les dossiers, téléphones et portails patients sont tombés en panne
- 5,6 millions de dossiers de patients affectés par des semaines de perturbations

**Coût total :
1,3 milliard
de dollars**

Les coûts cachés de la mise à jour des serveurs

- Un fournisseur d'énergie gère 400 serveurs nécessitant 4 800 correctifs par an
- Avec un taux d'échec de 1 %, cela signifiait 48 pannes par an
- On estime qu'environ 50 employés sont inactifs pendant quatre heures à chaque fois
- Coût horaire moyen par employé : 100 \$

Impact annuel des interruptions : 960 000 \$

Un crash en juillet 2024 qui a fait le tour du monde

- La plus grande panne informatique de l'histoire
- Des millions de serveurs sont tombés en panne
- Des services DNS/DHCP critiques interrompus dans le monde entier
- 10 000 vols cloués au sol
- D'innombrables hôpitaux affectés

Des milliers d'entreprises compromises

Selon une étude récente de Forrester, le DDI de niveau entreprise permet d'économiser considérablement du temps et de l'argent :

7,1 millions \$ d'économies
en passant d'une infrastructure héritée à un DDI moderne*

De 2 jours à 1 heure de gain de temps

en ce qui concerne le déploiement de machines virtuelles (VM) sur 1 000 sites**

14 000 heures
économisées sur le réseau grâce au DDI moderne

* The Total Economic Impact™ d'Infoblox DDI, Forrester Consulting, octobre 2023

** Les résultats d'une entreprise

POURQUOI UN DDI DE NIVEAU ENTREPRISE EST LA PREMIÈRE ÉTAPE DE LA MODERNISATION IT

Le passage au cloud hybride, au Zero Trust et à l'edge computing ne commence pas par de nouvelles applications ou des interfaces utilisateur attrayantes. Cela commence par des services réseau essentiels, fiables, évolutifs et sécurisés.

DNS, DHCP ET IPAM UNIFIÉS = DDI

Pour transformer votre réseau, vous devez d'abord transformer la façon dont il est déployé et géré. Le DDI de niveau entreprise intègre le déploiement et la gestion du DNS, du DHCP et de la gestion des adresses IP (IPAM) dans un flux de travail unique. Cette combinaison simplifie la complexité des services de réseau traditionnels et rationalise les opérations commerciales. Elle améliore également la visibilité du cloud hybride et inter-cloud, ce qui facilite l'automatisation des processus tout en vous permettant d'exécuter des services réseau sur site ou dans le cloud. Elle est spécialement conçue pour fournir la résilience, la visibilité et l'automatisation requises par les entreprises modernes.

En fait, les organisations qui utilisent un DDI de niveau entreprise ont signalé une augmentation de plus de 60 % de la productivité des tâches DDI, avec moins d'étapes manuelles et moins d'erreurs de configuration. Une entreprise a été en mesure de remplacer à 100 % des outils DDI vieillissants et non Microsoft et de réduire de plus de 50 % l'ensemble de l'infrastructure Microsoft requise.

LE DDI DE NIVEAU ENTREPRISE EST LA BASE D'UNE INFRASTRUCTURE IT MODERNE



GESTION CENTRALISÉE ET UNIFIÉE

Les solutions DDI de niveau entreprise offrent une automatisation et une orchestration centralisées des fonctions DNS, DHCP et IPAM dans divers environnements : sur site, hybrides et multi-cloud. En unifiant ces services réseau essentiels sous une console de gestion unique, les équipes informatiques bénéficient de :

- Opérations simplifiées
- Application améliorée des politiques
- Efficacité opérationnelle



VISIBILITÉ ACCRUE

Une plateforme DDI d'entreprise offre une visibilité en temps réel sur chaque appareil et service IP du réseau, ce qui est essentiel pour le contrôle opérationnel et la sécurité. Parmi les fonctionnalités clés, on trouve également :

- Découverte dynamique des ressources
- Suivi des baux et utilisation des adresses IP
- Analyse intégrée



OPTIONS DE DÉPLOIEMENT FLEXIBLES

Le DDI de niveau entreprise vous permet de déployer des services selon les objectifs commerciaux et vos stratégies IT, sans être limité par des conceptions de produits rigides. Cette flexibilité offre :

- Une prise en charge native du cloud et hybride
- Un DNS/DHCP sans infrastructure, proposé en tant que service
- Des options d'appareils virtuels et physiques
- Une architecture évolutive



ADMINISTRATION BASÉE SUR LES RÔLES

Les plateformes DDI de niveau entreprise intègrent des contrôles d'accès renforcés pour faciliter la collaboration entre les équipes NetOps, SecOps et CloudOps tout en garantissant la responsabilité. Cette administration collaborative permet :

- Un accès basé sur les autorisations
- Une possibilité d'audit et un suivi des modifications
- Une administration déléguée



POSTURE DE SÉCURITÉ RENFORCÉE

Les solutions DDI de niveau entreprise renforcent la sécurité en utilisant le DNS comme élément fondamental de la cybersécurité. Cette sécurité accrue comprend le blocage proactif du trafic vers les domaines malveillants et l'arrêt des attaques basées sur le DNS. Grâce à ses capacités de sécurité intégrées, les DDI modernes permettent :

- Une sécurité préventive
- Une visibilité en temps réel sur le trafic DNS et les anomalies
- Des politiques de sécurité cohérentes dans les environnements hybrides et multi-cloud

**LA MODERNISATION NE VISE PAS À APPORTER
DES CHANGEMENTS PAR PUR PLAISIR.
ELLE OFFRE RÉSILIENCE, VISIBILITÉ ET
RATIONALITÉ OPÉRATIONNELLE.**





LA SUITE DE PRODUITS INFOBLOX UNIVERSAL DDI™ OFFRE DES SERVICES RÉSEAU ESSENTIELS DE NIVEAU ENTREPRISE INÉGALÉS

Infoblox Universal DDI™ est la suite de produits DDI de niveau entreprise la plus puissante du secteur grâce à sa combinaison de gestion centralisée et de contrôle, d'automatisation, d'évolutivité et de sécurité dans les environnements hybrides, multi-cloud et sur site. Elle unifie le DNS, le DHCP et l'IPAM en une seule plateforme intégrée qui offre une visibilité en temps réel, une automatisation intelligente et une plus grande disponibilité pour les services réseau essentiels fonctionnant sur site ou sur des systèmes DNS natifs sur le cloud, comme AWS, Google Cloud et Azure. Elle permet également aux entreprises de continuer à utiliser leur DNS natif sur le cloud tout en utilisant Universal DDI pour la gestion.

L'architecture cloud-native d'Infoblox permet également des options de déploiement flexibles qui s'alignent sur les stratégies informatiques modernes des entreprises, tandis que des fonctionnalités avancées telles que l'intégration de la threat intelligence et l'extensibilité pilotée par API donnent aux entreprises les moyens de rationaliser leurs opérations, d'améliorer leur posture de sécurité et de soutenir la transformation numérique à l'échelle. Grâce à sa fiabilité éprouvée et à son adoption par les entreprises du monde entier, Universal DDI est la référence en matière de gestion et de sécurisation des réseaux complexes et dynamiques modernes.



GESTION UNIFIÉE ET CENTRALISÉE SUR LES CLOUDS ET SUR SITE

À la base, Universal DDI consolide le DNS, le DHCP et l'IPAM dans un plan de contrôle unifié, ce qui permet de rationaliser la gestion de ces services réseau essentiels dans l'infrastructure sur site et chez les trois principaux fournisseurs de cloud : AWS, Azure et Google Cloud. En centralisant le contrôle, Universal DDI :

- Élimine les silos
- Améliore la sécurité
- Permet un déploiement plus rapide des services réseau
- Simplifie les opérations
- Réduit le risque de mauvaises configurations



UNE VISIBILITÉ APPROFONDIE PERMET UNE MEILLEURE SÉCURITÉ ET CONFORMITÉ

Grâce à une visibilité en temps réel sur les plages d'adresses IP configurées, l'utilisation, l'état des baux, etc., les équipes informatiques peuvent détecter de manière proactive les anomalies, appliquer les politiques et éviter les surprises coûteuses. Certaines entreprises ont obtenu :



» **60 %**

d'identification plus rapide des appareils compromis lors d'incidents de sécurité

» **Plus de 70 %**

de temps en moins consacré à la préparation des rapports de conformité



DES OPTIONS DE DÉPLOIEMENT FLEXIBLES POUR S'ADAPTER À VOTRE ARCHITECTURE.

Que vous ayez besoin d'un modèle DDI as-a-service, physique ou virtuel sur site, ou hybride, Infoblox s'adapte à vos besoins. Déployez des services à la périphérie, sur le cloud ou les deux, avec une gestion des politiques des services distribués, assurant cohérence et automatisation intégrées.



PREUVE À L'APPUI : une entreprise de logistique mondiale a réduit le provisionnement des sites périphériques de sept jours à deux heures grâce aux modèles de déploiement automatisés d'Infoblox.



L'ADMINISTRATION BASÉE SUR LES RÔLES SIMPLIFIE LA GOUVERNANCE

Attribuez facilement des rôles en fonction des fonctions, des zones géographiques ou des exigences de conformité. Fini les accès tout ou rien ou les dérogations manuelles risquées.



PREUVE À L'APPUI : une agence fédérale américaine a utilisé Infoblox RBAC pour prendre en charge plus de 1 200 utilisateurs tout en assurant une séparation stricte entre les réseaux classifiés et non classifiés.



UNE SÉCURITÉ DNS QUI ARRÊTE LES MENACES PLUS TÔT

Infoblox Universal DDI offre une sécurité intégrée de niveau entreprise via Infoblox Threat Defense™. En intégrant les capacités DNS de protection avec DNS, DHCP et IPAM dans une plateforme unifiée, les équipes de sécurité peuvent arrêter les menaces de manière préventive, en moyenne plus de 63 jours avant les autres solutions. Universal DDI :

- Bloque de manière préventive le trafic vers les domaines malveillants et de phishing
- Stoppe les menaces basées sur le DNS, y compris le commandement et contrôle (C2), l'exfiltration de données et l'algorithme de génération de domaine (DGA), en temps réel.
- Identifie les domaines similaires pour protéger la réputation de la marque
- Applique des politiques de sécurité cohérentes du terminal jusqu'au cloud
- Accélère la réponse aux incidents avec la priorisation des événements DNS et l'attribution des endpoints

SÉPARER LES SERVICES ESSENTIELS RENFORCE LA RÉSILIENCE



Les DDI de qualité professionnelle dissocient les services réseau de l'identité, garantissant la disponibilité, la visibilité et la sécurité dans les environnements hybrides. Infoblox modernise les services réseau essentiels grâce à des solutions DDI résilientes, conçues pour répondre aux exigences d'échelle, de sécurité, d'automatisation et de contrôle d'accès basé sur les rôles.



NIST

National Institute of Standards and Technology SP 800-81

2.3.1. Services DNS dédiés : les cybercriminels et d'autres acteurs chercheront à amplifier et maximiser les perturbations de tout cyber-incident en attaquant les systèmes critiques, notamment les cibles qui hébergent plusieurs composants critiques.

Pour garantir la cyber-résilience, la coexistence de plusieurs services essentiels à la mission sur un même système doit être limitée (c'est-à-dire, séparation des tâches).

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.ipd.pdf>

INFOBLOX UNIVERSAL DDI PERMET D'ACCÉDER À CES PILIERS DE LA MODERNISATION



MODERNISATION DE L'IDENTITÉ



Défi :

Une entreprise était en train de migrer vers des plateformes hybrides de gestion des identités (Okta et Azure AD), mais ses services DNS et DHCP restaient liés à l'annuaire Microsoft Active Directory sur site.

Solution :

Infoblox Universal DDI a découplé les services réseau critiques de l'infrastructure héritée et a fourni des services DNS et DHCP natifs du cloud et évolutifs, avec une visibilité et une gestion unifiées.

Résultats :

- ✓ Migration transparente de plateforme de gestion des identités hybrides
- ✓ Meilleure disponibilité et plus grande facilité de gestion
- ✓ Réduction de la dépendance à l'ancien Microsoft Active Directory

Universal DDI a assuré une transformation d'identité fluide, sécurisée et évolutive, sans interruption.

TRANSFORMATION CLOUD



Défi :

Un grand fournisseur de soins de santé a migré ses charges de travail vers AWS et Azure, mais a rencontré des difficultés pour gérer le DNS dans des environnements fragmentés sur site et dans le cloud.

Solution :

Infoblox Universal DDI a fourni une plateforme centralisée pour la gestion des DNS à travers plusieurs fournisseurs de cloud et infrastructures privées.

Résultats :

- ✓ Visibilité à 360 degrés sur les environnements hybrides
- ✓ Disponibilité accrue et gestion simplifiée
- ✓ Automatisation simplifiée pour DevOps
- ✓ Prestation de services sécurisée et résiliente

100 %

abandon des anciens outils de sécurité DNS

30 %+

Gain de productivité SOC

MODERNISATION DES SERVICES EDGE



Défi :

Avec l'essor du travail à distance, de l'IoT et du traitement en périphérie, une entreprise de logistique avait besoin d'un DNS/DHCP fiable sur des dizaines de nœuds périphériques, sans présence informatique.

Solution :

Infoblox Universal DDI automatise le provisionnement DNS/DHCP à la périphérie avec des services résilients et gérés à distance.

Résultats :

- ✓ Configuration instantanée du site avec provisionnement sans contact
- ✓ 70 % de réduction du nombre de pannes sur les sites à distance
- ✓ Posture de sécurité renforcée avec un contrôle centralisé

Infoblox a apporté des services réseau de niveau entreprise à la périphérie, sans envoyer de personnel informatique sur le terrain.



**PARCE QUE SI LE
DNS TOMBE EN
PANNE, VOTRE
ENTREPRISE
S'ARRÊTE.
C'EST AUSSI
SIMPLE QUE CELA.**

infoblox®

INFOBLOX UNIVERSAL DDI : CONÇU POUR L'AVENIR

Pour les entreprises qui naviguent dans la transformation numérique et qui ont besoin de services réseau fiables, sécurisés et évolutifs, Universal DDI est une plateforme DDI native du cloud qui unifie la gestion, automatise les opérations et sécurise la périphérie. Contrairement aux outils DNS et DHCP hérités et cloisonnés, Infoblox fournit une infrastructure réseau moderne qui permet à l'entreprise d'être agile, résiliente, sécurisée et de réaliser des économies.

Infoblox Universal DDI n'est pas seulement une mise à niveau ; c'est une exigence fondamentale pour l'entreprise moderne. C'est ainsi que vous construisez un réseau résilient, réactif et adapté.



PRÊT À DÉPASSER LE STATU QUO ?

Pour en savoir plus, rendez-vous sur :

infoblox.com/fr/networkmodernization



Infoblox réunit réseau, sécurité et cloud pour former une base opérationnelle aussi résiliente qu'agile. Nous intégrons, sécurisons et automatisons de manière transparente les services réseau essentiels pour que les entreprises puissent se développer rapidement sans compromis.

Siège social
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr