

# Dell EMC PowerMax et VMAX All Flash : Embedded Management

Embedded Management (eManagement) avec Dell EMC Unisphere for PowerMax

## Résumé

Ce livre blanc fournit une présentation d'Embedded Management sur les systèmes Dell EMC™ PowerMax et VMAX™ All Flash.

Septembre 2020

## Révisions

Date	Description
Mai 2018	version initiale
Septembre 2019	Mises à jour pour la version PowerMaxOS du 3e trimestre 2019
Septembre 2020	Mises à jour pour la version PowerMaxOS du 3e trimestre 2020

## Remerciements

Auteur : Kevin Vaillancourt

Les informations contenues dans cette publication sont fournies « en l'état ». Dell Inc. ne fournit aucune déclaration ou garantie d'aucune sorte concernant les informations contenues dans cette publication et rejette plus spécialement toute garantie implicite de qualité commerciale ou d'adéquation à une utilisation particulière.

L'utilisation, la copie et la diffusion de tout logiciel décrit dans cette publication nécessitent une licence logicielle en cours de validité.

Copyright © 2018-2020 Dell Inc. ou ses filiales. Tous droits réservés. Dell Technologies, Dell EMC, Dell EMC et les autres marques citées sont des marques de Dell Inc. ou de ses filiales. D'autres marques éventuellement citées sont la propriété de leurs détenteurs respectifs. [01/11/2021] [Livre blanc technique] [H16856.3]

# Table des matières

Révisions.....	2
Remerciements.....	2
Table des matières .....	3
Synthèse .....	4
<b>1 Hyperviseur PowerMax .....</b>	<b>5</b>
1.1 Allocation des cœurs du processeur de l'hyperviseur : émulation multicœur .....	5
1.2 Allocation de mémoire à l'hyperviseur.....	6
1.3 Allocation de stockage à l'hyperviseur : appareil Cut-through .....	6
1.4 Connectivité réseau de l'hyperviseur .....	7
<b>2 Embedded Management .....</b>	<b>8</b>
2.1 Haute disponibilité d'eManagement .....	10
2.2 Sécurité de l'authentification Unisphere .....	12
<b>3 vApp Manager .....</b>	<b>14</b>
3.1 Exportation de fichiers log et de performances .....	15
3.2 Modifications de configuration .....	17
3.3 SÉCURITÉ DE L'AUTHENTIFICATION vApp Manager .....	19
3.4 Certificats.....	19
<b>4 Configuration client/serveur Solutions Enabler .....</b>	<b>21</b>
4.1 Configuration du serveur .....	21
4.2 Configuration du client.....	22
<b>5 Conclusion.....</b>	<b>24</b>
<b>A Support technique et ressources.....</b>	<b>25</b>
A.1 Ressources associées.....	25

## Synthèse

[La famille Dell EMC PowerMax](#) et les clients VMAX All Flash peuvent tirer parti de la gestion simplifiée des baies avec Dell EMC™ Unisphere™ for PowerMax intégré. Unisphere est une interface de gestion Web HTML5 intuitive qui permet aux responsables IT d'optimiser la productivité en réduisant considérablement les temps de provisionnement, de gestion et de surveillance des ressources de stockage.

Embedded Unisphere permet aux clients de simplifier la gestion, de réduire les coûts et d'améliorer la disponibilité en exécutant le logiciel de gestion de PowerMax et de VMAX All Flash directement sur la baie. Embedded Unisphere est configuré selon les paramètres d'usine afin de garantir une durée de configuration minimale sur site. La fonctionnalité s'exécute dans un conteneur au sein de l'hyperviseur PowerMaxOS, ce qui évite aux clients d'allouer leur propre équipement pour gérer leurs baies. Outre Unisphere, d'autres éléments essentiels du service de données eManagement incluent Solutions Enabler, Database Storage Analyzer et les logiciels de gestion SMI-S.

Unisphere for PowerMax offre les atouts indispensables pour accélérer la migration vers les datacenters All-Flash, tels que la simplification, la flexibilité et l'automatisation. Ce système est adapté aux clients qui assemblent et désassemblent fréquemment les configurations de stockage. En effet, Unisphere for PowerMax facilite la reconfiguration de la baie en simplifiant les procédures de suppression et de réaffectation des volumes. Avec Unisphere for PowerMax, les clients peuvent définir des configurations SRDF multisites en quelques minutes.

# 1 Hyperviseur PowerMax

PowerMaxOS 5978 s'exécute sur Dynamic Virtual Matrix pour tirer parti de la flexibilité scale-out des cœurs, du cache et des interfaces hôtes de cette architecture. L'hyperviseur de stockage intégré limite les besoins matériels et réseau externes, fournit des niveaux de disponibilité élevés et réduit énormément la latence. Les mises à niveau d'Hypervisor sont effectuées sans interruption de service.

Au sein de l'Hypervisor PowerMax, les machines virtuelles (VM) fournissent la plate-forme hôte qui comprend un traitement des processeurs, de la mémoire, une carte réseau (NIC), des ports, un stockage de données à l'aide d'un appareil Cut-through (CTD) et un réseau externe via la station pilote des modules de gestion (MMCS). Les VM sont exécutées au sein de l'émulation FA frontale.

La Figure 1 présente les principaux composants de PowerMax et de l'hyperviseur.

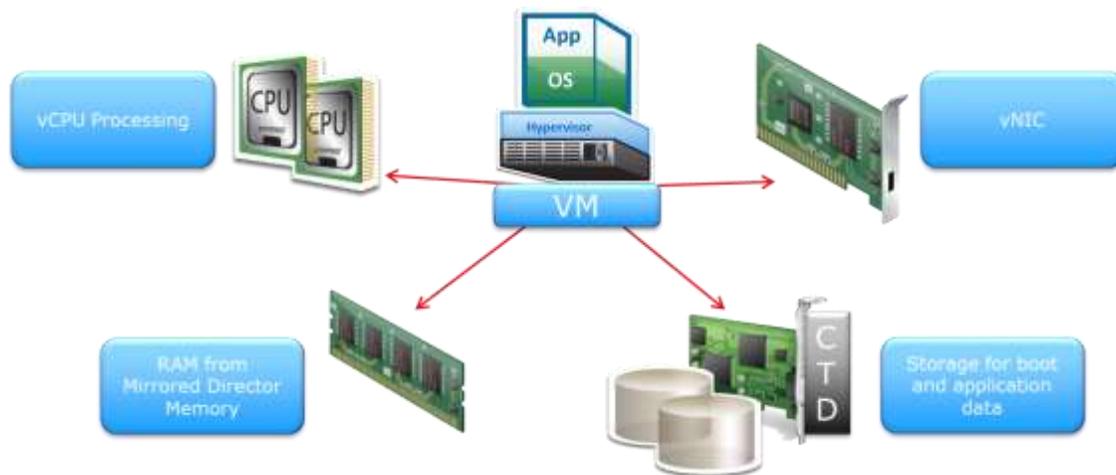


Figure 1 Concepts de l'hyperviseur : machines virtuelles

## 1.1 Allocation des cœurs du processeur de l'hyperviseur : émulation multicœur

En utilisant la nouvelle capacité d'émulation multicœur de PowerMax et VMAX All Flash, le traitement des processeurs est fourni à l'aide des cœurs de processeurs de l'émulation FA. Les cœurs sont mis en commun pour les fonctionnalités frontales, dorsales et pour PowerMaxOS comme le montre la Figure 2. Tous les cœurs de processeurs sur le directeur fonctionnent sur les E/S de tous les ports. Ainsi, les ports directeurs sont toujours répartis de manière équilibrée.

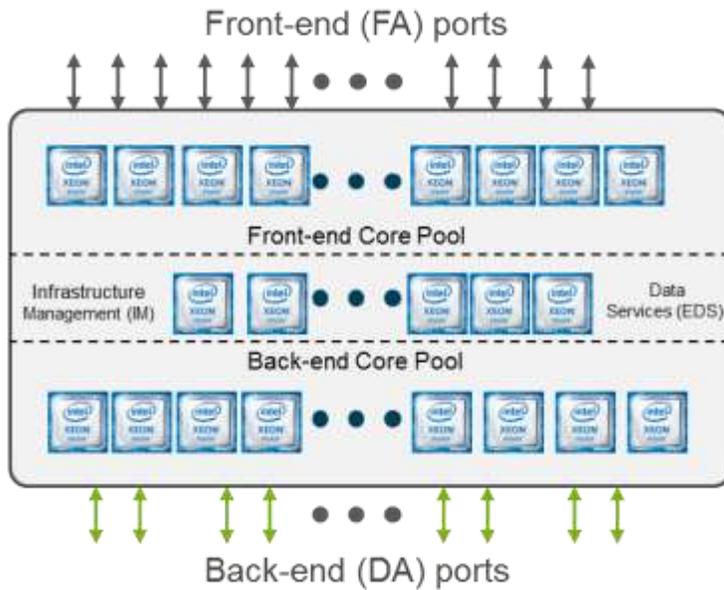


Figure 2 Émulation multicœur PowerMax

## 1.2 Allocation de mémoire à l'hyperviseur

La mémoire est allouée à l'hyperviseur, comme indiqué dans la Figure 3 depuis le cache directeur lors de la configuration initiale. Cette mémoire est ensuite allouée à chaque machine virtuelle (VM) sur ce directeur pour les applications intégrées. La quantité de mémoire allouée à une machine virtuelle dépend du type d'application, par exemple Embedded Management.

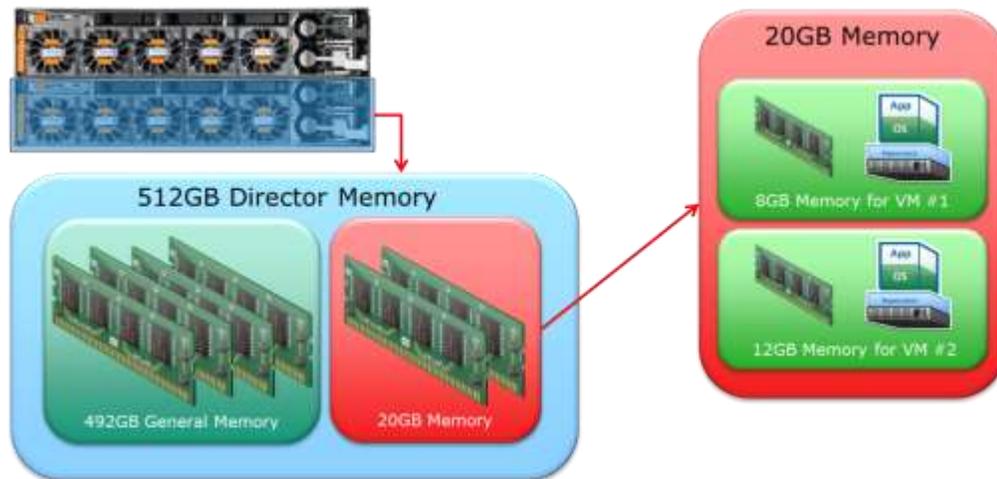


Figure 3 Allocation de mémoire à l'hyperviseur

## 1.3 Allocation de stockage à l'hyperviseur : appareil Cut-through

Le stockage de données de démarrage et d'applications est fourni à l'aide d'un appareil Cut-through (CTD), comme illustré dans la Figure 4, qui sert d'adaptateur HBA accédant aux LUN dans PowerMax et VMAX All Flash. Le CTD a deux composants permettant d'activer l'accès aux LUN via un port FA. Le premier est le thread de serveur CTD. Il s'exécute sur l'émulation FA et communique avec le client CTD dans le système d'exploitation intégré. Le second est le pilote client CTD. Le pilote client CTD est intégré dans le système d'exploitation hôte et communique avec le serveur CTD en s'exécutant sur l'émulation FA. Un système d'exploitation s'exécutant dans une VM doit disposer du pilote client CTD installé, afin d'accéder aux LUN.

Les ports d'applications intégrés sont des ports virtuels spécifiquement fournis pour une utilisation par les VM contenant les applications, comme le NAS intégré. Ils correspondent aux ports 32 à 63 pour l'émulation FA directeur. Les ports virtuels sont fournis pour éviter le conflit d'accès avec la connectivité physique. Comme pour les ports physiques, les LUN peuvent être provisionnés sur les ports virtuels.

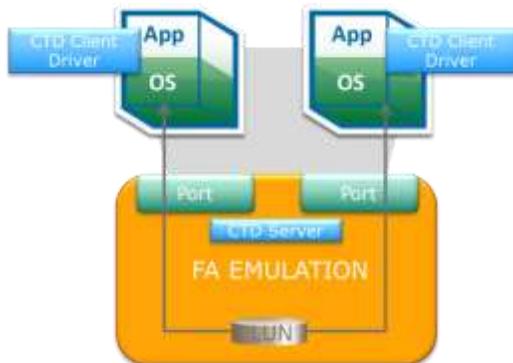


Figure 4 Appareil Cut-through (CTD)

## 1.4 Connectivité réseau de l'hyperviseur

La connectivité réseau pour les VM est fournie par une carte réseau virtuelle (vNIC). La vNIC est connectée au réseau interne pour fournir des communications à PowerMaxOS et d'autres instances de VM. La connectivité réseau externe de gestion de la VM est fournie via un composant PowerMaxOS appelé la passerelle NAT (Network Address Translation), qui fait partie de l'émulation du gestionnaire d'infrastructure (IM). La passerelle NAT (Network Address Translation) fournit des services de traduction entre les adresses IP internes et externes et utilise une connexion réseau séparée sur chacune des deux stations pilotes des modules de gestion (MMCS). Une baie PowerMax ou VMAX All Flash avec eManagement et connectivité ESRS nécessiterait alors un total de quatre connexions réseau physiques et quatre adresses IP. D'autres adresses IP sont requises si le NAS intégré est également configuré.

## 2 Embedded Management

Unisphere est une application Web HTML5 qui vous permet de configurer et de gérer les systèmes de stockage PowerMax et VMAX All Flash. Le terme Unisphere comprend « Unisphere for PowerMax » pour la gestion des systèmes PowerMax et All Flash Storage exécutant PowerMaxOS 5978, et « Unisphere for VMAX » pour la gestion des systèmes VMAX All Flash et VMAX Storage exécutant HYPERMAX OS 5977 et Enginuity OS 5876. HTML5 Unisphere offre plusieurs avantages :

- Sécurité renforcée
- Réduction du temps de réponse des applications
- Interface utilisateur à l'aspect moderne
- Alignement avec d'autres produits Dell EMC
- Gestion des comptes d'utilisateurs et des rôles
- Exécution d'opérations de configuration (création de volumes dynamiques, masquage de volumes, définition d'attributs de stockage, définition d'attributs de volume et définition de balises de port)
- Exécution et surveillance des opérations de réplication et de sauvegarde :
  - TimeFinder™ SnapVX
  - TimeFinder VP Snap
  - TimeFinder/Clone
  - TimeFinder/Mirror
  - Symmetrix Remote Data Facility (SRDF™)
  - Open Replicator for Symmetrix (ORS)
  - PowerProtect Storage Direct
- Gestion des fonctionnalités de stockage avancées, telles que :
  - Niveaux de service
  - Planification des charges applicatives
  - Technologie LUN virtuelle améliorée
  - Groupes de provisionnement automatisé
  - Provisionnement virtuel
  - Migration sans interruption (NDM)
  - NAS intégré (eNAS)
  - Cloud Mobility
- Surveillance des alertes, y compris la possibilité de configurer des notifications d'alerte externes
- Surveillance des données de performances du système de stockage :
  - Surveillance des performances et de la capacité au fil du temps
  - Analyse des données pour enquêter sur les problèmes
  - Visualisation de graphiques représentant les performances système en détail
  - Définition de seuils de performances et d'alertes
  - Affichage des mesures haute fréquence en temps réel
  - Analyse des causes premières
  - Affichage des cartes thermiques du système de stockage
  - Exécution de rapports planifiés et continus (requêtes) et exportation de ces données dans un fichier
  - Utilisation de tableaux de bord prédéfinis pour la plupart des composants du système
  - Personnalisation de vos propres modèles de tableau de bord
  - Exportation planifiée des tableaux de bord de performances
- Surveillance et dépannage des problèmes de performances des bases de données à l'aide de Database Storage Analyzer

---

**Remarque :** ProtectPoint a été renommé PowerProtect Storage Direct.

---

Unisphere a toujours été installé sur un serveur Windows ou Linux dédié, ou déployé en tant qu'appliance virtuelle (vAPP). Cette approche permet au client de gérer plusieurs systèmes à partir d'une seule instance Unisphere. Avec la version d'HYPERMAX OS 5977.691.684 et versions ultérieures, il est possible d'exécuter Unisphere en tant qu'appliance directement sur les contrôleurs VMAX All Flash au sein de l'hyperviseur natif. Cette option, appelée Embedded Management (eManagement), élimine la nécessité pour un hôte de gestion externe de contrôler et de gérer les baies PowerMax et VMAX All Flash.

eManagement est installé comme deux machines virtuelles pour la redondance et la haute disponibilité. Les machines virtuelles sont réparties en fonction de l'architecture de paires en miroir des baies PowerMax et VMAX All Flash afin d'assurer une consommation régulière des ressources, favorisant à la fois les performances et la capacité.

eManagement utilise les ressources suivantes :

- 8 cœurs de processeurs logiques partagés (4 par eManagement, partagés avec l'émulation FA)
- Espace de stockage total de 818 Go (démarrage, persistant et partagé)
- 2 adresses IP
- Le nombre total de ressources de mémoire varie en fonction du modèle, comme décrit dans la Tableau 1.

Tableau 1 Comparaison des ressources Unisphere

Composants de	VMAX All Flash				PowerMax	
	VMAX 250F/FX	VMAX 450F/FX	VMAX 850F/FX	VMAX 950F/FX	PowerMax 2000	PowerMax 8000
Mémoire (Go)	24	32	40	40	24	40

Pour lancer Unisphere, saisissez l'une des URL suivantes dans un navigateur Web :

- [https://<eManagement\\_IP>:8443](https://<eManagement_IP>:8443)
- [https://<eManagement\\_host\\_name>:8443](https://<eManagement_host_name>:8443)

Dans la fenêtre de connexion, comme illustré à la Figure 5, saisissez le nom d'utilisateur et le mot de passe de l'utilisateur de configuration initiale Unisphere, puis cliquez sur Login.

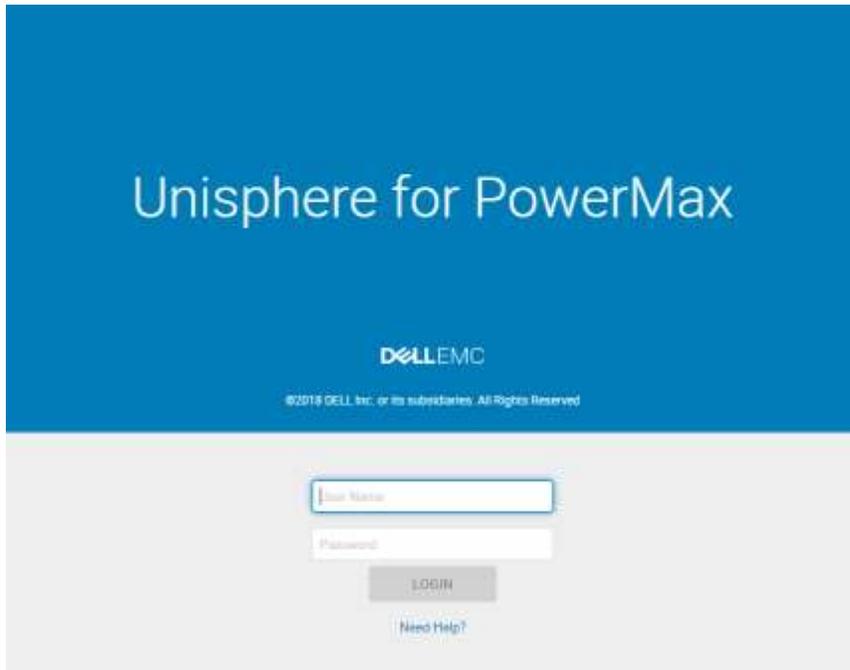


Figure 5 Fenêtre de connexion Unisphere for PowerMax

Le nom d'utilisateur par défaut de l'utilisateur de configuration initiale Unisphere est **smc**, et le mot de passe par défaut est **smc**.

---

**Remarque :** pour plus d'informations sur l'utilisation d'Unisphere, consultez l'aide en ligne Unisphere.

---

## 2.1 Haute disponibilité d'eManagement

La haute disponibilité d'eManagement est obtenue via un modèle actif/en veille pour les services intégrés suivants :

- Unisphere
- SMIS

Les services suivants s'exécutent en tant que services locaux sur chacune des machines virtuelles eManagement :

- vApp Manager
- Processus Solutions Enabler
  - Base
  - GNS
  - Watchdog
  - STP
  - Serveur SYMAPI
  - Witness Manager

Unisphere répondra aux demandes des clients sur les deux adresses IP externes dans toutes les conditions normales de fonctionnement, y compris après un basculement. La Figure 6 montre comment les connexions réseau pour les services actifs/en veille basculent des machines virtuelles eManagement actives aux machines virtuelles eManagement en veille.

Lorsque l'instance Unisphere active devient indisponible en provoquant un basculement, les utilisateurs de l'interface utilisateur Unisphere seront sujets à des erreurs dans les activités en cours et les séquences de l'assistant seront interrompues. L'utilisateur est déconnecté lors d'un basculement. Les programmes clients REST rencontrent des erreurs lors de l'échec et du basculement, mais peuvent être écrits pour récupérer automatiquement de ces erreurs.

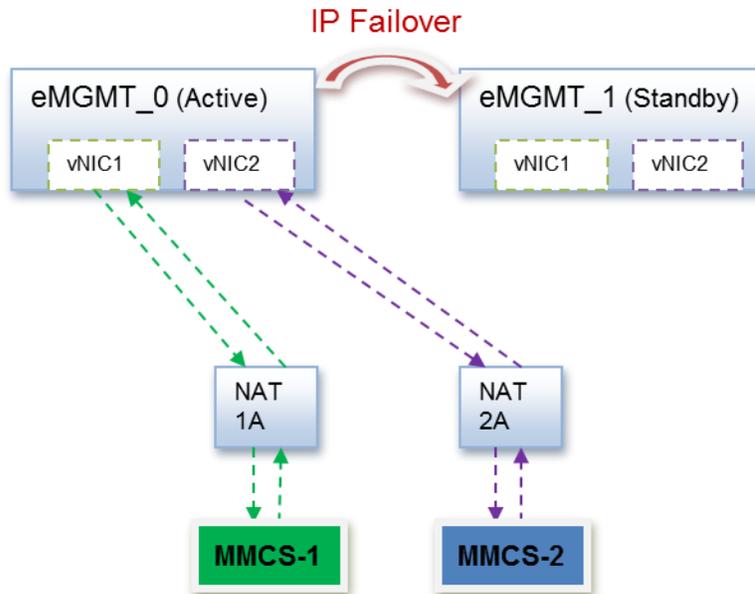


Figure 6 Scénario de basculement de l'adresse IP des services actifs/en veille eManagement

Sur la machine virtuelle eManagement en veille, les processus SMAS et SMAS DB seront affichés comme non exécutés. Il s'agit d'un état normal qui peut être affiché dans le volet vApp Manager Manage Daemons, comme illustré dans la Figure 7.

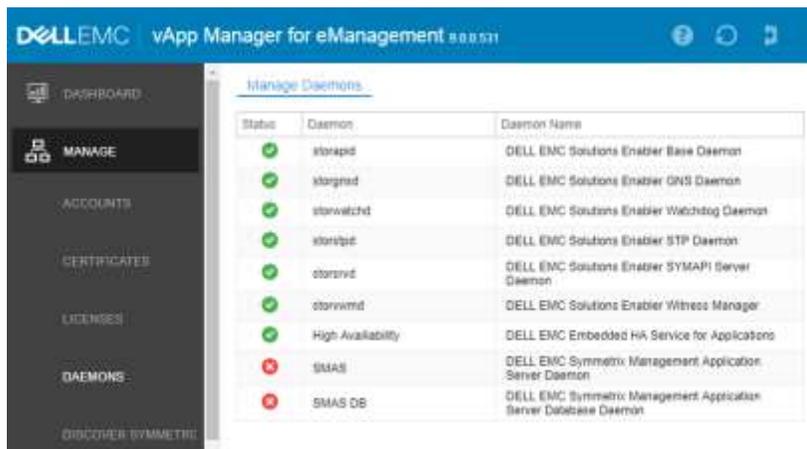


Figure 7 Processus eManagement en veille

## 2.2 Sécurité de l'authentification Unisphere

Embedded Unisphere prend en charge les types d'authentification suivants :

- LDAP
  - Les utilisateurs se connectent avec leur nom d'utilisateur et leur mot de passe LDAP-SSL (s'ils possèdent un compte d'utilisateur stocké sur un serveur LDAP-SSL).
  - Pour utiliser cette méthode, un administrateur Unisphere ou SecurityAdmin configure l'authentification LDAP-SSL dans Unisphere. L'aide en ligne Unisphere contient des instructions sur l'exécution de ces tâches.
- Utilisateurs locaux Unisphere
  - Les utilisateurs se connectent avec leur nom d'utilisateur et leur mot de passe Unisphere (s'ils possèdent un compte d'utilisateur Unisphere local).
  - Pour utiliser cette méthode, un utilisateur de configuration initiale Unisphere, un administrateur ou SecurityAdmin crée un compte d'utilisateur local Unisphere pour l'utilisateur. Les comptes d'utilisateur locaux sont stockés localement sur l'hôte du serveur SMAS et fonctionnent de la même manière que les autres méthodes de validation des informations d'identification de l'utilisateur. L'aide en ligne Unisphere contient des instructions sur l'exécution de ces tâches.
- Authentification utilisateur par certificat X.509
  - L'authentification des utilisateurs à l'aide de certificats X.509 est prise en charge sur eManagement. Un certificat émis par une autorité de certification (CA) tierce publique et de confiance peut être utilisé pour authentifier l'identité de confiance lors de l'utilisation du client Web Unisphere ou des interfaces d'API REST. L'utilisation de cartes à puce d'identité numérique telles que les cartes CAC (Common Access Card) et PIV (Personal Identity Verification) dans le cadre d'un processus d'authentification à plusieurs facteurs est également prise en charge.
  - L'authentification des utilisateurs par certificat peut être activée dans l'Assistant d'importation de certificats de vApp Manager et, après confirmation, le choix devient irréversible. Les certificats d'autorité de certification doivent être importés avant que l'authentification des utilisateurs par certificat puisse être utilisée. L'aide en ligne vApp Manager contient des instructions sur l'exécution de ces tâches.

Pour afficher les autorités d'authentification, comme le montre la Figure 8, ouvrez le panneau **Settings**, puis cliquez sur **Users and Groups > Authentication**.

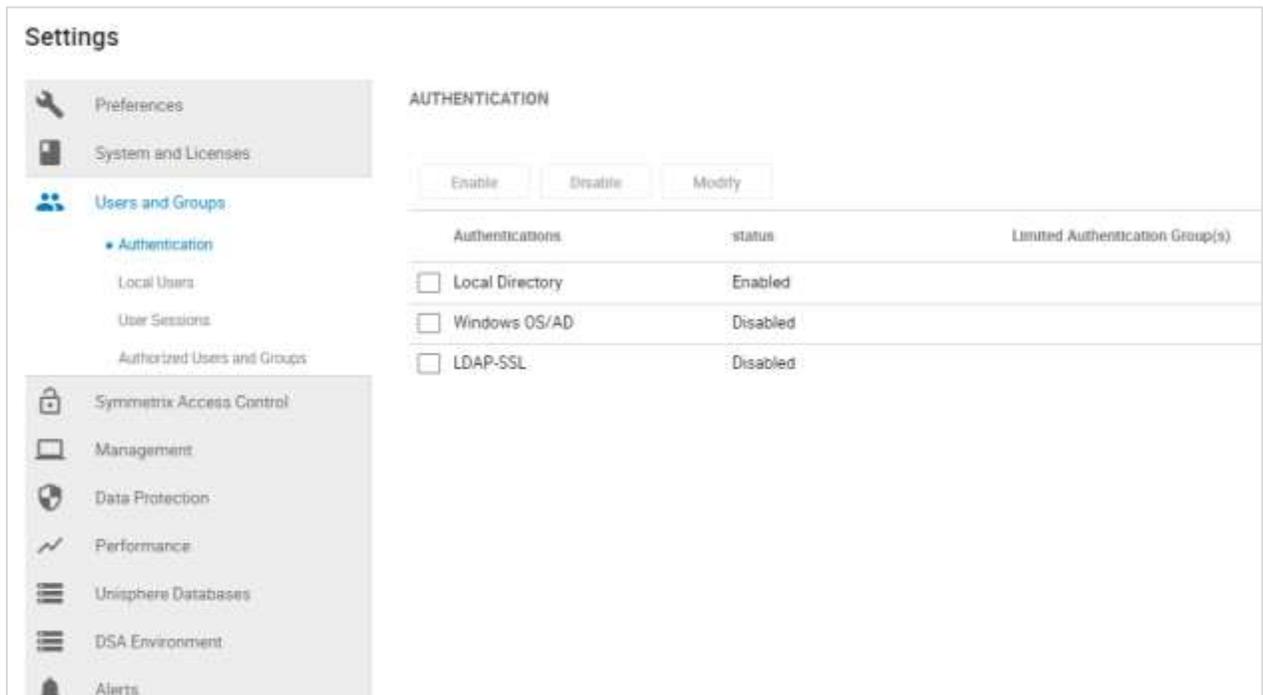


Figure 8 Authentication Unisphere

**Remarque :** Le système d'exploitation Microsoft® Windows® et Active Directory® s'appliquent uniquement à Unisphere installé sur des hôtes Windows.

Le *Guide de configuration de la sécurité Dell EMC PowerMax* fournit des informations supplémentaires sur l'authentification, l'autorisation et d'autres problèmes liés à la sécurité.

## 3 vApp Manager

Chaque conteneur eManagement inclut également un gestionnaire d'appliance virtuelle HTML5 (vApp) qui permet de configurer votre environnement de stockage. À l'aide de l'interface Web de vApp Manager, vous pouvez effectuer les tâches suivantes :

- Démarrer Unisphere
- Surveiller l'état de l'application
- Démarrer et arrêter les processus sélectionnés
- Télécharger des données persistantes
- Configurer le fichier nethost (requis pour l'accès client)
- Découvrir les systèmes de stockage
- Modifier les options et les options de processus
- Ajouter des clés de licence basées sur l'hôte
- Exécuter un ensemble limité de commandes CLI Solutions Enabler
- Charger les eLicenses basées sur VMAX et PowerMax
- Configurer l'annuaire LDAP
- Télécharger des logs de débogage SYMAPI
- Importer un certificat signé par une autorité de certification pour les navigateurs Web
- Importer un certificat personnalisé pour le processus storsrvd
- Vérifier l'utilisation du disque
- Effacer les fichiers temporaires
- Redémarrer l'appliance
- Configurer les entrées symavoid
- Gérer les utilisateurs
- Réinitialiser le nom d'hôte
- Mettre à jour le fichier /etc/hosts

vApp Manager est accessible en accédant à l'une des URL suivantes dans un navigateur Web :

- [https://<eManagement\\_IP>:5480](https://<eManagement_IP>:5480)
- [https://<eManagement\\_host\\_name>:5480](https://<eManagement_host_name>:5480)

Lorsque l'utilisateur se connecte pour la première fois, la connexion par défaut est utilisée avec le nom d'utilisateur et le mot de passe en tant que **seconfig**.

---

**Remarque :** Le mot de passe par défaut doit être modifié pour chacune des deux instances de vApp Manager.

---

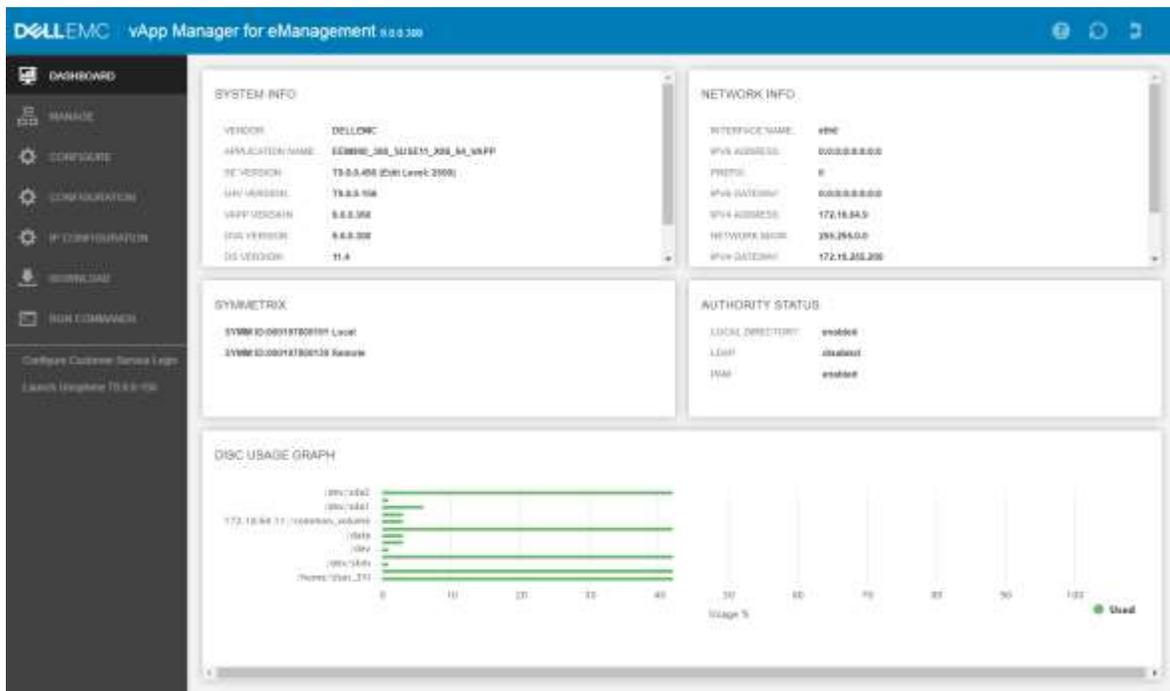


Figure 9 Tableau de bord vApp Manager for eManagement

Le tableau de bord vApp Manager de la Figure 9 fournit des détails sur la version d'eManagement, les informations réseau, l'autorité d'authentification et l'utilisation du disque. Ce livre blanc traite des tâches courantes. Pour obtenir des informations détaillées sur l'utilisation de vApp Manager, consultez l'aide en ligne de Dell EMC vApp Manager for eManagement.

### 3.1 Exportation de fichiers log et de performances

Les fichiers log et de performances suivants sont disponibles dans le menu Téléchargement de vApp Manager illustré à la Figure 10 :

- Journaux processus
- Journaux persistants
- Fichiers Grab Dell EMC
- Journaux vApp Manager
- Exporter les fichiers journaux et de données
- Effacer les fichiers temporaires

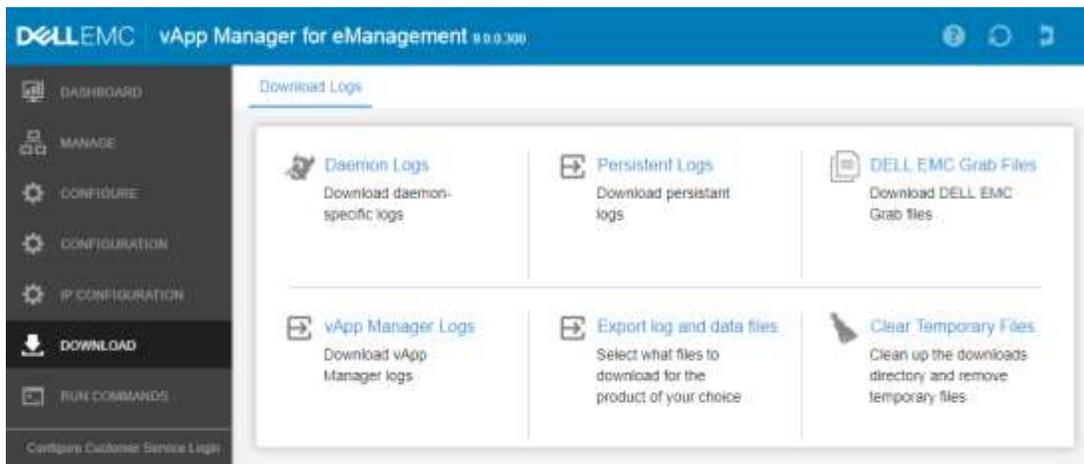


Figure 10 Journaux de téléchargement de vApp

Pour exporter des fichiers spécifiques, sélectionnez **Export log and data files**. Une fenêtre d'option s'ouvre pour sélectionner le journal du produit et le fichier de données que vous souhaitez télécharger, comme indiqué sur la Figure 11. Après avoir sélectionné le produit, la Figure 12 indique comment les fichiers peuvent être filtrés et sélectionnés en fonction de la date et du nom du fichier.

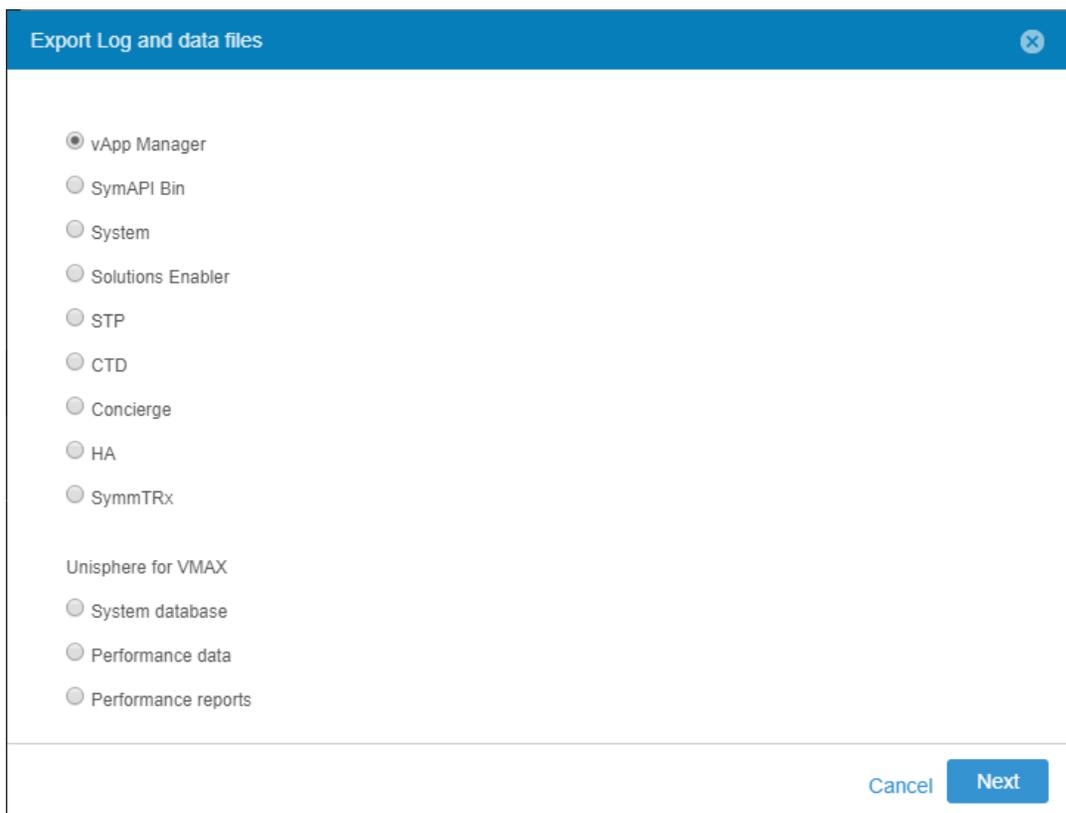


Figure 11 Exporter les fichiers journaux et de données

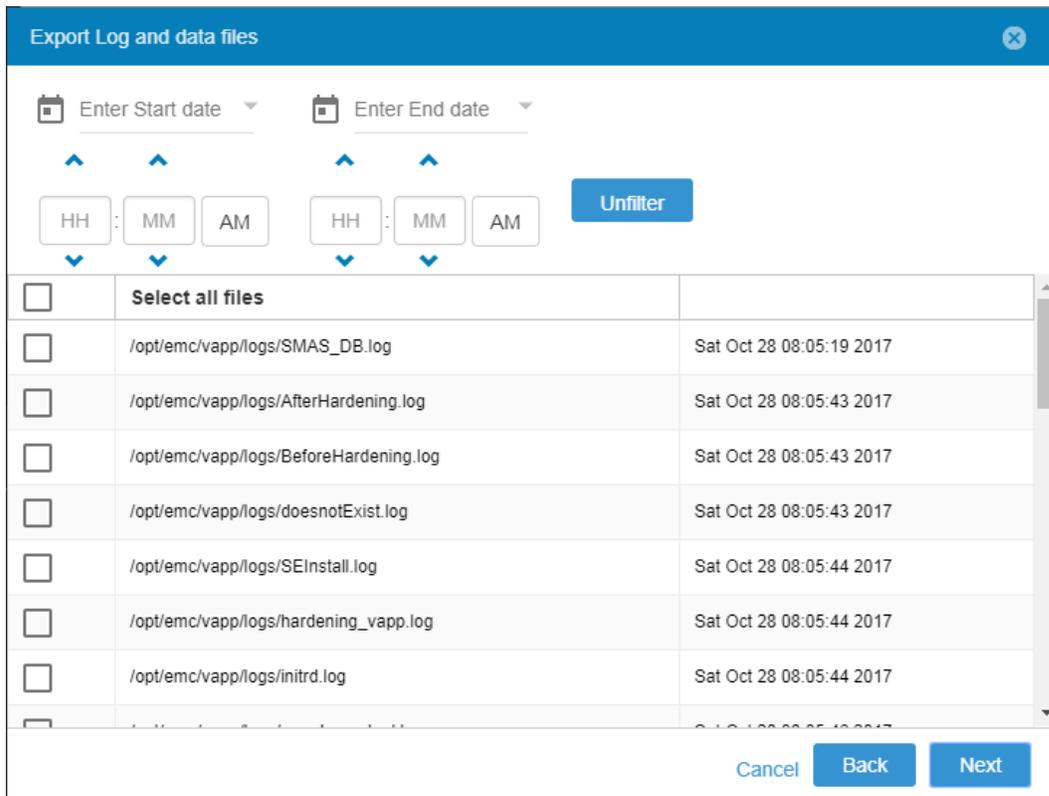


Figure 12 Filtrer et sélectionner un fichier

## 3.2 Modifications de configuration

L'adresse IP eManagement, le nom d'hôte, les serveurs DNS et la configuration NTP sont configurés au moment de l'installation de PowerMax et VMAX All Flash. En utilisant vApp Manager for eManagement, ces paramètres peuvent être modifiés sans l'intervention du service client.

Pour modifier le nom d'hôte ou de domaine, allez sur le volet Configuration hôte dans vApp Manager, comme indiqué sur la Figure 13, en sélectionnant **Configure > Host**. Ensuite, sélectionnez Change Host Name ou Change Domain Name.

Dans le volet Configuration hôte, le fichier des hôtes eManagement peut être modifié pour ajouter des hôtes qui ne font pas partie du DNS configuré.

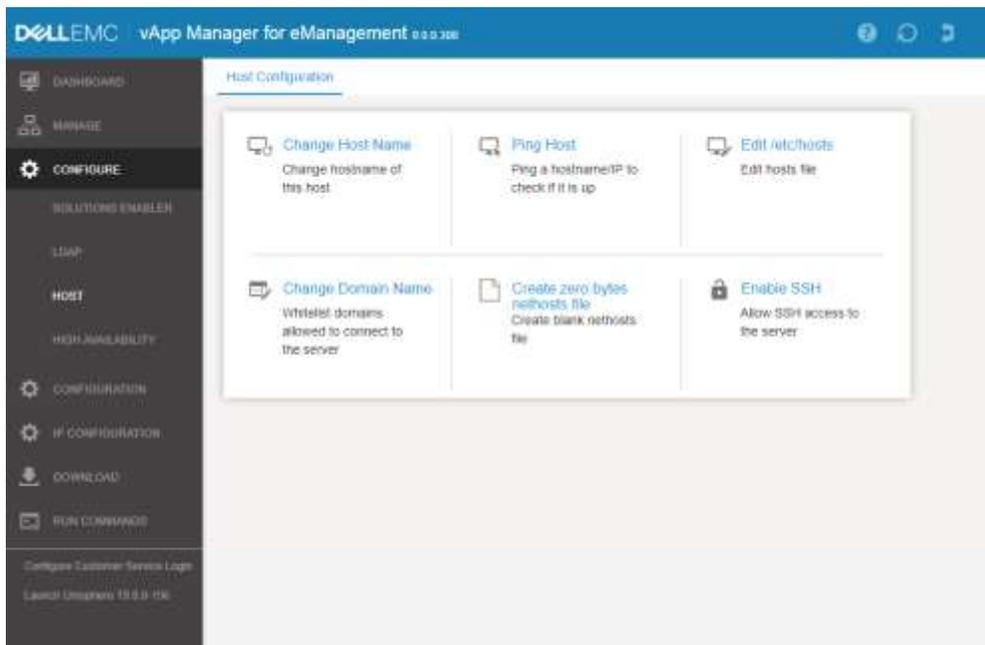


Figure 13 Configuration hôte

Pour afficher ou modifier la configuration IP d'eManagement, allez sur IP Configuration et IPv4 ou IPv6. Sur la Figure 14, vous avez la possibilité d'**obtenir la configuration (Get Config)** et d'afficher les valeurs actuelles, de modifier les valeurs actuelles en saisissant la nouvelle valeur dans la zone de texte, puis cliquer sur **Set Config** ou effacer la zone de texte avec **Reset Config**.

**Remarque :** Les plages d'adresses IP internes restreintes par défaut qui ne doivent pas être utilisées sont les suivantes : 172.16.0.0/16 ; 172.17.0.0/16 ; 172.18.0.0/16. Pour plus d'informations, consultez le *Guide de planification du site pour PowerMax*.

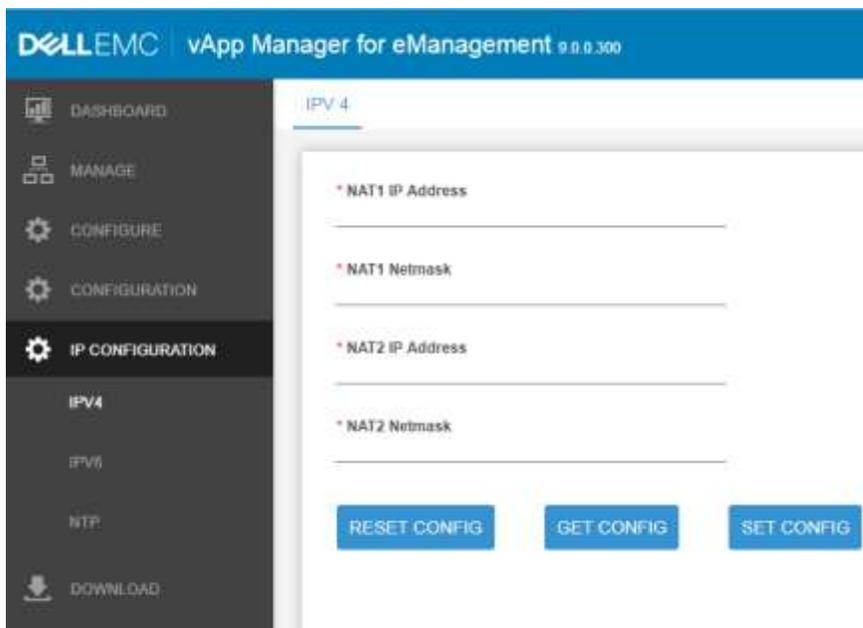


Figure 14 Configuration IP

### 3.3 SÉCURITÉ DE L'AUTHENTIFICATION vApp Manager

vApp Manager fournit deux types d'authentification utilisateur :

- Authentification du répertoire local (nom d'utilisateur et mot de passe)
- Authentification LDAP (Lightweight Directory Access Protocol)

LDAP permet de distribuer des services d'informations d'annuaire sur un réseau d'hôtes. Un client doit fournir un ensemble de paramètres pour configurer LDAP, qui permet ensuite la connexion au serveur LDAP et sécurise la communication entre les hôtes sur le réseau.

Pour configurer LDAP, allez sur l'Assistant de configuration LDAP, comme indiqué sur la Figure 15 en sélectionnant **Configurer > LDAP** et en remplissant les champs obligatoires.

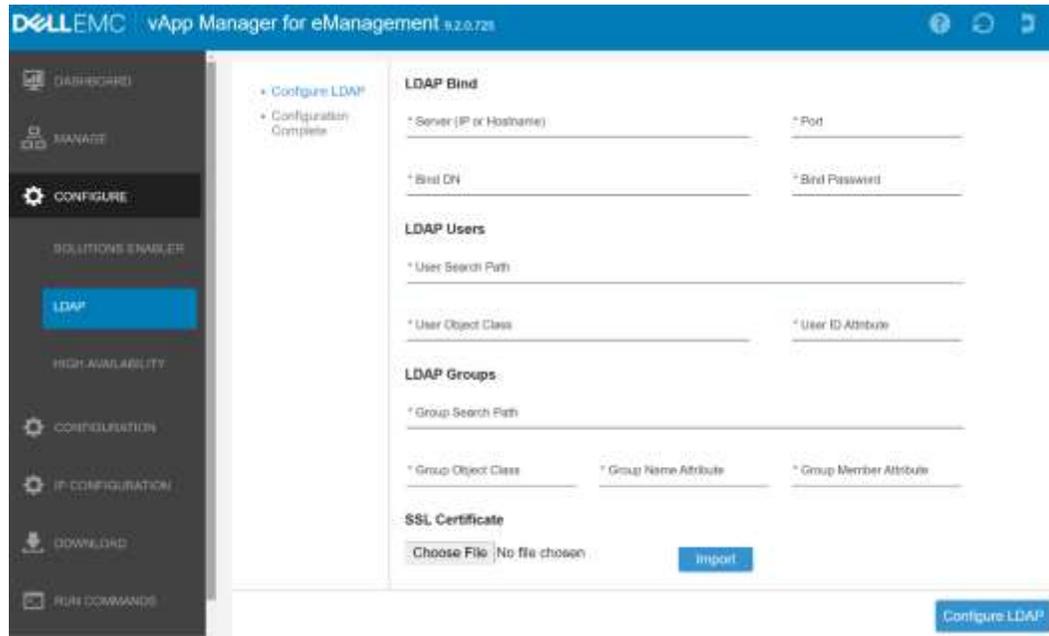


Figure 15 Assistant LDAP vApp

La gestion des utilisateurs locaux et authentifiés LDAP est effectuée en sélectionnant **Manage > Accounts**.

### 3.4 Certificats

Un certificat est un document électronique utilisé pour identifier un serveur, une société ou une autre entité, et associe cette identité à une clé publique. Lors de l'installation, le programme d'installation génère et installe le certificat de serveur auto-signé utilisé pour la sécurité au niveau du transport HTTPS. Les utilisateurs peuvent remplacer ce certificat par celui émis par un tiers de confiance à l'aide de vApp Manager.

Une autorité de certification (CA) est une entité tierce qui valide les identités et émet des certificats. Le certificat émis par l'autorité de certification lie une clé publique particulière au nom de l'entité que le certificat identifie (par exemple, le nom d'un serveur ou d'un appareil). Seule la clé publique que le certificat certifie fonctionne avec la clé privée correspondante appartenant à l'entité que le certificat identifie. Les certificats permettent d'éviter l'utilisation de fausses clés publiques pour l'usurpation d'identité.

Une demande de signature de certificat (CSR) est un message qu'un demandeur génère et envoie à une autorité de certification afin de demander un certificat d'identité numérique. La plupart des sociétés CA tierces ont besoin d'une CSR avant de créer un certificat numérique. Lorsqu'une CSR est générée, une paire de clés est également créée. Le demandeur qui envoie la CSR conserve la clé privée et demande à l'autorité de certification de signer le certificat. Cette méthode est plus sécurisée, car la clé privée reste avec le demandeur.

vApp Manager fournit un Assistant qui vous guide tout au long du processus d'obtention d'une CSR et d'importation de certificats CA pour l'appliance et pour Unisphere.

Le processus d'obtention d'un certificat CA est le suivant :

1. Créer un certificat auto-signé
2. Créer une CSR
3. Soumettre la CSR
4. Importer un certificat signé par une autorité de certification
5. Vérifier le certificat signé par l'autorité de certification

Pour remplacer le certificat de vApp Manager, Unisphere Server ou Solutions Enabler, allez sur l'Assistant d'importation de certificats, comme indiqué sur la Figure 16, en sélectionnant **Manage > Certificates**. Sélectionnez l'application appropriée pour importer le certificat SSL du client.

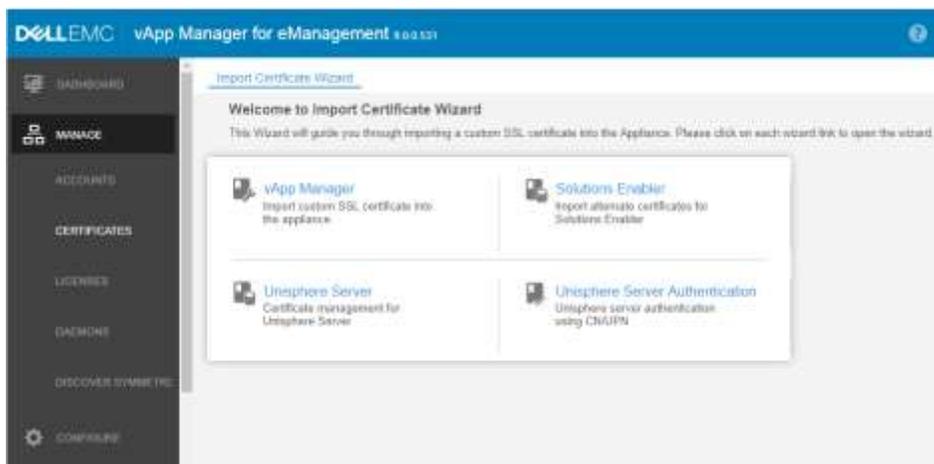


Figure 16 Assistant d'importation de certificats

Pour activer l'authentification utilisateur par certificat X.509, sélectionnez l'Assistant d'authentification du serveur Unisphere.

---

**Remarque :** Pour plus d'informations sur les étapes d'importation des certificats, consultez l'aide en ligne de vApp Manager.

---

## 4 Configuration client/serveur Solutions Enabler

Solutions Enabler fournit aux hôtes l'interface de ligne de commande Symmetrix (SYMCLI). SYMCLI est un ensemble complet de commandes permettant de gérer votre environnement. Les commandes de SYMCLI peuvent être appelées sur la ligne de commande ou dans les scripts. Ces commandes permettent de surveiller la configuration et l'état des appareils, ainsi que d'effectuer des opérations de contrôle sur les appareils et les objets de données qui se situent dans votre environnement de stockage. eManagement ne fournit pas d'interface de ligne de commande directe pour les administrateurs qui souhaitent être en mesure d'utiliser l'interface de ligne de commande riche en fonctionnalités de Solutions Enabler, mais il fournit un mécanisme client/serveur permettant d'y parvenir.

### 4.1 Configuration du serveur

Le serveur eManagement doit être configuré pour accepter les connexions client/serveur. Pour ce faire, configurez le processus storsrvd. L'accès à l'administration du système est fourni par vApp Manager pour eManagement.

La vApp eManagement est configurée en tant que serveur, qui exécute le processus storsrvd et fournit l'accès au serveur SYMAPI. Seuls les hôtes configurés via les paramètres nethost peuvent se connecter en tant que clients pour exécuter les commandes SYMCLI de Solutions Enabler. Si votre serveur eManagement a été configuré avec des serveurs DNS capables de résoudre le nom de domaine complet (FQDN) de votre hôte qui exécutera Solutions Enabler, vous pouvez saisir le nom de domaine complet de votre serveur et un utilisateur autorisé dans le fichier nethosts. L'adresse IP du client peut être saisie si le DNS n'est pas disponible. Si plusieurs utilisateurs doivent être spécifiés pour un serveur, ils doivent être saisis un par un. Les caractères génériques sont également acceptés dans le champ utilisateur, mais cela n'est pas recommandé pour des problèmes de sécurité évidents.

Le menu de configuration du fichier nethosts est accessible à partir de l'onglet **Configure > Solutions Enabler**, comme illustré sur la Figure 17.

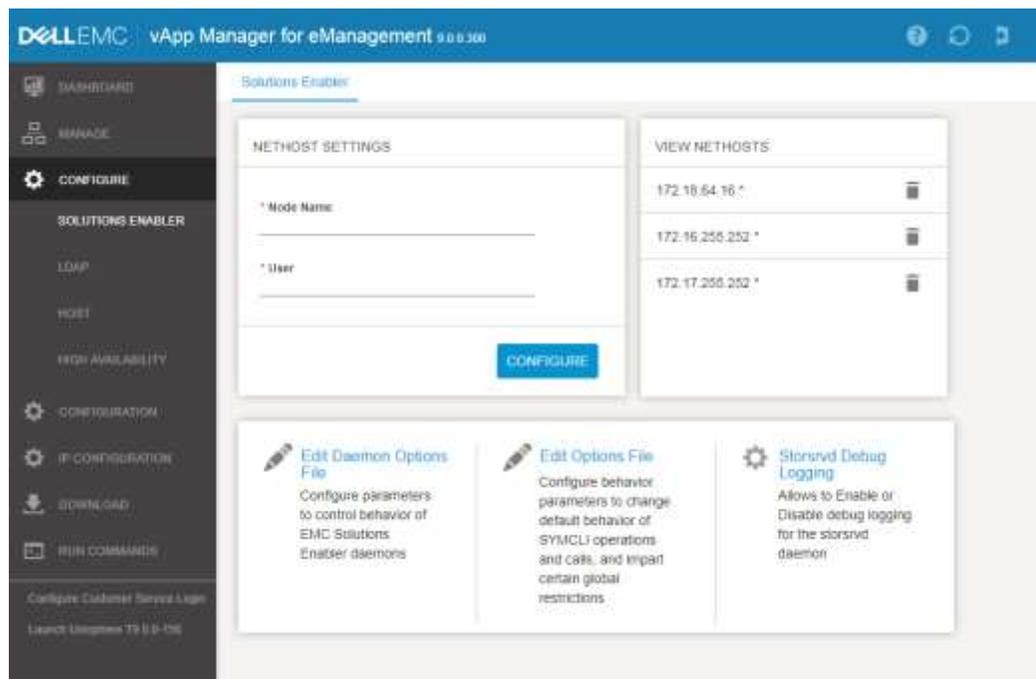


Figure 17 Configuration nethosts

Une fois que toutes les entrées des hôtes clients et des utilisateurs sont configurées, les paramètres sont visibles dans le volet View Nethosts. Si une erreur a été effectuée ou si une décision a été prise pour révoquer l'accès client/serveur pour un hôte, une option de suppression du nom d'hôte et de l'utilisateur se trouve à côté de l'entrée. Il vous suffit de sélectionner l'icône corbeille pour supprimer.

La configuration de base de Solutions Enabler doit être configurée pour permettre la communication client/serveur. Vous y accédez à partir de l'onglet **Configuration > Solutions Enabler Base Configuration**. Au bas des options se trouve **Use Access ID**, définissez cette valeur sur **ANY** comme indiqué sur la Figure 18.

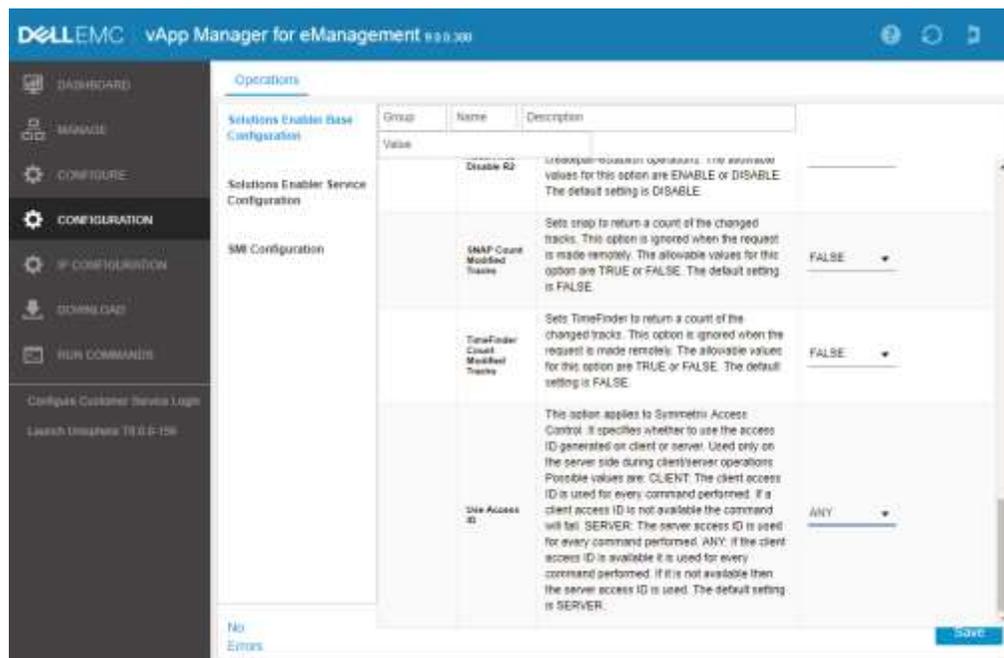


Figure 18 Configuration de base de Solutions Enabler > Utiliser l'ID d'accès

## 4.2 Configuration du client

Une fois le fichier nethosts configuré sur le serveur, l'étape suivante consiste à configurer le client pour l'accès au serveur. Solutions Enabler doit être installé sur l'hôte client. Téléchargez la version appropriée à partir de <https://support.emc.com> et suivez les instructions d'installation. Avec Solutions Enabler installé, le fichier netcfg doit être configuré pour pointer vers le serveur qui sera le serveur eManagement qui vient d'être configuré.

Le fichier netcfg se trouve dans C:\Program Files\EMC\SYMAPI\config sur les systèmes Windows et dans /var/symapi/config si l'hôte est Linux ou la plupart des variantes d'Unix. Si les emplacements par défaut ont été modifiés lors de l'installation de Solutions Enabler, ce fichier peut se trouver ailleurs.

Ouvrez le fichier netcnfg dans un éditeur de texte et faites défiler jusqu'à la fin. Les entrées par défaut sont similaires à celles affichées comme suit.

netcnfg par défaut :

```
#####
#
# This is a sample config for Ordered Pair of entries. SYMCLI will attempt #
# to use the first one, and on failure use the second. #
#
# SYMAPI_ORDERED Ordered TCPIP node001 WWW.XXX.YYY.ZZZ 2707 SECURE #
# SYMAPI_ORDERED Ordered TCPIP node002 WWW.XXX.YYY.AAA 2707 SECURE #
```

Les entrées par défaut peuvent être utilisées en supprimant le # au début et à la fin des lignes et en saisissant l'adresse IP des deux adresses IP externes (NAT) de vos serveurs eManagement. Les entrées Ordered tentent de se connecter à la première et, en cas d'échec, le client se connecte à la seconde conformément à la configuration haute disponibilité. Dans l'exemple ci-dessous, le fichier netcnfg a été modifié pour ajouter une chaîne de connexion personnalisée « eManagement ». À l'aide de cette méthode, il est possible d'avoir plusieurs entrées et de choisir de gérer l'un des nombreux systèmes.

Exemple de fichier netcnfg :

```
#####
#
# This is a sample config for Ordered Pair of entries. SYMCLI will attempt #
# to use the first one, and on failure use the second. #
#
# SYMAPI_ORDERED Ordered TCPIP node001 WWW.XXX.YYY.ZZZ 2707 SECURE #
# SYMAPI_ORDERED Ordered TCPIP node002 WWW.XXX.YYY.AAA 2707 SECURE #

eManagement Ordered TCPIP eManagement_host1 10.10.10.10 2707 SECURE
eManagement Ordered TCPIP eManagement_host2 10.10.10.11 2707 SECURE
```

Maintenant que le fichier netcnfg a été configuré, il ne reste plus qu'à définir une variable d'environnement dans votre invite de commande pour connecter le client au serveur et vérifier la connexion. L'exemple suivant montre la variable SYMCLI\_CONNECT définie sur un système Windows pour correspondre à l'entrée dans le fichier netcnfg. Sur les hôtes Linux/Unix, la commande d'exportation est remplacée par set.

Variable d'environnement SYMCLI :

```
C:\>set SYMCLI_CONNECT=eManagement
```

```
C:\>symcli -def
```

```
Symmetrix Command Line Interface (SYMCLI) Version V9.0.0.0 (Edit Level: 2500)
Built with SYMAPI Version V9.0.0.0 (Edit Level: 2500)
```

```
Current settings of the SYMCLI environment variables:
```

```
SYMCLI_CONNECT :eManagement
```

## 5 Conclusion

Embedded Unisphere for PowerMax permet aux clients de simplifier la gestion, de réduire les coûts et d'améliorer la disponibilité en exécutant le logiciel de gestion de PowerMax et de VMAX All Flash directement sur la baie.

Unisphere for PowerMax est une interface de gestion HTML5 intuitive qui permet aux responsables IT d'optimiser la productivité en réduisant considérablement les temps de provisionnement, de gestion et de surveillance des ressources de stockage. Unisphere for PowerMax offre les atouts indispensables pour accélérer la migration vers les datacenters All-Flash, tels que la simplification, la flexibilité et l'automatisation.

## A Support technique et ressources

[Dell.com/support](https://dell.com/support) propose des services et un support éprouvés répondant aux besoins des clients.

[Les livres blancs et vidéos techniques de stockage et de protection des données](#) fournissent une expertise qui contribue à garantir la réussite du client grâce à des produits de stockage et de protection des données Dell EMC.

### A.1 Ressources associées

- Aide en ligne de Dell EMC Unisphere for PowerMax
- Aide en ligne de Dell EMC vApp Manager for eManagement
- Guide de configuration de la sécurité de la famille Dell EMC PowerMax
- Guide de planification du site pour la famille Dell EMC PowerMax