Dell EMC Gamme Unity™

Dell EMC Unity 100 % Flash, Unity hybride, UnityVSA

Version 5.x

Guide de configuration de la sécurité

P/N 302-002-564 REV 09

DELL EMC

Publié en Juin 2019

EMC Computer Systems France
River Ouest 80 quai Voltaire CS 21002 95876 Bezons Cedex
Tél. : +33 1 39 96 90 00 Fax : +33 1 39 96 99 99
www.DellEMC.com/fr-fr/index.htm

SOMMAIRE

Ressources supplémentaires

En vue d'améliorer nos matériels et logiciels, des révisions sont régulièrement publiées. Par conséquent, il se peut que certaines fonctions décrites dans le présent document ne soient pas prises en charge par l'ensemble des versions des logiciels ou matériels actuellement utilisés. Pour obtenir les informations les plus récentes sur les fonctionnalités des produits, consultez les notes sur la version de vos produits. Si un produit ne fonctionne pas correctement ou ne fonctionne pas comme indiqué dans ce document, contactez un professionnel du support technique .

Obtenir de l'aide
Pour plus d'informations sur le support, les produits et les licences, procédez comme suit :

Informations sur les produits
Pour obtenir la documentation ou les notes de mise à jour relatives aux produits et fonctionnalités, accédez à la documentation technique Unity disponible sur le site : www.emc.com/fr-fr/documentation/unity-family.htm.

Résolution des problèmes
Pour obtenir des informations relatives aux produits, mises à jour logicielles, licences et services, consultez le site Web du support en ligne (enregistrement obligatoire) à l'adresse : https://Support.EMC.com. Après vous être connecté, recherchez la page de **support par produit** appropriée.

Support technique
Pour accéder au support technique et aux demandes de service, rendez-vous sur le site de support en ligne https://Support.EMC.com. Une fois connecté, recherchez **Créer une demande de service**. Pour pouvoir ouvrir une demande de service, vous devez disposer d'un contrat de support valide. Pour savoir comment obtenir un contrat de support valide ou si vous avez des questions concernant votre compte, contactez un responsable de compte.

Conventions utilisées dans ce document pour certains points particuliers

⚠ DANGER

Indique une situation dangereuse qui, si elle n'est pas évitée, entraînera des blessures graves voire mortelles.

⚠ AVERTISSEMENT

Indique une situation dangereuse qui, si elle n'est pas évitée, risque d'entraîner des blessures graves voire mortelles.

⚠ ATTENTION

Indique une situation dangereuse qui, si elle n'est pas évitée, risque d'entraîner des blessures mineures ou modérées.

NOTE

Indique des pratiques n'impliquant aucune blessure.

Remarque

Fournit des informations importantes, mais non vitales.

CHAPITRE 1

Introduction

Ce chapitre décrit brièvement diverses fonctions de sécurité implémentées sur le système de stockage.

Les thèmes abordés sont les suivants :

Présentation

Le système de stockage utilise diverses fonctions de sécurité pour contrôler les accès utilisateur et réseau, surveiller l'accès au système et son utilisation et prendre en charge la transmission des données de stockage. Ce document décrit les fonctions de sécurité disponibles.

Ce document s'adresse aux administrateurs responsables de la configuration et du fonctionnement du système de stockage.

Ce guide examine les paramètres de sécurité des catégories présentées dans le Tableau 1 à la page 10 :

Tableau 1 Catégories de paramètre de sécurité

Catégories de sécurité	Description :
Contrôle d'accès	Restriction de l'accès par l'utilisateur ou d'autres entités pour protéger les fonctions matérielles, logicielles ou de produits spécifiques.
Logs	Gestion de la consignation des événements.
Sécurité des communications	Sécurisation des communications réseau du produit.
Sécurité des données	Protection des données du produit.
Facilité de service	Contrôle continu des interventions de maintenance sur le produit effectuées par le fabricant ou ses partenaires de service.
Système d'alerte	Gestion des alertes et des notifications générées pour les événements liés à la sécurité.
Autres paramètres de sécurité	Paramètres de sécurité n'appartenant à aucune des précédentes catégories, comme la sécurité physique.

Informations sur les fonctions et les fonctionnalités connexes

Des informations relatives aux fonctions et fonctionnalités décrites dans ce document sont incluses dans ce qui suit pour Unity :

- *Guide d'utilisation de l'interface de ligne de commande Unisphere*
- Aide en ligne d'EMC Unisphere
- *Guide de programmation du fournisseur SMI-S*
- *Commandes de maintenance - Notes techniques*
- *Configuration et conditions requises des services à distance sécurisés*

Le jeu complet des publications pour clients EMC est disponible sur le site Web de support en ligne EMC à l'adresse http://Support.EMC.com. Une fois connecté au site Web, cliquez sur la page **Support par produit** pour rechercher des informations relatives à la fonction qui vous intéresse.

CHAPITRE 2

Contrôle d’accès

Ce chapitre décrit diverses fonctions de contrôle d'accès implémentées sur le système de stockage.

Les thèmes abordés sont les suivants :

Comptes de maintenance et de gestion par défaut du système de stockage

Le système de stockage est configuré avec des paramètres de compte utilisateur par défaut que vous devez utiliser la première fois que vous accédez au système de stockage et que vous le configurez. Voir Tableau 2 à la page 12.

Tableau 2 Paramètres de compte utilisateur par défaut

Type de compte	Nom d'utilisateur	Mot de passe	Privilèges
Gestion (Unisphere)	admin	Password123#	Privilèges d'administrateur permettant de réinitialiser les mots de passe par défaut, configurer les paramètres système par défaut, créer des comptes utilisateur et allouer du stockage.
Service	service	service	Exécution d'interventions de maintenance.

Remarque

Lors du processus de configuration initiale, vous devez modifier le mot de passe des comptes de gestion et de maintenance.

Gestion des comptes du système de stockage

Le Tableau 3 à la page 12 illustre les différentes méthodes de gestion des comptes du système de stockage.

Tableau 3 Méthodes de gestion des comptes

Rôles des comptes	Description
Gestion • Adminstrateur • Administrateur du stockage • Administrateur de la sécurité • Opérateur • Administrateur VM	Au terme du processus de configuration initiale du système de stockage, vous pouvez gérer les utilisateurs et les groupes du système de stockage (comptes locaux ou comptes LDAP, ou encore les deux) à partir de Unisphere ou de la CLI Unisphere. • Pour les comptes locaux, vous pouvez ajouter un nouvel utilisateur, supprimer un utilisateur sélectionné, modifier le rôle de l'utilisateur et redéfinir (changer) le mot de passe utilisateur. • Pour un utilisateur LDAP, vous pouvez ajouter un utilisateur LDAP, supprimer un utilisateur sélectionné et changer le rôle de l'utilisateur. • Pour un groupe LDAP, vous pouvez ajouter un groupe LDAP, supprimer un

Tableau 3 Méthodes de gestion des comptes (suite)

Rôles des comptes	Description
	groupe sélectionné et changer le rôle de l'utilisateur.
Service	Vous n'êtes autorisé ni à créer ni à supprimer des comptes de maintenance du système de stockage. Vous pouvez réinitialiser le mot de passe du compte de maintenance à partir de Unisphere. Sous Système, sélectionnez la fonction **Maintenance** > **Tâches de maintenance** > **Changer le mot de passe de maintenance**.

Remarque

Vous pouvez réinitialiser les mots de passe par défaut des comptes du système de stockage en appuyant sur le bouton de réinitialisation des mots de passe situé sur le châssis du système de stockage. Reportez-vous à *l'aide en ligne Unisphere* et au *guide d'information sur le matériel* du système pour obtenir plus d'informations.

Unisphere

L'authentification requise pour accéder à Unisphere s'effectue sur la base des informations d'identification du compte utilisateur (local ou LDAP). Les comptes utilisateur sont créés et gérés par la suite via la sélection **Gestion des utilisateurs** sous **Paramètres** > **Utilisateurs et groupes** dans Unisphere. Les autorisations qui s'appliquent à Unisphere dépendent du rôle associé au compte utilisateur.

Avant de pouvoir télécharger le contenu de l'interface utilisateur de Unisphere sur une station de gestion, l'utilisateur doit fournir ses informations d'identification à des fins d'authentification et établir une session sur le système de stockage. Une fois que l'utilisateur a saisi l'adresse réseau du système de stockage sous forme d'URL dans un navigateur Web, une page de connexion s'affiche pour lui permettre de s'authentifier en tant qu'utilisateur local ou via un serveur d'annuaire LDAP. Après authentification des informations d'identification fournies par l'utilisateur, l'interface utilisateur de la session de gestion est créée sur le système de stockage. L'interface utilisateur de Unisphere est ensuite téléchargée et instanciée sur la station de gestion de l'utilisateur. L'utilisateur peut alors surveiller et gérer le système de stockage dans la limite des autorisations que lui accorde son rôle.

LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole d'application pour l'interrogation de services d'annuaire s'exécutant sur des réseaux TCP/IP. LDAP fournit une gestion centralisée des informations d'authentification, d'identité et de groupe utilisées pour l'autorisation d'accès au système de stockage. L'intégration du système de stockage à un environnement LDAP existant offre un moyen de contrôler l'accès des utilisateurs et des groupes d'utilisateurs au système via la CLI Unisphere ou Unisphere.

Une fois les paramètres LDAP configurés pour le système, vous pouvez gérer les utilisateurs et les groupes d'utilisateurs, dans le contexte d'une structure de répertoires LDAP établie. Par exemple, vous pouvez attribuer des rôles d'accès

(Administrateur, Administrateur du stockage, Administrateur de la sécurité, Opérateur, Administrateur VM) aux utilisateurs ou groupes LDAP. Le rôle appliqué détermine le niveau d'autorisation dont dispose l'utilisateur ou le groupe dans l'administration du système de stockage. le système utilise les paramètres LDAP uniquement en vue de faciliter le contrôle de l'accès à la CLI Unisphere et à Unisphere, et non pour l'accès aux ressources de stockage.

Règles des sessions

Les sessions Unisphere présentent les caractéristiques suivantes :

- Expiration après une heure
- Délai d'expiration de la session non configurable
- Identifiants de session générés pendant l'authentification et utilisés pendant toute la durée de la session

Utilistion du nom d'utilisateur et du mot de passe

Les noms d'utilisateur des comptes Unisphere doivent respecter les conditions décrites dans le tableau suivant.

Tableau 4 Exigences relatives aux noms d'utilisateur des comptes Unisphere

Restriction	Nom d'utilisateur requis
Nombre minimal de caractères alphanumériques	1
Nombre maximal de caractères alphanumériques	64
Caractères spéciaux pris en charge	. (dot)

Les mots de passe des comptes Unisphere doivent respecter les conditions décrites dans le tableau suivant.

Tableau 5 Exigences relatives aux mots de passe des comptes Unisphere

Restriction	Critères pour créer un mot de passe
Nombre minimal de caractères	8
Nombre minimal de caractères majuscules	1
Nombre minimal de caractères minuscules	1
Nombre minimal de caractères numériques	1
Nombre minimal de caractères spéciaux • Caractères spéciaux pris en charge : ▪ !,@#$%^*_~?	1
Nombre maximal de caractères	40

Remarque

Vous pouvez modifier les mots de passe des comptes dans Unisphere en sélectionnant **Paramètres**, **Utilisateurs et groupes**, puis **Gestion des utilisateurs** > **Plus d'actions** > **Réinitialiser le mot de passe**. Lors de la modification d'un mot de passe, vous ne pouvez pas réutiliser l'un des trois derniers mots de passe. L'*aide en ligne de Unisphere* fournit des informations complémentaires à ce sujet.

NOTE

En mode STIG, le mot de passe doit comporter au moins 15 caractères. Le mode STIG définit également des conditions supplémentaires relatives au nombre, à la période de validité et à l'état d'expiration des mots de passe. Les comptes utilisateur créés avant l'activation du mode STIG ne sont pas affectés sauf si le mot de passe est modifié. Pour plus d'informations sur le mode STIG, reportez-vous à la section Gérer le mode STIG (déploiements physiques uniquement) à la page 86.

Autorisation

Le Tableau 6 à la page 15 montre les rôles attribuables aux utilisateurs locaux du système de stockage ainsi que les privilèges qui leur sont associés. Vous pouvez en outre attribuer ces rôles à des utilisateurs et groupes LDAP.

Tableau 6 Rôles et privilèges des utilisateurs locaux

Tâche	Opérateur	Administrateur du stockage	Administrateur de la sécurité	Administrateur	Administrateur VM
Modifier son propre mot de passe de connexion local	x	x	x	x	
Ajouter, supprimer ou modifier des hôtes				x	
Créer un stockage		x		x	
Supprimer le stockage		x		x	
Ajouter des objets de stockage, comme des LUN, des partages et des groupes de stockage, à des ressources de stockage		x		x	
Afficher la configuration et l'état du stockage	x	x	x	x	
Afficher les comptes utilisateurs Unisphere		x	x	x	
Ajouter, supprimer, modifier, verrouiller ou déverrouiller des comptes utilisateur Unisphere			x	x	
Afficher l'état actuel du logiciel ou de la licence	x	x	x	x	
Exécuter une mise à niveau de logiciel ou de licence				x	

Tableau 6 Rôles et privilèges des utilisateurs locaux (suite)

Tâche	Opérateur	Administrateur du stockage	Administrateur de la sécurité	Administrateur	Administrateur VM
Exécution de la configuration initiale				x	
Modifier la configuration du serveur NAS				x	
Modifier les paramètres système				x	
Modifier les paramètres réseau				x	
Modifier la langue de l'interface de gestion	x	x	x	x	
Afficher les informations des logs et des alertes	x	x	x	x	
Afficher l'état du chiffrement	x	x	x	x	
Effectuer la sauvegarde du magasin de clés de chiffrement, du log d'audit et du checksum			x	x	
Modifier le mode FIPS 140-2			x	x	
Modifier le mode STIG			x	x	
Établir des connexions VASA entre vCenter et le système de stockage				x	x

Dans le cas du rôle d'administrateur VM, une fois la connexion établie entre vCenter et le système de stockage, l'utilisateur vCenter peut afficher les informations de configuration et d'état du stockage pertinentes pour ce serveur vCenter et les serveurs VMware ESXi associés. Les informations qu'il est autorisé à visualiser sont déterminées par les mécanismes de contrôle d'accès vCenter.

Remarque

Vous pouvez modifier les rôles des comptes dans Unisphere en sélectionnant**Paramètres**, **Utilisateurs et groupes**, **Gestion des utilisateurs** > **Plus d'actions** > **Modifier le rôle**. L'*aide en ligne de Unisphere* fournit des informations complémentaires à ce sujet.

NAT
NAT n'est pas pris en charge pour la connexion locale via Unisphere au système de stockage.

Interface de ligne de commande (CLI) Unisphere

La CLI Unisphere offre les mêmes fonctions que celles disponibles via Unisphere.

L'exécution de la CLI Unisphere nécessite un logiciel de ligne de commande du système de stockage spécial. Vous pouvez télécharger ce logiciel à partir de la page produit de votre système de stockage sur le Support en ligne EMC (https://support.emc.com).

Règles des sessions
Le client CLI Unisphere ne prend pas en charge les sessions. Vous devez utiliser la syntaxe de ligne de commande pour spécifier le nom d'utilisateur et le mot de passe du compte à chaque commande que vous exécutez.

Vous pouvez utiliser la commande `-saveuser` de la CLI Unisphere pour enregistrer les informations d'identification (nom d'utilisateur et mot de passe) d'un compte donné dans un fichier du lockbox sécurisé stocké en local sur l'hôte où est installée la CLI Unisphere. Les données stockées ne sont disponibles que sur l'hôte sur lequel elles ont été enregistrées et pour l'utilisateur qui les a enregistrées. Après avoir enregistré les informations d'identification d'accès, la CLI les applique automatiquement au port et à la destination du système de stockage spécifiés chaque fois que vous exécutez une commande.

Utilisation des mots de passe
L'authentification auprès de la CLI Unisphere s'effectue sur la base des comptes de gestion créés et gérés via Unisphere. Les autorisations qui s'appliquent à Unisphere s'appliquent également aux commandes spécifiques en fonction du rôle associé au compte de connexion actif.

Enregistrement des paramètres
Vous pouvez enregistrer les paramètres suivants sur l'hôte sur lequel vous exécutez la CLI Unisphere :

- Informations d'identification d'utilisateur, telles que votre nom d'utilisateur et votre mot de passe, pour chaque système de stockage auquel vous accédez.
- Certificats SSL importés du système de stockage.
- Informations relatives au système par défaut accessible via la CLI Unisphere, telles que le nom ou l'adresse IP du système et son numéro de port.

La CLI Unisphere enregistre les paramètres dans un lockbox sécurisé résidant localement sur l'hôte sur lequel la CLI Unisphere est installée. Les données stockées ne sont disponibles que sur l'hôte sur lequel elles ont été enregistrées et pour l'utilisateur qui les a enregistrées. Le lockbox réside aux emplacements suivants :

- Sous Windows Server 2003 (XP) : `C:\Documents and Settings\$<user_name>\Local Settings\ApplicationData\.emc\uemcli\cert`
- Sous Windows 7, Windows 8 et Windows 10 : `C:\Users\${user_name}\AppData\Local\.emc\uemcli\cert`
- Sous UNIX/Linux : `<home_directory>/.emc/uemcli/cert`

Recherchez les fichiers config.xml et config.key. Si vous désinstallez la CLI Unisphere, ces répertoires et fichiers ne sont pas supprimés, ce qui vous donne la possibilité de les conserver. Si vous n'avez plus besoin de ces fichiers, supprimez-les.

Interface de maintenance SSH du système de stockage

Lorsqu'elle est activée, l'interface de maintenance SSH du système de stockage fournit une interface de ligne de commande permettant d'exécuter des opérations liées ou identiques à celles disponibles à partir de la page de maintenance de Unisphere (sous **Système**, sélectionnez **Maintenance** > **Tâches de maintenance** > **Activer SSH**).

Le compte de maintenance permet aux utilisateurs d'effectuer les tâches suivantes :

- Exécuter des commandes de maintenance du système de stockage spécialisées pour contrôler les paramètres système et les opérations du système de stockage ainsi que pour résoudre les problèmes rencontrés.

- Ils ne peuvent utiliser qu'un ensemble limité de commandes attribuées comme membre doté d'un compte utilisateur Linux non privilégié en mode shell restreint. Ce compte n'a accès ni aux fichiers système propriétaires, ni aux fichiers de configuration, ni aux données des utilisateurs ou des clients.

Pour plus d'informations sur les commandes de maintenance, consultez les notes techniques sur les *Commandes de maintenance*.

Le paramètre d'interface de maintenance SSH du système de stockage est préservé lors des redémarrages du système et des basculements, aussi bien en mode maintenance qu'en mode normal. Par conséquent, l'activation de l'interface de maintenance SSH du système de stockage garde l'interface activée jusqu'à ce qu'elle soit explicitement désactivée à la page Maintenance de Unisphere (sous **Système**, sélectionnez **Service** > **Tâches de maintenance** > **Désactiver le protocole SSH**).

Pour une sécurité maximale du système, il est recommandé de laisser l'interface de maintenance du système de stockage SSH désactivée à tout moment, à moins qu'elle ne soit vraiment nécessaire pour effectuer des opérations de maintenance sur le système de stockage. Après avoir effectué les opérations de maintenance nécessaires, désactivez l'interface SSH pour vous assurer que le système reste sécurisé.

Sessions

Les sessions de l'interface de maintenance SSH du système de stockage sont gérées sur la base des paramètres établis par le client SSH. Leurs caractéristiques sont déterminées par les paramètres de configuration du client SSH.

Utilisation des mots de passe

Le compte de maintenance est un compte que le personnel de maintenance peut utiliser pour exécuter des commandes Linux de base.

Le mot de passe par défaut de l'interface de maintenance du système de stockage est « service ». Lors de la configuration initiale du système de stockage, vous devez modifier le mot de passe de maintenance par défaut. Les restrictions relatives au mot de passe sont les mêmes que celles qui s'appliquent aux comptes de gestion Unisphere (reportez-vous à la section Utilistion du nom d'utilisateur et du mot de passe à la page 14). Pour plus d'informations sur la commande de maintenance du système de stockage, `svc_service_password`, utilisée pour gérer les paramètres de mot de passe du compte de maintenance du système de stockage, consultez le document *Notes techniques sur les commandes de maintenance*.

Autorisation

Comme indiqué dans Tableau 7 à la page 18, les autorisations du compte de maintenance sont définies de deux façons.

Tableau 7 Définition des autorisations du compte de maintenance

Type d'autorisation	Description
Autorisations du système de fichiers Linux	Les autorisations du système de fichiers déterminent la plupart des tâches que le compte de maintenance peut et ne peut pas effectuer sur le système de stockage. Par exemple, la majorité des outils et utilitaires Linux qui modifient le fonctionnement du système d'une quelconque façon nécessitent des privilèges de compte de superutilisateur. Étant donné que le compte de maintenance ne dispose pas de tels privilèges d'accès, il ne peut pas exécuter ces outils et utilitaires Linux. Il ne peut pas non plus modifier les fichiers de configuration exigeant un accès racine en lecture et/ou en écriture.

Tableau 7 Définition des autorisations du compte de maintenance (suite)

Type d'autorisation	Description
Listes de contrôle d'accès	Le mécanisme de listes de contrôle d'accès (ACL) du système de stockage utilise une liste de règles très spécifiques pour octroyer ou refuser de manière explicite l'accès aux ressources du système par le compte de maintenance. Les règles contenues dans l'ACL déterminent les autorisations dont bénéficie le compte de maintenance sur d'autres fonctions du système de stockage non couvertes par les autorisations du système de fichiers Linux standard.

Commandes de maintenance du système de stockage

L'environnement d'exploitation du système de stockage intègre diverses commandes de diagnostic des problèmes, de configuration système et de restauration système. Ces commandes offrent un niveau d'informations approfondi et un contrôle de système de niveau inférieur à celui disponible via Unisphere. Une description de ces commandes, ainsi que des exemples d'utilisation courants, sont disponibles dans le document *Notes techniques sur les commandes de maintenance*.

Port de service Ethernet du SP du système de stockage et IPMItool

Votre système de stockage permet d'accéder à la console via le port de service Ethernet situé sur chaque SP. Cet accès requiert l'utilisation de l'outil IPMItool. Similaire à SSH ou à Telnet, l'outil réseau IPMItool utilise le protocole IPMI pour s'interfacer avec chaque SP via une connexion Ethernet. IPMItool est un utilitaire Windows qui négocie un canal de communication sécurisé afin d'accéder à la console du SP d'un système de stockage. Pour pouvoir activer la console, l'utilitaire a besoin d'informations d'identification et d'une adresse IP. Pour plus d'informations sur IPMItool, consultez le document *IPMItool User Guide Technical Notes*.

L'interface du port de service Ethernet du SP offre les mêmes fonctions que l'interface de maintenance SSH et est soumise aux mêmes restrictions. Elle diffère néanmoins de celle-ci par le fait que les utilisateurs y accèdent via une connexion par port Ethernet plutôt qu'au moyen d'un client SSH.

Pour obtenir la liste des commandes de maintenance, consultez les *Notes techniques sur les commandes de maintenance*.

Fournisseur SMI-S

Le fournisseur SMI-S n'entraîne aucun changement au niveau de la sécurité. Le client SMI-S se connecte au système de stockage via le port HTTPS 5989. Les informations d'identification pour la connexion sont les mêmes que celles des utilisateurs de l'interface utilisateur ou de la CLI Unisphere. Toutes les règles de sécurité applicables aux utilisateurs de l'interface utilisateur et de la CLI valent aussi pour les connexions SMI-S. Les utilisateurs de l'interface utilisateur et de la CLI Unisphere peuvent ainsi s'authentifier via l'interface SMI-S. Il est inutile de définir des comptes utilisateur distincts pour cette interface. Une fois authentifié, le client SMI-S bénéficie des mêmes privilèges que ceux définis pour les comptes utilisateur de l'interface utilisateur et de la CLI Unisphere. Le *Guide de programmation du fournisseur SMI-S* de votre système de stockage fournit des informations sur la configuration de ce service.

Prise en charge de vSphere Storage API for Storage Awareness

vSphere Storage API for Storage Awareness (VASA) est une API de détection du stockage définie par VMware et indépendante du fournisseur. Un fournisseur VASA (VP) est un composant logiciel dédié au stockage qui agit comme un service d'information concernant le stockage pour vSphere. Les hôtes ESXi et vCenter Server se connectent au VP pour obtenir des informations sur les capacités, l'état et la topologie de stockage disponibles. Par la suite, vCenter Server fournit des informations aux clients vSphere. L'interface VASA est plutôt utilisée par les clients VMware par rapport aux clients Unisphere.

Le fournisseur VASA (VP) s'exécute sur le processeur de stockage (SP) actif du système de stockage. L'utilisateur vSphere doit configurer cette instance du VP en tant que fournisseur des informations VASA pour chaque système de stockage. En cas d'arrêt d'un SP, le processus associé, de même que le VP VASA, redémarrent sur le SP homologue. L'adresse IP bascule automatiquement. En interne, le protocole détectera une défaillance lors de l'obtention des événements de modification de configuration à partir du nouveau VP actif, mais les objets VASA seront automatiquement resynchronisés sans intervention de l'utilisateur.

Le système de stockage fournit des interfaces VASA 3.0 et VASA 2.0 pour vSphere 6, et des interfaces VASA 1.0 pour vSphere 5.x.

VASA 1.0 est utilisée pour la surveillance uniquement ; son utilisation concerne les clients VMware plutôt que les clients Unisphere. VASA 1.0 est une interface exclusivement destinée au reporting. Elle permet d'obtenir des informations de base sur le système de stockage et les périphériques de stockage qu'il expose à l'environnement virtuel afin de simplifier les tâches quotidiennes de provisionnement, de surveillance et de dépannage via vSphere :

- Visibilité du stockage : détection interne des modifications de propriétés et envoi d'informations à jour à vCenter
- Alarmes d'état de santé et de capacité : surveillance interne des changements d'état de santé et de dépassement des seuils de capacité, avec déclenchement d'alarmes appropriées à destination de vCenter :
  - état de santé de la baie, des SP, des ports d'E/S, des LUN et des systèmes de fichiers ;
  - signalement des changements d'état de santé de n'importe lequel de ces objets, par types de changement ;
  - alarmes de capacité des LUN et des systèmes de fichiers.
- Fonctions de stockage VASA : surveillance interne des changements de capacités de stockage, avec transmission à vCenter d'informations à jour sur les capacités.
- Intégration de Storage DRS : vSphere s'appuie sur les informations communiquées en interne par le VP et les intègre dans sa logique métier en vue de leur utilisation dans différents workflows Storage DRS.

VASA 3.0 et 2.0 prennent en charge les volumes virtuels (VVol). Les interfaces VASA 3.0 et VASA 2.0 prennent en charge des interfaces pour interroger les abstractions de stockage telles que les VVol et les conteneurs de stockage. Ces informations facilitent la prise de décision concernant le positionnement et la conformité des disques virtuels dans le cadre de la gestion basée sur les règles de stockage (SPBM). VASA 3.0 and VASA 2.0 prennent également en charge des interfaces pour provisionner et gérer le

cycle de vie des volumes virtuels utilisés pour la sauvegarde des disques virtuels. Ces interfaces sont appelées directement par les hôtes ESXi.

Pour plus d'informations sur VASA, vSphere et les VVol, consultez la documentation VMware et l'aide en ligne Unisphere.

Authentification VASA

Pour permettre à vCenter de se connecter au VP Unisphere, vous devez saisir trois types d'informations dans vSphere Client :

- l'URL du VP, au format suivant :
  - Pour VASA 3.0 et VASA 2.0, https://<Management IP address>:8443/vasa/version.xml
  - Pour VASA 1.0, https://<Management IP address>:8444/vasa/version.xml ou https://<Management IP address>:8444/vasa/services/vasaService
- le nom d'un utilisateur Unisphere (doté du rôle d'Administrateur VM ou d'Administrateur) :

  Remarque

  Le rôle d'Administrateur VM est strictement utilisé en vue d'enregistrer les certificats.

  - pour les utilisateurs locaux, utilisez la syntaxe : local /<username>
  - pour les utilisateurs LDAP, utilisez la syntaxe : <domain>/<username>
- le mot de passe associé à cet utilisateur.

Les informations d'identification Unisphere sont uniquement utilisées lors de cette étape de connexion initiale. Si les informations d'identification Unisphere sont valides pour le système de stockage cible, le certificat de vCenter Server est automatiquement enregistré auprès du système de stockage. Ce certificat est ensuite utilisé pour authentifier les demandes de connexion ultérieures de vCenter. L'installation ou le téléchargement de ce certificat dans le VP ne requiert aucune intervention manuelle. À l'expiration du certificat, vCenter doit en enregistrer un autre afin de prendre en charge une nouvelle session. La révocation du certificat par l'utilisateur entraîne l'invalidation de la session et l'arrêt de la connexion.

Session, connexion sécurisée et informations d'identification vCenter

Pour démarrer une session vCenter, un administrateur vSphere doit fournir l'URL et les informations d'identification du VP à vCenter Server via vSphere Client. vCenter Server utilise l'URL, les informations d'identification et le certificat SSL du VP pour établir une connexion sécurisée à ce dernier. Une session vCenter est terminée lorsque les événements suivants se produisent :

- Un administrateur supprime le VP de la configuration vCenter dans vSphere Client et que vCenter Server met fin à la connexion.
- vCenter Server tombe en panne ou un de ses services échoue, ce qui interrompt la connexion. Lorsque vCenter ou le service redémarre, il tente de rétablir la connexion SSL. S'il n'y parvient pas, il lance une nouvelle connexion SSL.
- Le fournisseur VASA échoue, ce qui interrompt la connexion. Lorsque le fournisseur VASA démarre, il peut répondre à la communication à partir de vCenter Server pour rétablir la connexion SSL et la session VASA.

Une session vCenter repose sur une communication HTTPS sécurisée entre vCenter Server et un VP. L'architecture VASA utilise des certificats SSL et des identifiants de session VASA pour sécuriser les connexions. Dans VASA 1.0, vCenter Server ajoutait le certificat VP à son magasin d'approbations dans le cadre de l'installation du VP ou de la création d'une connexion de session VASA. Le VP ajoutait

le certificat vCenter Server à son magasin d'approbations lors de l'appel de la fonction registerVASACertificate par le service SMS (Storage Monitoring Service). Dans VASA 3.0 et VASA 2.0, vCenter Server agit en tant qu'autorité de certification VMware (VMCA). Le VP transmet un certificat auto-signé à la demande, après autorisation de la demande. Il ajoute le certificat vCenter Server à son magasin d'approbations, puis émet une demande de signature de certificat et remplace son certificat auto-signé par le certificat signé VMCA. Les futures connexions seront authentifiées par le serveur (VP) en utilisant le certificat client (SMS) validé en fonction du certificat de signature racine précédemment enregistré. Un VP génère des identifiants uniques pour les objets d'entité de stockage et vCenter Server utilise l'identifiant pour demander des données pour une entité spécifique.

Un VP utilise les certificats SSL et l'identifiant de session VASA pour valider les sessions VASA. Une fois la session établie, un VP doit valider à la fois le certificat SSL et l'identifiant de session VASA associés à chaque appel de fonction émis à partir de vCenter Server. Le VP utilise le certificat de vCenter Server stocké dans son magasin d'approbations pour valider le certificat associé aux appels de fonctions en provenance du service vCenter SMS. Une session VASA est conservée sur plusieurs connexions SSL. Si une connexion SSL est supprimée, vCenter Server effectue une négociation SSL avec le VP pour rétablir la connexion SSL dans le contexte de la même session VASA. Si un certificat SSL expire, l'administrateur vSphere doit générer un nouveau certificat. vCenter Server établit une nouvelle connexion SSL et enregistre le nouveau certificat applicable au VP.

Remarque

L'annulation de l'enregistrement des VP 3.0 et 2.0 est différente de l'annulation de l'enregistrement des VP 1.0. Le service SMS n'appelle pas la fonction unregisterVASACertificate par rapport à un VP 3.0 ou 2.0, par conséquent, même après l'annulation, le VP peut continuer à utiliser son certificat signé VMCA issu du service SMS et continuer à avoir accès au certificat racine VMCA.

Authentification unique (SSO) avec Unisphere Central

La fonction d'authentification unique (SSO) ajoutée à Unisphere Central fournit des services d'authentification pour plusieurs systèmes de stockage qui sont configurés pour utiliser cette fonctionnalité. Cette fonction offre un moyen simple pour un utilisateur de se connecter à chaque système sans devoir renouveler son authentification auprès de chaque système.

Unisphere Central est le serveur centralisé d'authentification qui facilite l'authentification unique (SSO). Cette fonction permet à un utilisateur :

- De se connecter à Unisphere Central, puis de sélectionner et de démarrer Unisphere sur un système de stockage sans devoir rappeler les informations d'identification.
- Vous connecter à un système de stockage, puis choisir d'autres systèmes de stockage associés à la même instance Unisphere Central à laquelle vous connecter sans devoir rappeler les informations d'identification.

Unisphere Central exécute régulièrement une requête pour demander des informations d'état auprès des systèmes de stockage qu'il gère. L'identité associée aux demandes effectuées dans ce contexte est le certificat SSL/X.509 Unisphere Central. Ce certificat est signé par l'autorité de certification de Unisphere Central qui est approuvée par chaque instance du système de stockage que Unisphere Central est configuré pour gérer.

En outre, cette fonction fournit une fonction de déconnexion unique. Ainsi, lorsque vous vous déconnectez de la console Unisphere Central, vous fermez en même temps toutes les sessions associées du système de stockage.

Conditions requises
Pour utiliser l'authentification unique (SSO) :

- Les systèmes de stockage Unity et UnityVSA doivent exécuter OE version 4.0 ou supérieure.
- Unisphere Central version 4.0 ou une version ultérieure doit être utilisée.
- Le serveur Unisphere Central et les systèmes de stockage doivent être configurés pour l'authentification auprès du même répertoire AD/LDAP.
- L'utilisateur LDAP doit être directement mappé à un rôle Unisphere, ou être membre d'un groupe AD/LDAP qui est mappé à un rôle Unisphere à la fois sur le système de stockage et sur Unisphere Central.
- Chaque système de stockage doit activer la fonction d'authentification unique (SSO).
- L'utilisateur doit se connecter en tant qu'utilisateur LDAP.

Remarque

Si ces conditions ne sont pas remplies, l'utilisateur doit se connecter au système individuel en tant qu'utilisateur local et fournir des informations d'authentification pour accéder à ce système.

Pour activer l'authentification unique (SSO), vous devez avoir les privilèges Administrateur. Les utilisateurs disposant des privilèges Administrateur de stockage, Opérateur ou Administrateur VM ne peuvent pas activer l'authentification unique (SSO). Utilisez la commande uemcli suivante pour activer l'authentification unique (SSO) :

```
uemcli -d <IP address> -u <username> -p <password> /sys/ur set -
ssoEnabled yes
```

Chaque système de stockage configuré avec cette configuration activée peut être un client du serveur centralisé d'authentification et participer à l'environnement d'authentification unique (SSO). Pour plus d'informations sur cette commande, consultez le *Guide d'utilisation de l'interface de ligne de commande Unisphere*.

Considérations et restrictions
Le délai d'expiration de la session utilisateur entre le client Web et le serveur centralisé d'authentification est de 45 minutes.

Le délai d'expiration de la session application entre le client web et le système de stockage est de 1 heure.

Remarque

Reportez-vous à la Matrice de support simplifiée pour le système de stockage sur le site Web de support pour obtenir des informations sur la compatibilité et l'interopérabilité liées aux navigateurs Web.

Flux des processus d'authentification unique (SSO)

Les séquences suivantes représentent les flux des processus d'authentification relatifs à l'authentification unique (SSO) en corrélation avec Unisphere Central.

Accès à un système de stockage via Unisphere Central

1. L'utilisateur lance un navigateur Web sur une station de gestion et spécifie l'adresse réseau d'Unisphere Central en tant qu'URL.
2. Le navigateur est redirigé par le serveur Web vers une URL de connexion locale Unisphere Central et l'utilisateur voit apparaître un écran de connexion.
3. L'utilisateur saisit et envoie des informations d'identification LDAP. Le nom d'utilisateur est au format suivant : <LDAP DOMAIN>/username.
4. Un jeton de session est défini et le navigateur est redirigé par le système vers l'URL d'origine qui avait été spécifiée.
5. Le navigateur télécharge le contenu d'Unisphere et Unisphere Central est instancié.
6. L'utilisateur navigue alors dans Unisphere jusqu'à un système de stockage en particulier à surveiller.
7. L'utilisateur clique sur l'adresse réseau du système de stockage.
8. Une nouvelle fenêtre de navigateur est créée avec l'URL du système de stockage.
9. Le navigateur est redirigé vers le serveur d'authentification Unisphere Central où l'utilisateur est déjà authentifié.
10. Le navigateur est redirigé vers la page de téléchargement de Unisphere et une session est établie avec le système de stockage en utilisant le nouveau ticket de service.
11. Unisphere est téléchargé et instancié.
12. L'utilisateur démarre la gestion/surveillance du système de stockage.

Accès aux systèmes de stockage associés à Unisphere Central

1. L'utilisateur démarre un navigateur Web sur une station de gestion et spécifie l'adresse réseau d'un système de stockage en tant qu'URL.
2. Le navigateur est redirigé vers le service de connexion locale Unisphere Central et l'utilisateur voit apparaître un écran de connexion.
3. L'utilisateur saisit et envoie des informations d'identification LDAP. Le nom d'utilisateur est au format suivant : <LDAP DOMAIN>/username.
4. Un jeton de session est défini comme un cookie et le navigateur est redirigé par le système vers l'URL d'origine qui avait été spécifiée.
5. Le navigateur télécharge le contenu d'Unisphere et Unisphere est instancié.
6. L'utilisateur ouvre ensuite une autre fenêtre ou un autre onglet du navigateur Web et spécifie l'adresse réseau d'un autre système de stockage en tant qu'URL.
7. Le navigateur est redirigé vers le serveur d'authentification Unisphere Central où l'utilisateur est déjà authentifié. Un nouveau ticket de service est obtenu.
8. Le navigateur est redirigé vers la page de téléchargement de Unisphere et établit une session avec le deuxième système de stockage en utilisant le nouveau ticket de service.
9. Unisphere pour le deuxième système de stockage est téléchargé et instancié.
10. L'utilisateur démarre la gestion/surveillance du deuxième système de stockage.

Connexion à un système de stockage local

Lorsque vous utilisez un compte local ou, si la connectivité au serveur d'authentification Unisphere Central n'est pas disponible, vous pouvez vous connecter à un système de stockage local à l'aide du résident du serveur d'authentification sur le

système au lieu de vous connecter via Unisphere Central. Il existe deux façons de se connecter localement au système de stockage :

- Lorsque le navigateur est redirigé vers le serveur d'authentification Unisphere Central, une option permet à l'utilisateur de se rediriger vers le système et de se connecter localement.
- Si Unisphere Central est inaccessible, la syntaxe suivante d'URL peut être utilisée pour parcourir ou pour accéder localement au système et à la connexion : `https://<storagesystemIP>?casHome=LOCAL`

où *storagesystemIP* est l'adresse IP du système de stockage.

Authentification unique (SSO) et prise en charge NAT (Network Address Translation)

L'authentification unique (SSO) ne prend pas en charge la configuration NAT. En outre, la configuration NAT n'est pas prise en charge pour la connexion locale via Unisphere au système de stockage.

Sécurité sur les objets du système de fichiers

Dans un environnement multiprotocole, la stratégie de sécurité est définie au niveau du système de fichiers et est indépendante pour chaque système de fichiers. Chaque système de fichiers utilise sa stratégie d'accès pour déterminer comment rapprocher les différences entre les sémantiques de contrôle d'accès NFS et SMB. La sélection d'une stratégie d'accès détermine quel mécanisme est utilisé pour garantir la sécurité des fichiers sur le système de fichiers donné.

NOTE

Si l'ancien protocole SMB1 n'a pas besoin d'être pris en charge dans votre environnement, il peut être désactivé à l'aide de la commande de maintenance `svc_nas`. Pour plus d'informations sur cette commande de maintenance, consultez le document *Notes techniques sur les commandes de maintenance*.

Modèle de sécurité UNIX

Lorsque la stratégie UNIX est sélectionnée, toute tentative de modification de la sécurité en mode fichier à partir du protocole SMB est ignorée, comme la modification des listes de contrôle d'accès. Les privilèges d'accès UNIX font référence aux bits de mode d'un objet ou à la liste de contrôle d'accès (ACL) NFSV4 du système de fichiers. Les bits de mode sont représentés par une chaîne de bits. Chaque bit représente un mode d'accès ou un privilège accordé à l'utilisateur auquel appartient le fichier, au groupe associé à l'objet du système de fichiers et à tous les autres utilisateurs. Les bits de mode UNIX sont représentés sous la forme de trois ensembles de triplets concaténés rwx (lecture, écriture et exécution) pour chaque catégorie d'utilisateurs (utilisateur, groupe ou autre). Une ACL est une liste d'utilisateurs et de groupes d'utilisateurs à l'aide de laquelle vous pouvez contrôler ou refuser l'accès aux services.

Modèle de sécurité Windows

Le modèle de sécurité Windows est principalement basé sur des privilèges des objets, impliquant l'utilisation d'un descripteur de sécurité et de sa liste de contrôle d'accès (ACL). Lorsque la stratégie SMB est activée, les modifications appliquées aux bits de mode du protocole NFS sont ignorées.

L'accès à un objet du système de fichiers dépend de la manière dont les autorisations ont été paramétrées sur Autoriser ou Refuser via l'utilisation d'un descripteur de sécurité. Le SD décrit le propriétaire de l'objet et groupe les SID pour l'objet avec ses

ACL. Une ACL fait partie du descripteur de sécurité pour chaque objet. Chaque ACL contient des entrées de contrôle d'accès (ACE). Chaque ACE à son tour contient un seul SID qui identifie un utilisateur, un groupe ou un ordinateur et une liste de privilèges qui sont refusés ou autorisés pour ce SID.

Accès aux systèmes de fichiers dans un environnement multiprotocole

L'accès aux fichiers est fourni via des serveurs NAS. Un serveur NAS contient un ensemble de systèmes de fichiers où sont stockées des données. Le serveur NAS permet d'accéder à ces données pour des protocoles de fichiers NFS et SMB en partageant des systèmes de fichiers via des partages SMB et NFS. Le mode serveur NAS pour le partage multiprotocole permet de partager les mêmes données entre SMB et NFS. Du fait que le mode de partage multiprotocole offre un accès simultané SMB et NFS à un système de fichiers, le mappage des utilisateurs Windows sur les utilisateurs UNIX et la définition des stratégies de sécurité à utiliser (bits de mode, ACL et informations d'identification des utilisateurs) doivent être pris en compte et configurés de manière adéquate pour un partage multiprotocole.

Remarque

Pour plus d'informations sur la configuration et la gestion de serveurs NAS concernant le partage multiprotocole, le mappage utilisateur, les stratégies d'accès et les informations d'identification utilisateur, reportez-vous à l'aide en ligne de Unisphere et au *Guide d'utilisation de l'interface de ligne de commande (CLI) Unisphere*.

Mappage utilisateur

Dans un contexte multiprotocole, un utilisateur Windows doit être mis en correspondance avec un utilisateur UNIX. Toutefois, un utilisateur UNIX doit être mappé à un utilisateur Windows uniquement lorsque la politique d'accès est Windows. Ce mappage est nécessaire pour que la sécurité du système de fichiers puisse être exécutée, même si elle n'est pas native dans le protocole. Les composants suivants sont impliqués dans le mappage utilisateur :

- Services d'annuaire UNIX, fichiers locaux ou les deux
- Programmes de résolution Windows
- Mappage sécurisé (secmap) - cache contenant tous les mappages entre les identifiants SID et UID ou ID de groupe utilisés par un serveur NAS.
- ntxmap

Remarque

Le mappage de l'utilisateur n'affecte pas les utilisateurs ni les groupes locaux sur le serveur SMB.

Services d'annuaire UNIX et fichiers locaux

Les services d'annuaire UNIX (UDS) et les fichiers locaux sont utilisés pour les éléments suivants :

- Retourne le nom du compte UNIX correspondant pour un identifiant utilisateur (UID) particulier.
- Retourne l'UID et l'identifiant de groupe (GID) principal correspondants pour un nom de compte UNIX particulier.

Les services pris en charge sont les suivants :

- LDAP
- NIS
- Fichiers locaux
- Aucun (l'unique mappage possible s'effectue par le biais de l'utilisateur par défaut)

Il faudrait un UDS activé ou des fichiers locaux activés, ou bien les deux à la fois pour le serveur NAS lorsque le partage multiprotocole est activé. La propriété de service d'annuaire Unix du serveur NAS détermine qui est utilisé pour le mappage des utilisateurs.

Programmes de résolution Windows

Les programmes de résolution Windows sont utilisés pour effectuer les éléments suivants pour le mappage utilisateur :

- Retourne le nom du compte Windows correspondant pour un identifiant de sécurité particulier (SID)
- Retourne le SID correspondant pour un nom de compte Windows particulier

Les programmes de résolution Windows sont les suivants :

- Le contrôleur de domaine (DC) du domaine.
- La base de données du groupe local (LGDB) du serveur SMB

secmap

La fonction secmap consiste à stocker tous les mappages SID à UID et GID principal et UID à SID afin d'assurer une cohérence entre tous les systèmes de fichiers du serveur NAS.

ntxmap

ntxmap est utilisé pour associer un compte Windows à un compte UNIX lorsque le nom est différent. Par exemple, si un utilisateur dispose d'un compte qui est nommé Gerald sous Windows, mais que ce compte est appelé Gerry sous UNIX, ntxmap est utilisé pour établir la corrélation entre les deux.

Mappages SID à UID, GID principal

La séquence suivante est le processus utilisé pour résoudre un SID pour un UID, mappage GID principal :

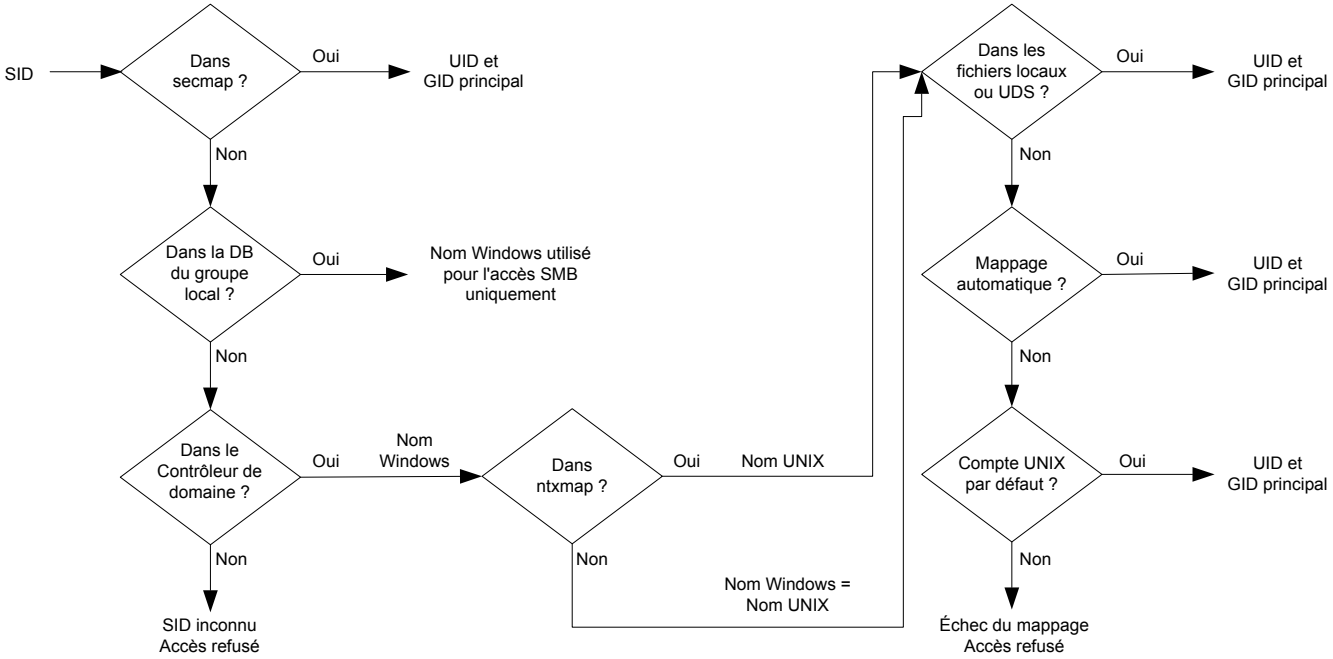
1. secmap est recherché dans le SID. Si le SID est trouvé, le mappage UID et GID est résolu.
2. Si le SID est introuvable dans secmap, le nom Windows associé à l'identifiant SID doit être trouvé.
    a. Les bases de données du groupe local des serveurs SMB du NAS sont recherchées pour le SID. Si le SID est trouvé, le nom Windows associé est le nom d'utilisateur local, ainsi que le nom du serveur SMB.
    b. Si le SID est introuvable dans la base de données du groupe local, le contrôleur du domaine est recherché. Si le SID est trouvé, le nom Windows associé est le nom d'utilisateur. Si le SID n'est pas résolu, l'accès est refusé.
3. Le nom de Windows est traduit dans un nom UNIX. ntxmap est utilisé à cette fin.
    a. Si le nom Windows se trouve dans ntxmap, l'entrée est utilisée en tant que nom UNIX.
    b. Si le nom Windows se trouve dans ntxmap, le nom Windows est utilisé en tant que nom UNIX.

4. L'UDS (serveur NIS, serveur LDAP ou fichiers locaux) est recherché en utilisant le nom UNIX.
   a. Si le nom d'utilisateur UNIX est trouvé dans l'UDS, le mappage UID et de l'ID de groupe est résolu.
   b. Si le nom UNIX est introuvable, mais que la fonctionnalité de mappage automatique pour les comptes Windows non mappés est activée, l'UID est automatiquement assigné.
   c. Si le nom d'utilisateur UNIX n'est pas trouvé dans l'UDS mais qu'il existe un compte UNIX par défaut, le mappage UID et de l'ID de groupe est résolu en fonction de celui du compte UNIX par défaut.
   d. Si le SID n'est pas résolu, l'accès est refusé.

Si le mappage est trouvé, il est ajouté dans la base de données secmap persistante. Si le mappage est introuvable, le mappage en échec est ajouté dans la base de données secmap persistante.

Le schéma suivant montre le processus permettant de résoudre un mappage SID à UID, GID principal :

Figure 1 Processus de résolution d'un mappage SID à UID, GID principal



Mappage UID à SID

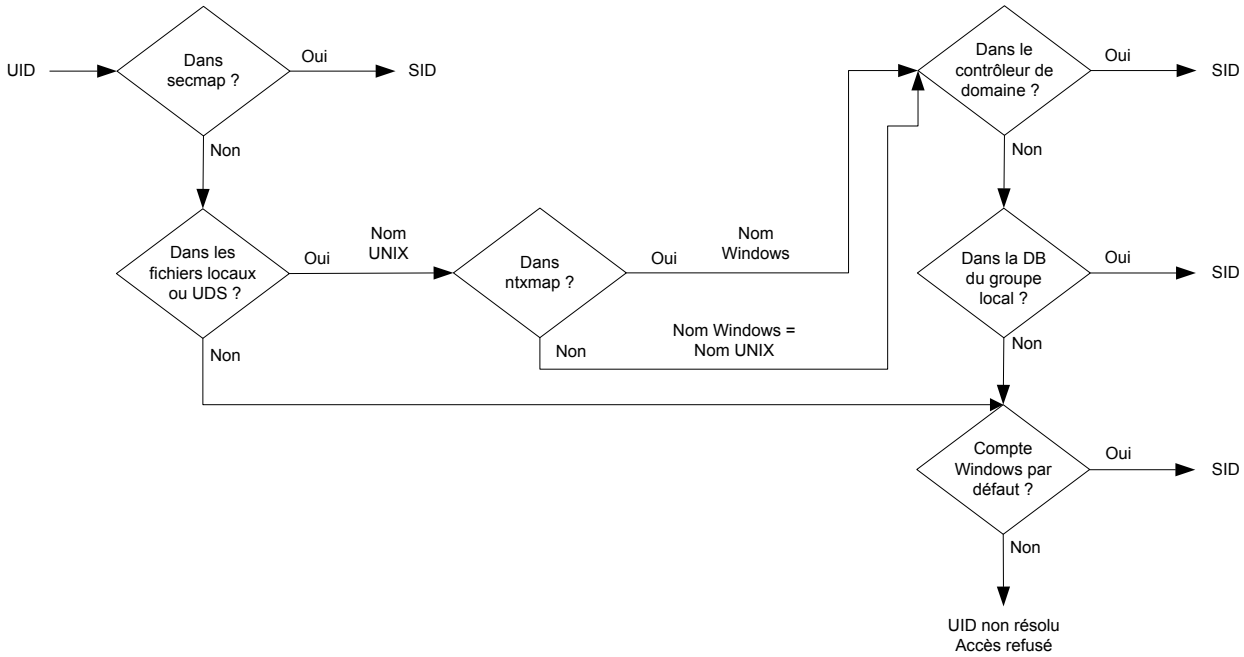
La séquence suivante est le processus utilisé pour résoudre un UID dans un mappage SID :

1. secmap est recherché pour l'UID. Si l'UID est trouvé, le mappage SID est résolu.
2. Si l'UID est introuvable dans secmap, le nom Windows associé à l'identifiant UID doit être trouvé.
    a. L'UDS (serveur NIS, serveur LDAP ou fichiers locaux) est recherché en utilisant l'UID. Si l'UID est trouvé, le nom UNIX associé est le nom d'utilisateur.
    b. Si l'UID n'est pas trouvé dans l'UDS, mais qu'il existe un compte Windows par défaut, l'UID est mappé sur le SID du compte Windows par défaut.
3. Si les informations du compte Windows par défaut ne sont pas utilisées, le nom UNIX est converti en nom Windows. ntxmap est utilisé à cette fin.
    a. Si le nom Windows se trouve dans ntxmap, l'entrée est utilisée en tant que nom Windows.
    b. Si le nom UNIX se trouve dans ntxmap, le nom UNIX est utilisé en tant que nom Windows.
4. Le contrôleur de domaine Windows ou la base de données du groupe local est recherché(e) en utilisant le nom Windows.
    a. Si le nom Windows est trouvé, le mappage SID est résolu.
    b. Si le nom Windows contient un point et que la partie du nom suivant le dernier point (.) correspond à un nom de serveur SMB, la base de données du groupe local de ce serveur SMB est recherchée pour résoudre le mappage SID.
    c. Si le nom Windows n'est pas trouvé mais qu'il existe un compte Windows par défaut, le mappage SID est résolu en fonction de celui du compte Windows par défaut.
    d. Si le SID n'est pas résolu, l'accès est refusé.

Si le mappage est trouvé, il est ajouté dans la base de données secmap persistante. Si le mappage est introuvable, le mappage en échec est ajouté dans la base de données secmap persistante.

Le schéma suivant montre le processus permettant de résoudre un mappage UID à SID :

Figure 2 Processus permettant de résoudre un mappage UID à SID



Stratégies d'accès pour NFS, SMB et FTP

Dans un environnement multiprotocole, le système de stockage utilise les stratégies d'accès du système de fichiers pour gérer le contrôle d'accès utilisateur de ses systèmes de fichiers. Il existe deux types de sécurité, UNIX et Windows.

Pour l'authentification de sécurité UNIX, les informations d'identification sont créées à partir des services d'annuaire UNIX (UDS), avec pour exception les accès NFS non sécurisés, où les informations d'identification sont fournies par le client d'hôte. Les droits des utilisateurs sont déterminés à partir des bits de mode et de la liste de contrôle d'accès (ACL) NFSV4. Les identificateurs d'utilisateurs et de groupes (UID et GID, respectivement) sont utilisés pour l'identification. Il n'y a pas de privilèges associés à la sécurité UNIX.

Pour l'authentification de sécurité Windows, les informations d'identification sont générées à partir du contrôleur de domaine Windows (DC) et de la base de données du groupe local (LGDB) du serveur SMB. Les droits des utilisateurs sont déterminés à partir des ACL SMB. Les ID de sécurité (SID) sont utilisés pour l'identification. Il existe des privilèges associés à la sécurité Windows, comme TakeOwnership, la sauvegarde et la restauration qui sont attribués par le LGDB ou l'objet de stratégie de groupe du serveur SMB.

Le tableau suivant décrit les règles d’accès qui définissent quelle sécurité est utilisée par quel protocole :

Règle d’accès	Description
Native (par défaut)	• Chaque protocole gère l’accès avec sa sécurité native. • La sécurité des partages NFS utilise les informations d'identification UNIX associées à la demande de vérification des bits de mode UNIX NFSv3 ou ACL NFSv4. L'accès est alors accordé ou refusé. • La sécurité des partages SMB utilise les informations d'identification Windows associées à la demande de vérification de la liste de contrôle d'accès (ACL) SMB. L'accès est alors accordé ou refusé. • Les bits de mode UNIX NFSv3 et les changements d’autorisation ACL NFSv4 sont synchronisés les uns par rapport aux autres. • Il n’y a aucune synchronisation entre les autorisations UNIX et Windows.
Windows	• Sécurise l'accès en mode fichier pour Windows et UNIX à l’aide de la sécurité Windows. • Utilise les informations d’identification Windows pour vérifier la liste ACL SMB. • Les autorisations pour les fichiers nouvellement créés sont déterminées par une conversion ACL SMB. Les changements d’autorisation ACL SMB sont synchronisés sur les bits de mode UNIX NFSv3 ou l’ACL NFSv4. • Les bits de mode NFSv3 et les changements d’autorisation ACL NFSv4 sont refusés.
UNIX	• Sécurise l'accès en mode fichier pour Windows et UNIX à l’aide de la sécurité UNIX.

Règle d'accès	Description
	• Suite à la demande d'accès SMB, les informations d'identification UNIX générées à partir de fichiers locaux ou UDS sont utilisées pour vérifier les autorisations des bits de mode NFSv3 ou des ACL NFSv4. • Les autorisations pour les fichiers nouvellement créés sont déterminées par UMASK. • Les changements d'autorisation des bits de mode UNIX NFSv3 ou l'ACL NFSv4 sont synchronisés sur l'ACL SMB. • Les changements d'autorisation de l'ACL SMB sont autorisés afin d'éviter toute interruption, mais ces autorisations ne sont pas conservées.

Pour le protocole FTP, l'authentification à l'aide de Windows ou UNIX dépend du format du nom de l'utilisateur qui est utilisé lors de l'authentification sur le serveur NAS. Si l'authentification Windows est utilisée, le contrôle d'accès FTP est similaire à celui de SMB ; dans le cas contraire, l'authentification est similaire à celle de NFS. Les clients FTP et SFTP sont authentifiés lorsqu'ils se connectent au serveur NAS. Il peut s'agir d'une authentification SMB (lorsque le format du nom d'utilisateur est `domain\user` ou `user@domain`) ou une authentification UNIX (pour les autres formats d'un nom d'utilisateur). L'authentification SMB est assurée par le contrôleur de domaine Windows du domaine défini dans le serveur NAS. L'authentification UNIX est assurée par le serveur NAS en fonction du mot de passe chiffré qui est stocké soit dans un serveur LDAP distant, soit dans un serveur NIS distant, soit dans le fichier de mots de passe local du VDM.

Informations d'identification de la sécurité en mode fichier

Pour appliquer la sécurité en mode fichier, le système de stockage doit générer des informations d'identification qui sont associées à la demande SMB ou NFS en cours de traitement. Il existe deux types d'informations d'identification : Windows et UNIX. Les informations d'identification Windows et UNIX sont générées par le serveur NAS pour les cas d'utilisation suivants :

- Pour créer des informations d'identification UNIX avec plus de 16 groupes pour une demande NFS. La propriété des informations d'identification étendues du serveur NAS doit être définie pour offrir cette possibilité.
- Pour créer des informations d'identification UNIX pour une demande SMB lorsque la stratégie d'accès au système de fichiers est UNIX.
- Pour créer des informations d'identification Windows pour une demande SMB.
- Pour créer des informations d'identification Windows pour une demande NFS lorsque la stratégie d'accès au système de fichiers est Windows.

Remarque

Pour une demande NFS lorsque la propriété des informations d'identification n'est pas définie, les informations d'identification UNIX de la demande NFS sont utilisées. Lors de l'utilisation de l'authentification Kerberos pour une demande SMB, les informations d'identification Windows de l'utilisateur du domaine sont incluses dans le ticket Kerberos de la demande de configuration de session.

Un cache persistant des informations d'identification est utilisé dans les cas suivants :

- Les informations d'identification Windows créées pour accéder à un système de fichiers ayant une stratégie d'accès Windows.

- Les informations d'identification UNIX pour l'accès via NFS si l'option d'informations d'identification étendue est activée.

Il existe une instance de cache pour chaque serveur NAS.

Autorisation d'accès à des utilisateurs non mappés
Le multiprotocole requiert les éléments suivants :

- Un utilisateur Windows doit être mappé sur un utilisateur UNIX.
- Un utilisateur UNIX doit être mappé sur un utilisateur Windows pour générer les informations d'identification Windows lorsque l'utilisateur accède à un système de fichiers qui dispose d'une stratégie d'accès Windows.

Deux propriétés sont associées au serveur NAS par rapport aux utilisateurs non mappés :

- L'utilisateur UNIX par défaut.
- L'utilisateur Windows par défaut.

Lorsqu'un utilisateur Windows non mappé tente de se connecter à un système de fichiers multiprotocole et que le compte utilisateur UNIX par défaut est configuré pour le serveur NAS, l'identifiant de l'utilisateur (UID) et l'identifiant du groupe principal (GID) de l'utilisateur UNIX par défaut sont utilisés dans les informations d'identification Windows. De même, lorsqu'un utilisateur UNIX non mappé tente de se connecter à un système de fichiers multiprotocole et que le compte utilisateur Windows par défaut est configuré pour le serveur NAS, les informations d'identification Windows de l'utilisateur Windows par défaut sont utilisées.

NOTE

Si l'utilisateur UNIX par défaut n'est pas défini dans les Services d'annuaire UNIX (UDS), l'accès SMB est refusé pour les utilisateurs non mappés. Si l'utilisateur Windows par défaut ne se trouve pas dans la LGDB ou le DC Windows, l'accès NFS sur un système de fichiers qui dispose d'une stratégie d'accès Windows est refusé pour les utilisateurs non mappés.

Remarque

L'utilisateur UNIX par défaut peut être un nom de compte UNIX existant valide ou peut utiliser le nouveau format `@uid=xxxx,gid=yyyy@`, où *xxxx* et *yyyy* sont, respectivement, les valeurs numériques décimales de l'UID et du GID principal. La configuration peut être effectuée via Unisphere ou l'interface de ligne de commande.

Informations d'identification UNIX pour demandes NFS
Pour gérer les demandes NFS pour un système de fichiers avec protocole NFS uniquement ou multiprotocole avec une stratégie d'accès UNIX ou une stratégie d'accès native, les informations d'identification UNIX doivent être utilisées. Les informations d'identification UNIX sont toujours intégrées dans chaque demande ; toutefois, les informations d'identification sont limitées à 16 groupes supplémentaires. La propriété `extendedUnixCredEnabled` du serveur NFS permet de générer des informations d'identification avec plus de 16 groupes. Si cette propriété est définie, l'UDS actif est interrogé avec l'UID pour obtenir le GID principal et tous les GID de groupe auxquels il appartient. Si l'UID ne se trouve pas dans l'UDS, les informations d'identification UNIX intégrées dans la demande sont utilisées.

Remarque

Pour l'accès sécurisé NFS, les informations d'identification sont toujours créées à l'aide de l'UDS.

Informations d'identification UNIX pour demandes SMB

Pour gérer les demandes SMB pour un système de fichiers multiprotocole avec une stratégie d'accès UNIX, les informations d'identification Windows doivent d'abord être générées pour l'utilisateur SMB lors de la configuration de la session. L'identifiant de session de l'utilisateur Windows est utilisé pour trouver l'annuaire AD. Ce nom est ensuite utilisé (éventuellement via ntxmap) pour rechercher un UID et GID Unix à partir de l'UDS ou du fichier local (fichier passwd). L'UID du propriétaire est inclus dans les informations d'identification Windows. Lors de l'accès à un système de fichiers avec une règle d'accès UNIX, l'UID de l'utilisateur est utilisé pour interroger les UDS afin de créer les informations d'identification UNIX, de la même façon que lors de la génération d'informations d'identification étendues pour NFS. L'UID est requis pour la gestion des quotas.

Informations d'identification Windows pour les demandes SMB

Pour gérer les demandes SMB pour un système de fichiers avec protocole SMB uniquement ou multiprotocole avec une stratégie d'accès Windows ou une stratégie d'accès native, les informations d'identification Windows doivent être utilisées. Les informations d'identification Windows pour SMB doivent être générées à une seule reprise, au moment de la demande de configuration de la session lorsque l'utilisateur se connecte.

Lors de l'utilisation de l'authentification Kerberos, les informations d'identification de l'utilisateur sont incluses dans le ticket Kerberos de la demande de configuration de session, ce qui n'est pas le cas lors de l'utilisation du NT LAN Manager (NTLM). D'autres informations sont alors interrogées depuis la LGDB ou le DC Windows. Pour Kerberos, la liste de SID du groupe supplémentaire provient du ticket Kerberos et de la liste de SID du groupe local supplémentaire. La liste des privilèges est extraite du LGDB. Pour NTLM, la liste de SID du groupe supplémentaire provient du DC Windows et de la liste de SID du groupe local supplémentaire. La liste des privilèges est extraite du LGDB.

En outre, l'UID correspondant et l'ID de groupe principal sont également récupérés à partir du composant de mappage utilisateur. Étant donné que le SID du groupe principal n'est pas utilisé pour la vérification d'accès, le GID principal UNIX est utilisé à la place.

Remarque

NTLM est une ancienne suite de protocoles de sécurité propriétaires qui fournit l'authentification, l'intégrité et la confidentialité aux utilisateurs. Kerberos est un protocole standard ouvert qui permet une authentification plus rapide grâce à l'utilisation d'un système de tickets. Kerberos ajoute une plus grande sécurité que le NTLM aux systèmes sur un réseau.

Informations d'identification Windows pour demandes NFS

Les informations d'identification Windows sont uniquement générées/récupérées lorsqu'un utilisateur tente d'accéder, via une demande NFS, à un système de fichiers qui dispose d'une stratégie d'accès Windows. L'UID est extrait de la demande NFS. Il existe un cache global des informations d'identification Windows pour permettre d'éviter de générer des informations d'identification pour chaque demande NFS avec une durée de conservation associée. Si les informations d'identification Windows sont détectées dans ce cache, aucune autre action n'est requise. Si les informations

d'identification Windows sont introuvables, l'UDS ou le fichier local est interrogé pour trouver le nom de l'UID. Le nom est ensuite utilisé (éventuellement via ntxmap) pour trouver un utilisateur Windows, et les informations d'identification sont récupérées à partir du contrôleur de domaine Windows ou LGDB. Si le mappage est introuvable, les informations d'identification Windows de l'utilisateur Windows par défaut sont utilisées à la place ou l'accès est refusé.

NFS sécurisé

NFS sécurisé est l'utilisation de Kerberos pour authentifier les utilisateurs ayant NFSv3 et NFSv4. Kerberos assure l'intégrité (signature) et la confidentialité (chiffrement). Il n'est pas nécessaire d'activer les options d'intégrité et de confidentialité. Il s'agit d'options d'exportation NFS.

Sans Kerberos, le serveur s'appuie entièrement sur le client pour authentifier les utilisateurs : le serveur fait confiance au client. Avec Kerberos, le serveur s'appuie sur le Centre de distribution de clés (KDC). C'est le KDC qui effectue l'authentification et gère les comptes (entités de sécurité) et le mot de passe. En outre, aucun mot de passe sous quelque forme qu'elle soit n'est envoyé sur le réseau.

Sans Kerberos, les informations d'identification de l'utilisateur sont envoyées sur le réseau non chiffrées et peuvent donc être usurpées. Avec Kerberos, l'identité (l'entité de sécurité) de l'utilisateur est intégrée au ticket Kerberos chiffré, qui ne peut être lu que par le serveur cible et le KDC. Ils sont les seuls à connaître la clé de chiffrement.

Le chiffrement AES128 et AES256 de Kerberos est pris en charge en même temps que NFS sécurisé. En plus de NFS sécurisé, cela impacte également SMB et LDAP. Ces chiffrements sont désormais pris en charge par défaut par Windows et Linux. Ces nouveaux chiffrements sont bien plus sécurisés mais c'est le client qui décide ou non de les utiliser. Le serveur se sert de l'entité de sécurité de l'utilisateur pour créer les informations d'identification de cet utilisateur en interrogeant l'UDS actif. Étant donné que NIS n'est pas sécurisé, il n'est pas recommandé de l'utiliser avec NFS sécurisé. Il est recommandé d'utiliser Kerberos avec LDAP ou LDAPS.

NFS sécurisé peut être configuré via Unisphere ou la CLI UEM.

Relations de protocole fichier

Avec Kerberos, les éléments suivants sont obligatoires :

- DNS : vous devez utiliser un nom DNS à la place des adresses IP
- NTP : tous les participants doivent être synchronisés en temps opportun.
- UDS : doit être utilisé pour créer les informations d'identification
- Nom d'hôte : Kerberos fonctionne avec des noms au lieu d'adresses IP

En fonction de la valeur du nom d'hôte, NFS sécurisé utilise un ou deux SPN. Si le nom d'hôte est au format FQDN (nom de domaine complet) hôte.domaine :

- Le SPN court est : nfs/host@REALM
- Le SPN long est : nfs/host.domainFQDN@REALM

Si le nom d'hôte n'est pas au format FQDN, seul le SPN court est utilisé.

Comme avec SMB où un serveur SMB peut être joint à un domaine, un serveur NFS peut être joint à un royaume (le terme Kerberos équivalent au terme Domaine). Pour cela, deux options sont possibles :

- Utiliser le domaine windows configuré, le cas échéant
- Configurez entièrement un royaume Kerberos basé sur le KDC UNIX

Si l'administrateur choisit d'utiliser le domaine Windows configuré, il n'y a rien d'autre à faire. Chaque SPN utilisé par le service NFS est automatiquement ajouté/supprimé

dans le KDC lorsque le serveur SMB est associé/dissocié. Notez que le serveur SMB ne peut pas être détruit si NFS sécurisé est configuré pour utiliser la configuration SMB.

Si l'administrateur choisit d'utiliser un royaume Kerberos basé sur UNIX, une configuration supplémentaire est nécessaire :

- Nom du royaume : Nom du royaume Kerberos, qui ne contient normalement que des lettres majuscules.
- Configurez entièrement un royaume Kerberos basé sur le KDC UNIX.

Pour garantir qu'un client monte une exportation NFS avec une sécurité spécifique, un paramètre de sécurité, sec, est fourni. Il indique la sécurité minimale autorisée. Il existe 4 types de sécurité :

- AUTH_SYS : La sécurité standard existante qui n'utilise pas Kerberos. Le serveur approuve les informations d'identification fournies par le client
- KRB5 : Authentification à l'aide de Kerberos v5
- KRB5i : Authentification Kerberos plus intégrité (signature)
- KRB5p : Authentification Kerberos plus intégrité, plus confidentialité (chiffrement)

Si un client NFS tente de monter une exportation avec une sécurité inférieure à la sécurité minimale configurée, l'accès est refusé. Par exemple, si l'accès minimal est KRB5i, tout montage utilisant AUTH_SYS ou KRB5 est refusé.

Création des informations d'identification
Lorsqu'un utilisateur se connecte au système, il présente uniquement son entité de sécurité, soit user@REALM, qui est extraite du ticket Kerberos. Contrairement à la sécurité AUTH_SYS, l'entité de sécurité n'est pas incluse dans la demande NFS. La partie utilisateur (avant le @) est extraite de l'entité de sécurité, puis utilisée pour rechercher L'UID correspondant dans l'UDS. Le système utilise cet UID pour créer l'entité de sécurité à l'aide de l'UDS actif, selon une procédure similaire à celle de l'activation des informations d'identification NFS Extended (sauf que, sans Kerberos, l'UID est fourni directement par la demande).

Si l'entité de sécurité n'est pas mappée dans l'UDS, les informations d'identification de l'utilisateur UNIX par défaut qui ont été configurées sont utilisées à la place. Si l'utilisateur UNIX par défaut n'est pas défini, les informations d'identification utilisées sont nobody.

Réplication
Lorsqu'un serveur NAS est la cible d'une réplication, il est possible d'accéder aux données via NFS pour la sauvegarde ou la reprise après sinistre. NFS sécurisé ne peut pas être utilisé dans ces cas, étant donné que l'utilisation des adresses IP directes n'est pas compatible avec Kerberos. En outre, le nom de domaine complet (FQDN) ne peut pas être utilisé car il peut être mappé aux interfaces de production sur la source ou aux interfaces locales sur la destination.

Contrôle d'accès dynamique

Le contrôle d'accès dynamique (DAC) permet aux administrateurs d'appliquer des autorisations et des restrictions de contrôle d'accès sur les ressources en fonction de règles bien définies pouvant concerner le degré de confidentialité des ressources, la tâche ou le rôle de l'utilisateur, et la configuration du périphérique qui est utilisé pour accéder à ces ressources.

Le contrôle d'accès basé sur les revendications (CBAC) avec contrôle d'accès dynamique (DAC) est une fonction de Windows Server 2012 qui permet de définir le contrôle d'accès sur le contrôleur de domaine via un ensemble de stratégies d'accès

central (CAP). Chaque stratégie d'accès central (identifiée par son CAPID) dispose d'un nombre de règles d'accès central (CAR) associées. Les stratégies CAP peuvent être attribuées à des objets de stratégie de groupe (GPO). Il s'agit du mécanisme permettant de distribuer des stratégies CAP à chaque serveur de fichiers. La stratégie CAP s'applique à une ressource spécifique (répertoire ou fichier) déterminée par le CAPID. Lorsqu'un serveur NAS est créé avec les partages Windows (SMB), il récupère la stratégie CAP et la règle CAR appropriées en cas de liaison avec le domaine.

Chaque règle CAR dispose des attributs suivants :

- Expression cible des ressources
- Liste ACL des autorisations effectives
- Liste ACL des autorisations proposées (facultatif)

L'expression cible des ressources (expression d'applicabilité) est évaluée pour déterminer si la CAR s'applique ou non à une ressource donnée (par exemple, @Resource.Department != @User.Department). Si cette expression prend la valeur TRUE, la liste ACL des autorisations effectives est utilisée lors de la vérification d'accès ; dans le cas contraire, la règle est ignorée. La liste ACL des autorisations proposées permet à l'administrateur de mesurer les effets des modifications proposées à appliquer aux autorisations effectives. Lorsque l'évaluation des autorisations proposées est activée, toutes les différences détectées entre les autorisations effectives et les autorisations proposées au cours d'un contrôle d'accès sont consignées dans le fichier log du serveur.

Un client Windows (Windows Server 2012 ou Windows 8.x) peut être utilisé pour associer une stratégie CAP à des ressources (répertoires ou fichiers), le cas échéant (facultatif). Lorsque cette opération est effectuée, la stratégie CAP spécifiée est appliquée par le serveur NAS pour les ressources applicables. Un client Windows peut également permettre d'effectuer la classification manuelle des ressources (par exemple, en définissant le pays ou le département).

Par défaut, la fonction DAC CBAC est activée sur le système de stockage. Toutefois, une commande de service, `svc_dac`, vous permet d'effectuer les opérations suivantes :

- Activer ou désactiver la fonction DAC - en cas de désactivation, la stratégie CAP associée à une ressource est ignorée (autrement dit, seule la fonction DACL détermine l'accès).
- Activer ou désactiver l'évaluation des autorisations proposées. Chaque règle CAR peut contenir des autorisations proposées à distribuer aux serveurs de fichiers. Généralement, seules ces autorisations ne sont pas évaluées. La commande `svc_dac` peut servir à évaluer ces autorisations. Une fois la fonction activée, toutes les différences entre les autorisations effectives et les autorisations proposées sont envoyées vers le log du serveur. L'évaluation des autorisations proposées vous permet de tester en toute sécurité les modifications proposées pour les règles CAR.
- Interroger les stratégies CAP ou les règles CAR associées à un compname du serveur NAS (par nom unique ou ID).
- Ajouter ou supprimer des règles de restauration personnalisées (pour remplacer la règle de restauration par défaut).
- Contrôler les commentaires de consignation fournis par le DAC à des fins de diagnostic.

Pour des informations détaillées sur la commande `svc_dac`, reportez-vous aux *Notes techniques sur les commandes de maintenance de la gamme EMC Unity*.

CHAPITRE 3

Consignation

Ce chapitre décrit diverses fonctions de consignation implémentées sur le système de stockage.

Les thèmes abordés sont les suivants :

Consignation

Le système de stockage conserve les types de logs répertoriés dans le tableau suivant pour le suivi des événements qui surviennent sur le système.

Tableau 8 Logs

Type de journal	Description
Log système	Informations affichées dans Unisphere pour signaler aux utilisateurs des événements du système de stockage exploitables par l'utilisateur. Ces enregistrements sont consignés dans la langue configurée par défaut pour le système. **Remarque** Les événements exploitables par l'utilisateur incluent les événements d'audit. Toutefois, tous les événements consignés ne s'affichent pas dans l'interface utilisateur graphique. Ces entrées de log d'audit ne répondant pas à un certain seuil de gravité sont consignées par le système, mais ne s'affichent pas dans l'interface utilisateur.
Alerte système	Informations utilisées par le personnel de maintenance pour diagnostiquer ou surveiller l'état ou le comportement du système de stockage. Ces enregistrements sont consignés en anglais uniquement.

Affichage et gestion des logs

Les fonctions de consignation répertoriées dans le tableau suivant sont disponibles pour les systèmes de stockage.

Tableau 9 Fonctions de consignation

Fonctionnalité	Description
Vidage du log	Lorsque le log du système de stockage atteint deux millions d'entrées, les 500 000 entrées les plus anciennes sont supprimées (compte tenu de leurs date et heure d'enregistrement) de sorte qu'il n'en reste que 1,5 million. Vous pouvez activer la consignation à distance de manière à ce que les entrées du log soient téléchargées sur un nœud réseau distant pour y être archivées ou sauvegardées. Pour plus d'informations, reportez-vous à la section Consignation à la page 40.
Niveaux de consignation	Il est impossible de configurer les niveaux de consignation pour le système de stockage. Vous ne pouvez les configurer que pour les journaux exportés, comme le décrit la section Consignation à la page 40.
Intégration des alertes	Il est possible d'afficher les informations d'alerte du système de stockage de différentes façons : • Affichage des alertes uniquement : ▪ Dans Unisphere, accédez à **Événements** > **Alertes**. • Afficher le log des événements :

Tableau 9 Fonctions de consignation (suite)

Fonctionnalité	Description
	▪ À l'aide de la CLI Unisphere, saisissez la commande `uemcli /event/alert/hist show`. ▪ Dans Unisphere, accédez à **Système** > **Service** > **Logs**.
Gestion externe du log	Vous pouvez activer la consignation à distance de manière à ce que les entrées du log soient téléchargées sur un nœud réseau distant pour y être archivées ou sauvegardées. Sur ce nœud, vous pouvez utiliser des outils tels que syslog pour filtrer et analyser les résultats du log. Pour plus d'informations, reportez-vous à la section Consignation à la page 40.
Synchronisation de l'heure	L'heure de consignation est enregistrée au format GMT d'après l'heure du système de stockage (laquelle peut être synchronisée sur l'heure réseau locale via un serveur NTP).

Options de consignation à distance

Le système de stockage prend en charge la consignation des messages utilisateur/d'audit vers cinq hôtes distants maximum. Le système de stockage doit pouvoir accéder à l'hôte distant, et la sécurité du contenu des fichiers log doit être assurée par le biais de contrôles d'accès réseau ou de la sécurité système au niveau de l'hôte distant.

Par défaut, le système de stockage peut transférer les informations du log sur le port 514 à l'aide du protocole UDP. Les paramètres de consignation à distance suivants peuvent être définis au moyen de Unisphere. Connectez-vous à Unisphere et cliquez sur **Paramètres** > **Gestion** > **Consignation à distance**.

- Activez la consignation sur un hôte distant.
- Adresse IP ou nom réseau auquel le système de stockage envoie les informations de consignation à distance.
- Type de messages de log à envoyer. Utilisez le champ Site pour définir le type de message de log. Il est recommandé de sélectionner les options Messages au niveau utilisateur.
- Niveau de gravité des événements à envoyer à un hôte distant
- Numéro et type de port (UDP ou TCP) à utiliser pour la transmission du log.

Configuration de l'hôte qui recevra les messages de log du système de stockage
Avant de configurer la consignation à distance pour un système de stockage, vous devez configurer un système distant qui recevra les messages de consignation provenant du système de stockage. Un administrateur/racine de l'ordinateur récepteur peut configurer le serveur syslog distant ou le serveur rsyslog qui recevra les informations sur les logs en modifiant le fichier de configuration de serveur syslog ou rsyslog (syslogng.conf ou rsyslog.conf) sur le système distant.

Remarque

Pour plus d'informations sur la configuration et l'exécution d'un serveur syslog distant, consultez la documentation relative au système d'exploitation exécuté sur le système distant.

CHAPITRE 4

Sécurité des communications

Ce chapitre décrit diverses fonctions de sécurité des communications implémentées sur le système de stockage.

Les thèmes abordés sont les suivants :

Utilisation des ports

Les communications avec l'interface Unisphere et la CLI s'effectuent par HTTPS sur le port 443. Les tentatives d'accès à Unisphere sur le port 80 (par HTTP) sont automatiquement redirigées sur le port 443.

Ports réseau du système de stockage

Le Tableau 10 à la page 44 présente l'ensemble des services réseau (et les ports correspondants) disponibles sur le système de stockage.

Tableau 10 Ports réseau du système de stockage

Service	Protocole	Port	Description
FTP	TCP	21	Le port 21 est le port de contrôle sur lequel le service FTP écoute les demandes FTP entrantes.
SFTP	TCP/UDP	22	Autorise les notifications d'alertes via SFTP (FTP sur SSH). SFTP est un protocole client/serveur. Les utilisateurs peuvent effectuer des transferts de fichiers sur un système de stockage situé sur le sous-réseau local, via SFTP. Permet également la connexion de contrôle FTP en sortie S'il est fermé, FTP n'est pas disponible.
SSH/SSHD, VSI	TCP/UDP	22	Autorise l'accès SSH (s'il est activé). Également utilisé pour le plug-in VSI. S'il est fermé, les connexions de gestion utilisant SSH et le plug-in VSI ne sont pas disponibles.
Mise à jour DNS dynamique	TCP/UDP	53	Utilisé conjointement avec le protocole DHCP pour transmettre les requêtes DNS au serveur DNS. S'il est fermé, la résolution de noms DNS ne fonctionne pas.
Client DHCP	UDP	67	Permet au système de stockage d'agir en tant que client DHCP lors du processus de configuration initial. Il transmet les messages du client (le système de stockage) au serveur DHCP en vue de l'obtention automatique des informations sur l'interface de gestion. Il sert également à configurer le protocole DHCP pour l'interface de gestion d'un système de stockage déjà déployé. S'il est fermé, les adresses IP dynamiques ne sont pas attribuées à l'aide de DHCP.
Client DHCP	UDP	68	Permet au système de stockage d'agir en tant que client DHCP lors du

Tableau 10 Ports réseau du système de stockage (suite)

Service	Protocole	Port	Description
			processus de configuration initial. Il reçoit les messages du serveur DHCP à destination du client (le système de stockage) en vue de l'obtention automatique des informations sur l'interface de gestion. Il sert également à configurer le protocole DHCP pour l'interface de gestion d'un système de stockage déjà déployé. S'il est fermé, les adresses IP dynamiques ne sont pas attribuées à l'aide de DHCP.
HTTP	TCP/UDP	80	Redirection du trafic HTTP vers Unisphere et la CLI Unisphere. S'il est fermé, le trafic de gestion vers le port HTTP par défaut n'est pas disponible.
NAS, VAAI-NAS	TCP	111	Fournit des datastores NAS pour VMware et est utilisé pour VAAI-NAS. S'il est fermé, les datastores NAS et VAAI-NAS ne sont pas disponibles.
Portmapper, rpcbind (infrastructure réseau)	TCP/UDP	111	Ouvert par le service portmapper ou rpcbind standard, il s'agit d'un service réseau du système de stockage auxiliaire. Il ne peut pas être arrêté. Par définition, si un système client dispose d'une connectivité réseau vers le port, il peut l'interroger. Aucune authentification n'est effectuée.
NTP	UDP	123	Synchronisation de l'heure NTP. S'il est fermé, l'heure n'est pas synchronisée entre les baies.
DCE Remote Procedure Call (DCERPC) et NDMP	UDP	135	Plusieurs fonctions pour le client Microsoft. Également utilisé pour NDMP.
Service de noms NETBIOS (SMB)	TCP/UDP	137	Le service de noms NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction (Wins). S'il est désactivé, ce port désactive tous les services associés à SMB.
Service de datagrammes NETBIOS (SMB)	UDP	138	Le service de datagrammes NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction. Seul le service de navigation est utilisé. S'il est

Tableau 10 Ports réseau du système de stockage (suite)

Service	Protocole	Port	Description
			désactivé, ce port désactive la fonction de navigation.
Service de session NETBIOS (SMB)	TCP/UDP	139	Le service de session NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction. Si les services SMB sont activés, ce port est ouvert. Cela est particulièrement nécessaire pour les versions antérieures du système d'exploitation Windows (avant Windows 2000). Les clients autorisés à accéder aux services SMB du système de stockage doivent disposer d'une connectivité réseau vers le port pour assurer la continuité des opérations.
SNMP Unix Multiplexer	TCP	199	Communications SNMP. S'il est fermé, les mécanismes d'alerte du système de stockage reposant sur SNMP ne sont pas envoyés.
LDAP	TCP/UDP	389	Requêtes LDAP non sécurisées. S'il est fermé, les requêtes d'authentification LDAP non sécurisées ne sont pas disponibles. La configuration du service LDAP sécurisé est une solution alternative.
Protocole SLP (Service Location Protocol)	TCP/UDP	427	Permet aux hôtes (ou autres ressources) de découvrir les services disponibles fournis par un système de stockage.
HTTPS	TCP/UDP	443	Trafic HTTP sécurisé vers Unisphere et la CLI Unisphere. S'il est fermé, la communication avec la baie n'est pas possible. **Remarque** Dans le cas de SMI-S, il sert à la gestion de la baie. À noter cependant que le port 5989 est dédié par défaut à cette tâche.
SMB	TCP	445	SMB (sur le contrôleur de domaine) et port de connectivité SMB pour clients Windows 2000 et supérieurs. Les clients autorisés à accéder aux services SMB du système de stockage doivent disposer d'une connectivité réseau vers le port pour assurer la continuité des

Tableau 10 Ports réseau du système de stockage (suite)

Service	Protocole	Port	Description
			opérations. La désactivation de ce port désactive tous les services associés à SMB. Si le port 139 est également désactivé, le partage de fichiers SMB est désactivé.
DHCP (IPv6 uniquement)	UDP	546	Client DHCP (v6). S'il est fermé, les adresses IP dynamiques ne sont pas attribuées à l'aide de DHCP.
DHCP (IPv6 uniquement)	UDP	547	Serveur DHCP (v6). S'il est fermé, les adresses IP dynamiques ne sont pas attribuées à l'aide de DHCP.
LDAPS	TCP/UDP	636	Requêtes LDAP sécurisées. S'il est fermé, l'authentification LDAP sécurisée n'est pas disponible.
FTP	TCP	1024:65535	Utilisé pour le transfert FTP passif. Le port 1024:65535 est lié aux données, tandis que le port 1025:65535 est liée à la gestion.
mountd (NFS)	TCP/UDP	1234	Utilisé pour le service mount, qui est un composant principal du service NFS (versions 2, 3 et 4) et un composant important de l'interaction entre le SP et le serveur NAS.
NAS, VAAI-NAS	TCP	2049	Fournit des datastores NAS pour VMware et est utilisé pour VAAI-NAS. S'il est fermé, les datastores NAS et VAAI-NAS ne sont pas disponibles.
NFS	TCP/UDP	2049	Utilisé pour fournir des services NFS.
UDI SSH	TCP	2222	Redirige le trafic à partir du port 22 pour l'eth* du périphérique.
iSCSI	TCP	3260	Permet l'accès aux services iSCSI. S'il est fermé, les services iSCSI en mode fichier ne sont pas disponibles.
NFS	TCP/UDP	4 000	Utilisé pour fournir des services statd NFS. statd surveille l'état de verrouillage des fichiers NFS. Il fonctionne conjointement avec le service lockd afin d'offrir des fonctions de restauration après sinistre pour NFS. S'il est fermé, les services NAS statd ne sont pas disponibles.
NFS	TCP/UDP	4001	Utilisé pour fournir des services lockd NFS. lockd est le processus de verrouillage de fichiers NFS. Il traite les demandes de verrouillage émanant des

Tableau 10 Ports réseau du système de stockage (suite)

Service	Protocole	Port	Description
			clients NFS et fonctionne conjointement avec le processus statd. S'il est fermé, les services NAS lockd ne sont pas disponibles.
NFS	TCP/UDP	4002	Utilisé pour fournir des services NFS rquotad. Le processus rquotad fournit des informations de quota aux clients NFS qui ont monté un système de fichiers. S'il est fermé, les services NAS rquotad ne sont pas disponibles.
SMB	UDP	4003	Permet de consulter ou modifier la liste de contrôle d'accès SMB à partir d'un hôte Linux avec les outils `emcgetsd` ou `emcsetsd`.
PAX (Portable Archive Interchange) (services de sauvegarde)	TCP	4658	• PAX est un protocole d'archivage de système de stockage qui utilise les formats de bande UNIX standard. • Ce service doit établir une liaison avec plusieurs interfaces réseau internes. Par conséquent, il se connecte également à l'interface externe. Les demandes entrantes émanant du réseau externe sont cependant rejetées. • Les informations générales sur PAX figurent dans la documentation EMC correspondante relative aux sauvegardes. Cette rubrique contient plusieurs modules techniques qui présentent différents outils de sauvegarde.
VSI	TCP	5080	Ce port prend en charge le plug-in VSI. S'il est fermé, le plug-in VSI n'est pas disponible.
Services de réplication	TCP	5085	Associé aux services de réplication
KMIP (Key Management Interoperability Protocol)	TCP	5696	Pour KMIP, prend en charge la gestion des clés externes à l'aide de KMIP. En cas de fermeture, les services KMIP ne sont pas disponibles.
SMI-S	TCP	5989	Dans le cas de SMI-S, il sert à la gestion de la baie. Le client SMI-S se connecte à la baie via le port HTTPS SMI-S TCP 5989. Le *Guide de programmation du fournisseur SMI-S* fournit plus d'informations sur la configuration de ce service.

Tableau 10 Ports réseau du système de stockage (suite)

Service	Protocole	Port	Description
VASA	TCP	8443	Fournisseur VASA pour VASA 2.0.
VASA	TCP	8444	Fournisseur VASA pour VASA 1.0.
RCP (services de réplication)	TCP	8888	Utilisé par le réplicateur (sur le côté secondaire). Le réplicateur le laisse ouvert dès lors que certaines données doivent être répliquées. Une fois démarré, ce service ne peut pas être arrêté.
NDMP	TCP	10 000	• Vous permet de contrôler la restauration et la sauvegarde d'un serveur Network Data Management Protocol (NDMP) via une application de sauvegarde réseau, sans nécessiter l'installation d'un logiciel tiers sur le serveur. Dans un système de stockage, le serveur NAS fonctionne comme un serveur NDMP. • Le service NDMP peut être désactivé si la sauvegarde sur bande NDMP n'est pas utilisée. • Le service NDMP est authentifié à l'aide d'un nom d'utilisateur et d'un mot de passe. Le nom d'utilisateur peut être configuré. La documentation NDMP décrit comment configurer le mot de passe pour différents environnements.
NDMP	TCP	10500:10531	Pour les sessions de sauvegarde/ restauration tridirectionnelle, les serveurs NAS utilisent les ports 10500 à 10531.
IWD	Interne	60260	Processus de configuration initiale IWD. S'il est fermé, l'initialisation de la baie n'est pas disponible via le réseau.

Ports que le système de stockage peut contacter

Le système de stockage fonctionne comme un client réseau dans de nombreuses situations, par exemple lorsqu'il communique avec un serveur LDAP. Dans ces cas, le système de stockage initie la communication et l'infrastructure réseau doit prendre en charge ces connexions. Le Tableau 11 à la page 50 décrit les ports auxquels un système de stockage doit avoir accès pour que le service correspondant fonctionne correctement. Cela inclut l'interface de ligne de commande Unisphere.

Tableau 11 Connexions réseau pouvant être initiées par le système de stockage

Service	Protocole	Port	Description
FTP	TCP	20	Port utilisé pour les transferts de données FTP. Ce port peut être ouvert par l'activation de FTP, comme décrit à la ligne suivante. L'authentification est effectuée sur le port 21 et définie par le protocole FTP.
FTP/SFTP	TCP	21	Autorise les notifications d'alertes via SFTP (FTP sur SSH). SFTP est un protocole client/serveur. Les utilisateurs peuvent effectuer des transferts de fichiers sur un système de stockage situé sur le sous-réseau local, via SFTP. Permet également la connexion de contrôle FTP en sortie S'il est fermé, FTP n'est pas disponible.
SSH/SSHD, VSI	TCP	22	Autorise l'accès SSH (s'il est activé). Également utilisé pour le plug-in VSI. S'il est fermé, les connexions de gestion utilisant SSH et le plug-in VSI ne sont pas disponibles.
SMTP	TCP	25	Permet au système d'envoyer des e-mails. S'il est fermé, les notifications par e-mail ne sont pas disponibles.
DNS	TCP/UDP	53	Requêtes DNS. S'il est fermé, la résolution de noms DNS ne fonctionne pas.
DHCP	UDP	67-68	Permet au système de stockage de faire office de client DHCP. S'il est fermé, les adresses IP dynamiques ne sont pas attribuées à l'aide de DHCP.
HTTP	TCP	80	Redirection du trafic HTTP vers Unisphere et la CLI Unisphere. S'il est fermé, le trafic de gestion vers le port HTTP par défaut n'est pas disponible.
Kerberos	TCP/UDP	88	Fournit un ticket Kerberos en sortie. S'il est fermé, l'authentification Kerberos et tous les protocoles qui l'utilisent, par exemple SMB, LDAP, GPO, secNFS, etc., ne sont pas disponibles.
Portmapper, rpcbind (infrastructure réseau)	TCP/UDP	111	Ouvert par le service portmapper ou rpcbind standard, il s'agit d'un service réseau du système de stockage auxiliaire. Il ne peut pas être arrêté. Par définition, si un système client dispose d'une connectivité réseau vers le port, il peut l'interroger. Aucune authentification n'est effectuée.
NTP	UDP	123	Synchronisation de l'heure NTP. S'il est fermé, l'heure n'est pas synchronisée entre les baies.
Service de noms NETBIOS (SMB)	TCP/UDP	137	Le service de noms NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction (Wins). S'il est désactivé, ce port désactive tous les services associés à SMB.
Service de datagrammes NETBIOS (SMB)	UDP	138	Le service de datagrammes NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction. Seul le service de navigation est utilisé. S'il est désactivé, ce port désactive la fonction de navigation.

Tableau 11 Connexions réseau pouvant être initiées par le système de stockage (suite)

Service	Protocole	Port	Description
Service de session NETBIOS (SMB)	TCP/UDP	139	Le service de session NETBIOS est associé aux services de partage de fichiers SMB du système de stockage et constitue l'un des principaux composants de cette fonction. Si les services SMB sont activés, ce port est ouvert. Cela est particulièrement nécessaire pour les versions antérieures du système d'exploitation Windows (avant Windows 2000). Les clients autorisés à accéder aux services SMB du système de stockage doivent disposer d'une connectivité réseau vers le port pour assurer la continuité des opérations.
LDAP	TCP/UDP	389[a]	Requêtes LDAP non sécurisées. S'il est fermé, les requêtes d'authentification LDAP non sécurisées ne sont pas disponibles. La configuration du service LDAP sécurisé est une solution alternative.
Protocole SLP (Service Location Protocol)	TCP/UDP	427	Permet aux hôtes (ou autres ressources) de découvrir les services disponibles fournis par un système de stockage.
HTTPS	TCP	443	Trafic HTTPS vers Unisphere et l'interface de ligne de commande Unisphere, et pour les services sécurisés à distance si la fonction ESRS est activée et Integrated ESRS est configurée sur le système de stockage. S'il est fermé, la communication avec la baie n'est pas possible.
Kerberos	TCP/UDP	464	Permet la modification et la définition du mot de passe Kerberos. S'il est fermé, SMB est affecté.
Syslog distant	UDP	514[a]	Syslog - Consigner des messages du système sur un hôte distant. Vous pouvez configurer le port hôte utilisé par le système.
LDAPS	TCP/UDP	636[a]	Requêtes LDAP sécurisées. S'il est fermé, l'authentification LDAP sécurisée n'est pas disponible.
VMware	TCP	843	VMawareness - Permet la communication du SDK VMware avec vSphere. S'il est fermé, la découverte VCenter/ESX n'est pas disponible.
FTP	TCP	1024:65535	Fournit la connexion de contrôle FTP en sortie. S'il est fermé, FTP n'est pas disponible.
SOCKS	TCP	1080	Le port 1080 est le port utilisé par défaut lorsqu'aucun port n'est spécifié et que la fonction ESRS est activée et que les services ESRS intégrés sont configurés sur le système de stockage. De plus, un pare-feu est utilisé entre le système de stockage et un serveur proxy. Si le port par défaut ou spécifié par l'utilisateur est fermé, la communication avec la baie via le port sera impossible.
mountd (NFS)	TCP/UDP	1234	Utilisé pour le service mount, qui est un composant principal du service NFS (versions 2, 3 et 4) et un composant important de l'interaction entre le SP et le serveur NAS.
NFS	TCP/UDP	2049	Utilisé pour fournir des services NFS.

Tableau 11 Connexions réseau pouvant être initiées par le système de stockage (suite)

Service	Protocole	Port	Description
HTTP	TCP	3128	Le port 3128 est le port utilisé par défaut lorsqu'aucun port n'est spécifié et que la fonction ESRS est activée et que les services ESRS intégrés sont configurés sur le système de stockage. De plus, un pare-feu est utilisé entre le système de stockage et un serveur proxy. Si le port par défaut ou spécifié par l'utilisateur est fermé, la communication avec la baie via le port sera impossible.
iSNS	TCP	3205	Utilisé pour envoyer les enregistrements iSNS (Internet storage naming service) au serveur iSNS.
iSCSI	TCP	3260	Permet l'accès aux services iSCSI. S'il est fermé, les services iSCSI en mode fichier ne sont pas disponibles.
NFS	TCP/UDP	4 000	Utilisé pour fournir des services statd NFS. statd surveille l'état de verrouillage des fichiers NFS. Il fonctionne conjointement avec le service lockd afin d'offrir des fonctions de restauration après sinistre pour NFS.
NFS	TCP/UDP	4001	Utilisé pour fournir des services lockd NFS. lockd est le processus de verrouillage de fichiers NFS. Il traite les demandes de verrouillage émanant des clients NFS et fonctionne conjointement avec le processus statd.
NFS	TCP/UDP	4002	Utilisé pour fournir des services NFS rquotad. Le processus rquotad fournit des informations de quota aux clients NFS qui ont monté un système de fichiers.
VSI	TCP	5080	Ce port prend en charge le plug-in VSI. S'il est fermé, le plug-in VSI n'est pas disponible.
KMIP	TCP	5696	Pour KMIP, prend en charge la gestion des clés externes à l'aide de KMIP. En cas de fermeture, les services KMIP ne sont pas disponibles.
HTTPS	TCP	8443	Trafic HTTPS pour le support sécurisé à distance si la fonction ESRS est activée et Integrated ESRS est configurée sur le système de stockage. S'il est fermé, il y aura une diminution considérable des performances du support à distance, ce qui aura un impact direct sur le temps de résolution des problèmes sur le système de stockage Unity.
REST	TCP	9443	Utilisé pour envoyer des notifications de service vers un serveur de passerelle ESRS lorsque ESRS est activée et Centralized ESRS est configurée sur le système de stockage.
Common AntiVirus Agent (CAVA)	TCP	12228	Utilisé pour fournir une solution de protection antivirus CAVA aux clients utilisant un serveur NAS. En cas de fermeture, la solution antivirus CAVA ne sera pas disponible.
IWD	Interne	60260	Processus de configuration initiale IWD. S'il est fermé, l'initialisation de la baie n'est pas disponible via le réseau.

a. Les numéros de port LDAP et LDAPS peuvent être remplacés à partir de Unisphere lors de la configuration des services d'annuaire. Le numéro de port par défaut s'affiche dans une zone de saisie et peut être remplacé par l'utilisateur. De même, le numéro de port Syslog distant peut être remplacé à partir de Unisphere.

Certificat du système de stockage

Le système de stockage génère automatiquement un certificat auto-signé lors de sa première initialisation. Ce certificat est conservé à la fois en NVRAM et sur la LUN back-end. Il est ensuite présenté aux clients qui essaient de se connecter au système de stockage par l'intermédiaire du port de gestion.

Le certificat est configuré pour expirer après 3 ans. Toutefois, le système de stockage le régénère un mois avant sa date d'expiration. Vous pouvez par ailleurs télécharger un nouveau certificat à l'aide de la commande de maintenance `svc_custom_cert`. Cette commande installe le certificat SSL spécifié au format PEM en vue de son utilisation avec l'interface de gestion Unisphere. Pour plus d'informations sur cette commande de maintenance, consultez le document *Notes techniques sur les commandes de maintenance*. Vous ne pouvez pas afficher le certificat via Unisphere ou la CLI Unisphere. Il est cependant possible de le visualiser au moyen d'un client de type navigateur ou d'un outil Web qui tente de se connecter au port de gestion.

Remarque

Si la baie est en mode FIPS et qu'un certificat est généré hors baie, outre le codage PEM du certificat, la clé privée doit être au format PKCS#1. Vous pouvez utiliser la commande openssl pour effectuer cette conversion. Une fois les fichiers .cer et .pk générés, cette étape supplémentaire est obligatoire si le certificat est utilisé sur une baie en mode FIPS.

Pour renforcer la sécurité, certaines entreprises utilisent le chaînage de certificats d'AC. Une chaîne de certificats relie entre eux plusieurs certificats d'AC. Le certificat d'AC principal correspond au certificat racine qui figure à la fin de la chaîne de certificats d'AC. Dans la mesure où le système a besoin de la chaîne de certificats complète pour vérifier l'authenticité d'un certificat reçu, demandez à l'administrateur du serveur d'annuaire si la méthode de chaînage de certificats est utilisée. Si tel est le cas, vous devez concaténer tous les certificats appropriés dans un seul fichier et télécharger cette version. Le certificat doit être codé au format PEM/Base64 et utiliser le suffixe .cer.

Remplacement d'un certificat auto-signé du système de stockage avec des certificats signés provenant d'une autorité de certification locale

Avant de pouvoir télécharger de nouveaux certificats pour le système de stockage à partir d'une autorité de certification locale afin de remplacer les certificats SSL auto-signés Unisphere existants, vous devez procéder comme suit :

1. Créez une clé privée sur le processeur de stockage (SP).

Remarque

Par exemple :

```
22:59:02 service@unknown spa:~/openssl> openssl genrsa -des3 -out
unitycert.key -passout pass:emcemc
Generating RSA private key, 2048 bit long modulus
.............................+++
.....................................................................
+++
e is 65537 (0x10001)
```

2. Supprimez la phrase de passe de la clé sur le SP.

NOTE

Cette étape est très importante. Si la phrase de passe n'est pas supprimée de la clé, cela entraînera un dysfonctionnement du SP.

Remarque

Par exemple :

```
22:59:08 service@unknown spa:~/openssl> openssl rsa -in unitycert.key -
passin pass:emcemc -out unitycert.pk
writing RSA key
```

3. Demandez une CSR sur le SP.

Remarque

Par exemple :

```
22:59:12 service@unknown spa:~/openssl> openssl req -new -sha256 -key
unitycert.pk -out unitycert.csr -days 1825
-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'
```

Ici, **`-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'`** est un exemple, vous devez le modifier pour qu'il corresponde à votre environnement.

4. Obtenez la CSR signée par votre CA (serveur Windows CA, serveur Openssl CA ou autre serveur CA). Voici des exemples d'envoi d'une CSR à un serveur CA pour signature, par les moyens suivants :
   - Imprimez la CSR à l'aide de la commande `cat`, copiez-la ou collez-la dans votre bloc-notes local et nommez-la unitycert.csr.

```
23:00:01 service@unknown spa:~/openssl> cat unitycert.csr
 -----BEGIN CERTIFICATE REQUEST-----
MIICljCCAX4CAQAwUTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1BMREwDwYDVQ
QH
DAhTYXJhc290YTEPMA0GA1UECgwGTXlDdXN0MREwDwYDVQQDDAgxMC4wLjAuMT
CC

ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOBxqufN1Vpm0hq5K5UU0o
```

```
cd
teL2hJr5T1WIOmwQreX4nIdHIxVoWmyepmT7IZJIrQZQc8GuFDRx5qZ/
cwlxoup7
3aprMKCx8Ka6nQE3ue46tehYxqwA7mCyT1XYIW7c5l1HJmEddj
+Lqj23OwXTkOjX
skzubLfI08zDgYyW+KrmMmnAQIpPucHiX8FmjhilNGUXXiN7f/
jtDq4M1QZcj2Vp
CVySMB5b1bGs1u10HQcv/
aBSE5cU7FAxaLyJpIHJnk8fPXJo02hSu6B3NG7RDa1B
35gW6qqlbFIjXUlWtzi4JKA6GIzCq576YcGeQA5QuIrKqE6feeTjsKD1Ac9tXa
cC
AwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQBpJn2Fu9noAMhn
+IbTJf9EVTAYsZGc
ddtgZcnVgEpI/dxB0p4ME210hg28UEwKl0wFAypGm8LaMxg0lbtfpUpU31JbaS
+2
lJc/79vxTfrWWNnSF95C+wer2LB93VLov8MSQqPZfl0LPb4NRU/
XaE4l9Vh5DYl4
/FmwHXsifwV5f1TUkvhC8YTwn5frWQjruz
+ItZ3z9DetQX0OXYXMcaPX5Qp6aU5m
dsXFHDDiaVbOofJN9z6OPOsWUhn0ZwEpnW8q/
+V72MdBIfiwEjoQqZZKh4w1l0/7
uElP8BfS7vH/i87OCqHJM0g/O3IndF+p5wYzmhrDPg/f3belQVQvKs7Z
-----END CERTIFICATE REQUEST-----
```

- Téléchargez la CSR par protocole SCP (Secure Copy Protocol).

Remarque

Pour télécharger les fichiers CSR à l'aide du protocole SCP, utilisez un outil tiers (par exemple, WinSCP) pour vous connecter à l'interface IP de gestion Unity (nom d'utilisateur : service), puis copiez le fichier `unitycert.csr` sur l'ordinateur local.

5. Après avoir obtenu le certificat signé du serveur CA, téléchargez-le sur le SP et enregistrez son nom sous `unitycert.crt` (correspondant à `unitycert.pk`).

Remarque

Par exemple :

```
$ svc_custom_cert unitycert

Example:
service@spa spa:~> svc_custom_cert pod6 Successfully installed custom
certificate files. Restarting web server ...
Unsupported
Sun May 22 05:37:48 2016:7645\0x7f44ba3e27c0:32:Module CIC/1.1.10.6
loaded
```

Interfaces, services et fonctions du système de stockage compatibles IPv6

Vous pouvez configurer les interfaces d'un système et attribuer des adresses IPv6 (Internet Protocol version 6) aux différents services et fonctions. La liste suivante répertorie les fonctions prenant en charge le protocole IPv6 :

- Interfaces (SF, iSCSI) : allocation statique d'une adresse IPv4 ou IPv6 à une interface.
- Hôtes : attribution d'un nom de réseau, d'une adresse IPv4 ou d'une adresse IPv6 à un hôte.

- Routes : configuration d'une route pour le protocole IPv4 ou IPv6.
- Diagnostics : exécution d'une commande de diagnostic `ping` depuis la CLI sur une adresse de destination IPv4 ou IPv6. Dans Unisphere, sélectionnez **Paramètres** > **Accès** > **Routage** > **Commande ping/traceroute** pour accéder à l'écran de la commande Ping/traceroute qui prend aussi en charge les adresses de destination IPv6.

Tous les composants du système de stockage prennent en charge IPv4, et la plupart prennent en charge IPv6. Le Tableau 12 à la page 56 indique la disponibilité de la prise en charge d'IPv6 par type de paramètre et composant :

Tableau 12 Prise en charge d'IPv6 par type de paramètre et composant

Type de paramètre	Composant	Prise en charge d'IPv6
Paramètres de gestion Unisphere	Port de gestion	Oui
	Serveur DNS (Domain Name System)	Oui
	Serveur NTP (Network Time Protocol)	Oui
	Serveur de consignation à distance	Oui
	Serveur LDAP	Non
Paramètre de configuration hôte Unisphere	Microsoft Exchange	Oui
	Datastore VMware (NFS)	Oui
	Datastore VMware (VMFS)	Oui
	Datastore Hyper-V	Oui
Paramètre d'alerte Unisphere	Destinations de trap SNMP	Oui
	Serveur SMTP	Oui
	Services à distance sécurisés EMC (ESRS)	Non
Paramètre du serveur de stockage	Serveur iSCSI	Oui
	Serveur de dossiers partagés	Oui
	Serveur NIS (Network Information Service) (pour serveurs NAS NFS)	Oui
	Serveur Active Directory (pour serveurs NAS SMB)	Oui
	Serveur iSNS (Internet Storage Service)	Oui
Autre	Destinations PING	Oui
	Log distant	Oui
	LDAP	Oui

Norme d'adressage IPv6

IPv6 (Internet Protocol version 6) est une norme d'adressage IP développée par l'IETF (Internet Engineering Task Force) pour compléter et, à terme, remplacer la norme d'adressage IPv4 actuellement utilisée par la plupart des services Internet.

IPv4 utilise des adresses IP de 32 bits, soit environ 4,3 milliards d'adresses possibles. Avec la recrudescence des internautes et des périphériques reliés à Internet, l'espace d'adressage IPv4 disponible est devenu insuffisant. Le protocole IPv6 résout le problème de pénurie d'adresses, car il utilise des adresses sur 128 bits, soit un total d'environ 340 trillions d'adresses. Il remédie également à d'autres problèmes liés à l'IPv4, comme la mobilité, la configuration automatique et la capacité globale d'extension.

Une adresse IPv6 est une valeur hexadécimale contenant huit champs de 16 bits séparés par le signe deux-points :

`hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh`

Chaque champ d'une adresse IPv6 est composé de chiffres compris entre 0 et 9, ou de lettres allant de A à F.

Pour en savoir plus, consultez les informations relatives à la norme IPv6 (RFC 2460) sur le site Web de l'IETF (http://www.ietf.org).

Accès à l'interface de gestion du système de stockage à partir d'une adresse IPv6

Lorsque vous définissez des connexions de gestion dans le système de stockage, vous pouvez configurer le système pour qu'il accepte les types d'adresses IP suivants :

- adresses IPv6 (Internet Protocol version 6) statiques, adresses IPv4 obtenues via DHCP et adresses IPv4 statiques ;
- adresses IPv4 uniquement.

Vous pouvez attribuer les adresses IPv6 à l'interface de gestion de manière statique. L'adresse IPv6 de l'interface de gestion peut être définie sur deux modes : manuelle/statique ou désactivée. La désactivation d'IPv6 ne supprime pas la liaison entre le protocole et l'interface. La commande de désactivation supprime toute adresse IPv6 unicast attribuée à l'interface de gestion si bien que le système de stockage ne répond plus aux demandes envoyées sur IPv6. Par défaut, la fonction IPv6 est désactivée.

Après l'installation, le câblage et la mise sous tension du système, vous devez attribuer une adresse IP à l'interface de gestion du système de stockage. Si le système de stockage ne fait pas partie d'un réseau dynamique ou si vous préférez lui attribuer une adresse IP statique de façon manuelle, vous devez télécharger, installer et exécuter le logiciel Connection Utility. Pour plus d'informations sur Connection Utility, reportez-vous à la section Exécution de Connection Utility à la page 59.

Les demandes entrantes adressées au système de stockage sur IPv6 via l'interface de gestion sont prises en charge Vous pouvez configurer l'interface de gestion d'un système de stockage pour qu'elle fonctionne dans un environnement exclusivement IPv4 ou IPv6, ou bien mixte. Il est également possible de gérer le système de stockage à l'aide de l'interface utilisateur et de l'interface de ligne de commande (CLI) Unisphere.

Les services sortants, tels que NTP et DNS, prennent en charge l'adressage IPv6 au moyen d'adresses IPv6 explicites ou bien de noms DNS. Si un nom DNS est résolu à la fois en adresse IPv6 et IPv4, le système de stockage communique avec le serveur sur IPv6.

Les commandes CLI set et show de l'interface de réseau de gestion qui sont utilisées pour gérer les interfaces de gestion comprennent les attributs relatifs à IPv6. Pour plus d'informations sur ces commandes et attributs de l'interface de réseau de gestion, consultez le *Guide d'utilisation de l'interface de ligne de commande Unisphere*.

Configuration de l'interface de gestion via DHCP

Après l'installation, le câblage et la mise sous tension du système, vous devez attribuer une adresse IP à l'interface de gestion du système de stockage. Si le système de stockage fonctionne dans un réseau dynamique comprenant des serveurs DHCP et DNS, l'adresse IP de gestion peut être attribuée de manière automatique.

Remarque

Si vous n'utilisez pas le système de stockage dans un réseau dynamique ou que vous préférez lui attribuer une adresse IP statique de façon manuelle, vous devez installer et exécuter le logiciel Connection Utility. Pour plus d'informations sur Connection Utility, reportez-vous à la section Exécution de Connection Utility à la page 59.

La procédure de configuration réseau appropriée comprend la définition de la plage d'adresses IP disponibles, des masques de sous-réseau corrects, ainsi que des adresses de passerelles et de serveurs de noms. Pour plus d'informations sur la configuration de serveurs DHCP et DNS, consultez votre documentation réseau.

DHCP est un protocole utilisé pour attribuer des adresses IP dynamiques aux périphériques d'un réseau. Il vous permet de gérer les adresses IP depuis un serveur centralisé et d'attribuer automatiquement une adresse IP unique à chaque nouveau système de stockage rattaché au réseau de votre entreprise. Ce système d'adressage dynamique simplifie l'administration réseau, car le logiciel assure le suivi des adresses IP à la place de l'administrateur.

Le serveur DNS utilise le protocole IP pour convertir les noms de domaine en adresses IP. Par opposition aux adresses IP numériques, les noms de domaine sont alphabétiques, ce qui les rend généralement plus faciles à mémoriser. Un réseau IP reposant sur des adresses IP, chaque fois que vous utilisez un nom de domaine, le serveur DNS le convertit en adresse IP correspondante. Par exemple, le nom de domaine www.Javanet.com équivaut à l'adresse IP 209.94.128.8.

Aucune information administrative, telle que noms d'utilisateur ou mots de passe, n'est échangée lors de la configuration DHCP/DNS dynamique. La configuration des éléments IP de gestion (préférence DHCP, serveurs DNS et NTP) est régie par le framework de sécurité Unisphere existant. Les événements DNS et DHCP, comme l'obtention d'une nouvelle adresse IP à l'expiration du bail, sont consignés dans des logs d'audit du système de stockage. Si la configuration de l'adresse IP de gestion du système de stockage n'est pas configurée via DHCP, aucun port réseau supplémentaire n'est ouvert.

Les adresses IP dynamiques (DHCP) ne doivent pas être utilisées pour les composants des serveurs ESRS (Services à distance sécurisés EMC, Édition virtuelle), des serveurs Policy Manager ou des périphériques gérés.

Remarque

Si vous utilisez le protocole DHCP pour attribuer des adresses IP aux composants ESRS (serveurs ESRS VE, Policy Manager ou périphériques gérés), des adresses IP statiques doivent leur être définies. Les attributions d'adresses IP utilisées par les périphériques EMC ne doivent pas expirer. EMC vous recommande d'attribuer des adresses IP statiques à ces périphériques que vous souhaitez faire gérer par ESRS.

Exécution de Connection Utility

Remarque

Si le système de stockage fonctionne dans un environnement réseau dynamique comprenant des serveurs DHCP et DNS, vous n'avez pas besoin d'utiliser le logiciel Connection Utility. Une adresse IP dynamique (IPv4 uniquement) peut être automatiquement attribuée à l'interface de gestion du système de stockage. Lorsqu'un système de stockage utilise une adresse IP statique, celle-ci lui est associée manuellement via le logiciel Connection Utility. Le problème, avec les adresses statiques, est qu'il suffit d'une simple faute d'inattention pour que la même adresse de gestion IP soit attribuée par erreur à deux systèmes de stockage. Cela crée un conflit susceptible d'entraîner la perte de la connectivité réseau. L'emploi de DHCP pour attribuer des adresses IP de façon dynamique réduit le risque de conflits. Les systèmes de stockage configurés pour l'attribution d'adresses IP via DHCP n'ont pas besoin d'adresses IP statiques.

Le programme d'installation de Connection Utility est disponible à partir du site Web de Support en ligne EMC (https://support.emc.com), sous la sélection **Téléchargements**, dans la barre de menus de la page produit de votre système de stockage. Une fois le logiciel téléchargé, installez-le sur un hôte Windows. Si vous exécutez Connection Utility à partir d'un ordinateur situé sur le même sous-réseau que le système de stockage, Connection Utility découvre automatiquement tout système de stockage non configuré. Si vous exécutez Connection Utility sur un autre sous-réseau, vous pouvez enregistrer la configuration sur une clé USB, puis la transférer sur le système de stockage. Si le système de stockage se trouve sur un sous-réseau différent de celui de l'hôte qui exécute le logiciel Connection Utility, vous pouvez sélectionner cette option pour configurer et enregistrer manuellement les informations de nom d'hôte et de réseau IP sur un lecteur USB sous la forme d'un fichier texte. Ensuite, vous pouvez insérer le disque USB dans un SP, ce qui définira automatiquement les informations de nom d'hôte et de réseau IP.

Remarque

Vous ne pouvez pas modifier l'adresse IP de gestion lorsque les deux processeurs de stockage (SP) sont en Mode maintenance.

Après avoir exécuté Connection Utility et transféré la configuration sur votre système de stockage, vous pouvez vous connecter à ce dernier via un navigateur Web à partir de l'adresse IP que vous avez attribuée à l'interface de gestion du système de stockage :

Lorsque vous vous connectez au système de stockage pour la première fois, l'Assistant Configuration initiale démarre. L'Assistant Configuration initiale vous permet de procéder à la configuration initiale du système de stockage pour créer des ressources de stockage.

Remarque

Pour plus d'informations concernant le logiciel Connection Utility, reportez-vous au *Guide d'installation de la gamme Unity*.

Chiffrement et signature du protocole (SMB)

La prise en charge du protocole SMB 3.0 et de Windows 2012 sur le système de stockage permet aux hôtes compatibles SMB de bénéficier de fonctions de chiffrement SMB. Le chiffrement SMB assure l'accès sécurisé aux données des partages de fichiers SMB. Il garantit la sécurité des informations sur les réseaux non approuvés grâce à un chiffrement de bout en bout des données SMB en transit entre la baie et l'hôte. Les données sont protégées des attaques de type écoute électronique/espionnage sur les réseaux non approuvés.

Le chiffrement SMB peut être configuré pour chaque partage. Une fois le chiffrement activé sur un partage, tout client SMB3 doit chiffrer l'ensemble des demandes liées au partage. Sinon, l'accès au partage lui est refusé.

Pour activer le chiffrement SMB, définissez l'option **Chiffrement du protocole** dans les propriétés du partage SMB avancées dans Unisphere ou définissez-le via les commandes CLI `create` et `set` pour les partages SMB. Aucun paramétrage n'est requis sur le client SMB.

Remarque

Pour plus d'informations sur la définition du chiffrement SMB, consultez l'aide en ligne de Unisphere et le *Guide d'utilisation de l'interface de ligne de commande Unisphere*.

SMB permet également la validation de l'intégrité des données (signature). Ce mécanisme permet de s'assurer qu'un paquet n'a pas été intercepté, modifié ou rediffusé. La signature SMB ajoute une signature à chaque paquet et garantit qu'un tiers n'a pas changé les paquets.

Pour utiliser la signature SMB, cette fonction doit être activée sur le client et le serveur engagés dans une transaction. Par défaut, les contrôleurs de domaine Windows Server exigent que les clients utilisent la signature SMB. Pour les domaines Windows Server (Windows 2000 et versions ultérieures), la signature SMB est définie à l'aide d'une stratégie d'objet de stratégie de groupe (GPO). Pour Windows XP, les services de GPO pour la signature SMB ne sont pas disponibles. Vous devez utiliser les paramètres du Registre Windows.

Remarque

La configuration de la signature SMB via GPO a une incidence sur tous les clients et les serveurs au sein du domaine et remplace les paramètres individuels du Registre. Consultez la documentation de sécurité Microsoft pour plus d'informations sur l'activation et la configuration de la signature SMB.

Dans SMB1, l'activation de la signature réduit considérablement les performances, en particulier lors de l'accès sur un réseau WAN. La dégradation des performances avec la signature SMB2 et SMB3 est limitée par rapport à SMB1. L'impact sur les performances de la signature sera supérieur lors de l'utilisation de réseaux plus rapides.

NOTE

Si l'ancien protocole SMB1 n'a pas besoin d'être pris en charge dans votre environnement, il peut être désactivé à l'aide de la commande de maintenance `svc_nas`. Pour plus d'informations sur cette commande de maintenance, consultez le document *Notes techniques sur les commandes de maintenance*.

Configurer la signature SMB avec des GPO

Le Tableau 13 à la page 61 explique les objets de stratégie de groupe (GPO) disponibles pour la signature SMB1.

Remarque

Pour SMB2 et SMB3, chaque version possède un GPO pour chaque côté (côté serveur et côté client) permettant d'activer l'option des communications signées numériquement (toujours). Ni le côté serveur, ni le côté client ne disposent d'un GPO pour activer l'option des communications signées numériquement (si le client l'accepte).

Tableau 13 SMB1 signant les GPO

Nom du GPO	Ce qu'il contrôle	Paramètre par défaut
Serveur du réseau Microsoft : Communications signées numériquement (toujours)	Indique si le composant SMB côté serveur requiert la signature	Désactivé
Serveur du réseau Microsoft : Communications signées numériquement (si le client accepte)	Si le composant SMB côté serveur a la signature activée	Désactivé
Client du réseau Microsoft : Communications signées numériquement (toujours)	Indique si le composant SMB côté client requiert la signature	Désactivé
Client du réseau Microsoft : Communications signées numériquement (si le serveur accepte)	Si la signature est activée sur le composant SMB côté client	Activé

Vous pouvez également configurer la signature SMB via le Registre Windows. Si le service GPO n'est pas disponible, comme dans un environnement Windows NT, les paramètres du Registre sont utilisés.

Configurer la signature SMB avec le Registre Windows

Les paramètres du Registre affectent uniquement le serveur ou le client individuel que vous configurez. Les paramètres du Registre sont configurés sur les stations de travail et les serveurs Windows, et ont une incidence sur les stations de travail et serveurs individuels Windows.

Remarque

Les paramètres du Registre suivants concernent Windows NT avec Service Pack 4 ou version ultérieure. Ces entrées de Registre existent dans Windows Server, mais elles doivent être définies via les GPO.

Les paramètres côté serveur se trouvent à l'emplacement : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\`

Remarque

Pour SMB2 et SMB3, chaque version possède une clé de Registre pour chaque côté (côté serveur et côté client) permettant d'activer l'option requiresecuritysignature. Ni le côté serveur, ni le côté client possède une clé de Registre pour activer l'option enablesecuritysignature.

Tableau 14 SMB1 côté serveur signant les entrées de Registre

Entrées de registre	Valeurs	Objectif
`enablesecuritysignature`	• 0 désactivé (par défaut) • 1 activé	Détermine si la signature SMB est activée.
`requiresecuritysignature`	• 0 désactivé (par défaut) • 1 activé	Détermine si la signature SMB est obligatoire.

Les paramètres côté client se trouvent dans : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanworkstation\parameters\`

Tableau 15 SMB1 côté client signant les entrées de Registre

Entrées de registre	Valeurs	Objectif
`enablesecuritysignature`	• 0 désactivé • 1 activé (par défaut)	Détermine si la signature SMB est activée.
`requiresecuritysignature`	• 0 désactivé (par défaut) • 1 activé	Détermine si la signature SMB est obligatoire.

Réflexion de paquets IP

La réflexion de paquets IP fournit à votre réseau un niveau de sécurité supplémentaire. Étant donné que la majorité du trafic réseau sur un serveur NAS (y compris toutes les E/S de système de fichiers) est initiée par le client, le serveur NAS utilise la réflexion de paquets pour répondre aux demandes du client. Grâce à cette fonction, il n'y a pas besoin de déterminer la route d'acheminement pour envoyer les paquets de réponses. Comme les paquets de réponses sortent toujours par la même interface que les paquets de demandes, ceux-ci ne peuvent pas être utilisés pour alimenter indirectement d'autres réseaux locaux. S'il existe deux périphériques réseau, l'un connecté à Internet et l'autre connecté à l'Intranet, les réponses aux demandes Internet n'apparaissent pas sur l'Intranet. En outre, les réseaux internes utilisés par le système de stockage ne sont pas affectés par les paquets provenant de réseaux externes.

La réflexion des paquets IP peut être activée pour chaque serveur NAS. Elle est désactivée par défaut pour tous les serveurs NAS.

Multitenancy des IP

Le multitenancy IP offre la possibilité d'attribuer des partitions de stockage isolées en mode fichier aux serveurs NAS sur un processeur de stockage. Les tenants permettent la gestion économique des ressources disponibles, tout en garantissant que la visibilité et la gestion de ce tenant sont uniquement limitées à des ressources attribuées.

Remarque

S'il s'agit de la première création d'un tenant dans votre environnement, le système doit générer automatiquement une valeur UUID (Universal Unique Identifier) pour ce tenant. Pour les tenants existants de votre environnement dont la valeur UUID est générée par le système, entrez la valeur UUID manuellement.

Avec le multitenancy IP, chaque tenant peut avoir ses propres :

- Adresses IP et numéros de port.
- Domaine de réseau VLAN.
- Table de routage.
- Pare-feu IP.
- Un serveur DNS ou d'autres serveurs d'administration pour permettre au tenant de disposer de sa propre validation et authentification de sécurité.

Le multitenancy IP s'implémente en ajoutant un tenant au système de stockage, en associant un ensemble de réseaux VLAN au tenant, puis en créant un serveur NAS pour chacun des réseaux VLAN du tenant, si besoin. Il est recommandé de créer un pool séparé pour le tenant et d'associer ce pool à tous les serveurs NAS du tenant.

Remarque

Un pool désigne un ensemble de disques fournissant des caractéristiques de stockage spécifiques pour les ressources qui les utilisent.

Notez les points relatifs à la fonctionnalité multitenancy IP suivants :

- Il existe une relation un-à-plusieurs entre les tenants et les serveurs NAS. Un tenant peut être associé à plusieurs serveurs NAS, mais un serveur NAS ne peut être associé qu'à un seul tenant.
- Vous pouvez associer un serveur NAS à un tenant lors de la création du serveur NAS. Une fois que vous créez un serveur NAS associé à un tenant, vous ne pouvez pas en modifier les propriétés.
- Lors de la réplication, les données d'un tenant sont transférées sur le réseau du fournisseur de services plutôt que sur le réseau du tenant.
- Étant donné que plusieurs tenants peuvent partager le même système de stockage, un pic de trafic d'un tenant peut affecter négativement le temps de réponse des autres tenants.

À propos des VLAN

Les VLAN sont des réseaux logiques qui fonctionnent indépendamment d'une configuration réseau physique. Par exemple, les VLAN permettent de placer tous les ordinateurs d'un service sur le même sous-réseau logique, ce qui peut renforcer la sécurité et réduire le trafic de diffusion du réseau.

Lorsque plusieurs interfaces logiques sont affectées à une carte réseau unique, il est possible d'attribuer un VLAN différent à chaque interface. Lorsque chaque interface possède un VLAN différent, un paquet n'est accepté que si son adresse IP de destination est identique à l'adresse IP de l'interface et si sa balise VLAN est identique à l'ID de VLAN (ID VLAN) de l'interface. Si l'ID VLAN d'une interface est réglé sur 0, les paquets sont envoyés sans balises de VLAN.

Il existe deux manières de travailler avec les VLAN :

- Configurez un port de switch avec un ID VLAN, puis connectez le port du serveur NAS ou une interface iSCSI à ce port de switch. Le système Unity ignore qu'il fait partie du VLAN, et aucune configuration spéciale du serveur NAS ou de l'interface iSCSI n'est nécessaire. Dans ce cas, l'ID VLAN est réglé sur 0.
- Mettre en œuvre la multitenancy IP à l'aide de VLAN. Dans ce scénario, chaque tenant est associé à un ensemble d'un ou de plusieurs VLAN, et le serveur NAS est chargé d'interpréter les balises VLAN et de traiter les paquets de manière appropriée. Ceci permet au serveur NAS de se connecter à plusieurs VLAN et à leurs sous-réseaux correspondants via une connexion physique unique. Avec cette méthode, les ports du switch pour les serveurs sont configurés pour inclure des balises VLAN sur les paquets envoyés au serveur.

Prise en charge de la gestion pour FIPS 140-2

La norme FIPS 140-2 (Federal Information Processing Standard 140-2) décrit les exigences formulées par le gouvernement fédéral américain auxquelles les produits IT doivent satisfaire pour un usage sensible mais non classifié (SBU). Ladite norme définit les exigences de sécurité devant être satisfaites par un module cryptographique utilisé dans un système de sécurité qui protège les informations non classifiées au sein de systèmes IT. Pour plus d'informations sur la norme FIPS 140-2, consultez la publication correspondante.

Le système de stockage prend en charge le mode FIPS 140-2 pour les modules SSL qui gèrent le trafic de gestion des clients. Les communications de gestion arrivant et sortant du système sont codées via SSL. Dans le cadre de ce processus, le client et le logiciel de gestion du stockage négocient une suite de chiffrement à utiliser dans l'échange. L'activation du mode FIPS 140-2 restreint l'ensemble négociable des suites de chiffrement à celles qui sont répertoriées dans la publication des fonctions de sécurité approuvées FIPS 140-2. Si le mode FIPS 140-2 est activé, certains de vos clients existants risquent de ne plus pouvoir communiquer avec les ports de gestion du système s'ils ne prennent pas en charge les suites de chiffrement approuvées FIPS 140-2. Le mode FIPS 140-2 ne peut pas être activé sur un système de stockage si des certificats non conformes à la norme FIPS sont présents dans le magasin de certificats. Avant d'activer le mode FIPS 140-2, vous devez supprimer du système de stockage tous les certificats non conformes à la norme FIPS.

Gestion du mode FIPS 140-2 sur le système de stockage

Seul l'administrateur ou l'administrateur de la sécurité dispose des privilèges nécessaires pour gérer la configuration du mode FIPS 140-2. Utilisez la commande CLI suivante pour définir la configuration du mode FIPS 140-2 sur un système de stockage :

`uemcli /sys/security set -fips140Enabled yes` active le mode FIPS 140-2.

`uemcli /sys/security set -fips140Enabled no` désactive le mode FIPS 140-2.

Utilisez la commande CLI suivante pour déterminer le mode FIPS 140-2 actif pour le système de stockage :

```
uemcli /sys/security show
```

Lorsque vous modifiez la configuration du mode FIPS 140-2 sur un système de stockage, les deux SP sont automatiquement redémarrés dans l'ordre afin d'appliquer la nouvelle configuration. Lorsque le premier SP a terminé de redémarrer, l'autre SP redémarre. Le système ne fonctionnera réellement dans le mode FIPS 140-2 configuré qu'à la fin du redémarrage des deux SP.

Prise en charge de la gestion des communications SSL

Les communications de gestion internes et externes au système de stockage sont chiffrées à l'aide du protocole SSL. Dans le cadre de ce processus, le client et le système de stockage négocient l'utilisation d'un protocole SSL. Par défaut, le système de stockage prend en charge les protocoles TLS 1.0, TLS 1.1 et TLS 1.2 pour les communications SSL. Le système de stockage comprend un paramètre d'administration permettant de désactiver le protocole TLS 1.0 à partir du système. La désactivation du protocole TLS 1.0 à l'aide de ce paramètre signifie que le système de stockage prend uniquement en charge les communications SSL via les protocoles TLS 1.1 et TLS 1.2. TLS 1.0 n'est pas considéré comme un protocole valide.

Remarque

La désactivation du protocole TLS 1.0 peut avoir un impact sur les applications clientes existantes qui ne sont pas compatibles avec les protocoles TLS 1.1 ou TLS 1.2. Dans ce cas, le protocole TLS 1.0 doit rester activé. Les fonctionnalités suivantes ne sont pas actives si le protocole TLS 1.0 est désactivé :

- Conseils techniques
- Notifications de mise à jour liées au logiciel, micrologiciel du disque et pack de langues
- Réplication à partir des versions OE antérieures à 4.3 vers les versions OE 4.3

Gestion du protocole TLS 1.0 sur le système de stockage

Seul l'administrateur ou l'administrateur de la sécurité dispose des privilèges nécessaires pour gérer le protocole TLS 1.0. Utilisez la commande suivante pour définir le paramètre d'activation TLS 1.0 sur un système de stockage :

`uemcli /sys/security set -tls1Enabled yes` permet d'utiliser le protocole TLS 1.0.

`emcli /sys/security set -tls1Enabled no` ne permet pas d'utiliser le protocole TLS 1.0.

Pour plus d'informations sur cette commande, consultez le *Guide d'utilisation de l'interface de ligne de commande Unisphere*.

Prise en charge de la gestion en mode shell restreint (rbash)

L'interface de maintenance SSH du système de stockage est consolidée avec le mode shell (rbash) restreint. Cette fonctionnalité est activée par défaut pour le compte de maintenance lors de la mise à niveau vers Unity OE version 4.5 ou ultérieure. Bien qu'il soit possible de désactiver temporairement le mode shell restreint, il n'est pas persistant et il est réactivé automatiquement lorsque l'une des conditions suivantes est remplie :

- Le processeur de service principal est redémarré.
- 24 heures sont passées depuis la désactivation du mode shell restreint.

Cette fonctionnalité améliore la posture de sécurité du système de stockage Unity en limitant l'accès des utilisateurs du compte de maintenance de la façon suivante :

- Ils ne peuvent utiliser qu'un ensemble limité de commandes attribuées à un membre doté d'un compte utilisateur Linux non privilégié en mode shell restreint. Ils ne peuvent pas accéder au fichiers système propriétaires, aux fichiers de configuration ou aux données utilisateur ou client.
- Ils ne peuvent pas exécuter du code non fiable qui peut être éventuellement utilisé pour exploiter les vulnérabilités des réaffectations de privilèges au niveau local.

Outre les scripts de maintenance, une liste blanche contient les commandes de base disponibles pour le personnel de maintenance. Il s'agit des commandes sécurisées ou des commandes avec contrôle de sécurité à partir desquelles les utilisateurs ne peuvent pas éviter au mode de shell restreint. Ces commandes sont essentielles pour que le personnel de maintenance Dell EMC soit en mesure de fournir un service de maintenance sans élever le privilège jusqu'à la racine. Pour plus d'informations sur ces commandes, reportez-vous à l'article 528422 de la base de connaissances.

NOTE

Une analyse de vulnérabilité réseau ne peut pas être effectuée avec le mode shell restreint par défaut. Les utilisateurs administrateurs de Unisphere doivent désactiver le mode shell restreint afin de faciliter une analyse de sécurité. Pour une sécurité maximale du système, il est vivement recommandé de laisser le mode shell restreint activé de manière permanente, à moins qu'il ne soit nécessaire d'effectuer une analyse de sécurité. Pour que le système ne soit pas exposé aux vulnérabilités des réaffectations de privilèges au niveau local, activez le mode shell restreint dès que l'analyse de sécurité est terminée.

Gestion du mode de shell restreint sur le système de stockage

Seul l'administrateur dispose des privilèges nécessaires pour gérer la configuration du mode de shell restreint. Utilisez la commande CLI suivante pour définir la configuration du mode de shell restreint sur un système de stockage :

`uemcli /sys/security set -rbashEnabled yes` active le mode shell restreint pour le mode d'utilisateur de maintenance.

`uemcli /sys/security set -rbashEnabled no` désactive le mode de shell restreint.

Utilisez la commande CLI suivante pour déterminer le mode de shell restreint actuel pour le système de stockage :

```
uemcli /sys/security show
```

CHAPITRE 5

Paramètres de sécurité des données

Ce chapitre décrit les fonctions de sécurité disponibles sur le système de stockage pour les types de stockages pris en charge.

Les thèmes abordés sont les suivants :

À propos de Data at Rest Encryption (déploiements physiques uniquement)

Data at Rest Encryption (D@RE) est fourni via le chiffrement basé sur le contrôleur (CBE) au niveau du disque physique. L'objectif de cette fonction est de s'assurer que toutes les données et les informations d'identification des clients seront protégées par un chiffrement fort, principalement pour garantir la sécurité en cas de perte d'un disque.

Une clé de chiffrement de données (DEK) unique est générée pour chaque disque et permet de chiffrer les données lorsque celles-ci sont envoyées vers le disque. La clé DEK est utilisée pour chiffrer et déchiffrer les données utilisateur à l'aide d'un algorithme de chiffrement AES (Advanced Encryption Standard) de 256 bits avec le mode d'opération XTS (XOR Encrypt XOR Tweakable Block Cipher with Ciphertext Stealing).

La clé de chiffrement KEK (Key Encryption Key), générée de manière aléatoire et créee par RSA BSAFE, est de 256 bits. Elle est utilisée pour encapsuler les clés DEK au moment de la génération de clé DEK afin que les clés DEK soient protégées et sécurisées lorsqu'elles transitent vers le système de stockage. L'algorithme utilisé pour encapsuler et désencapsuler les clés DEK à l'aide de la clé KEK est AES Key Wrap 256 bits, tel que spécifié dans le RFC 3394.

La clé KWK (Key Encryption Key Wrapping Key) est une clé générée de manière aléatoire de 256 bits, créée par RSA BSAFE et utilisée pour encapsuler la clé KEK au moment de la génération, de sorte que la clé KEK est protégée lorsqu'elle transite dans la baie et vers le contrôleur SAS (Serial Attached SCSI). L'algorithme utilisé pour encapsuler et désencapsuler les clés KEK à l'aide de la clé KWK est AES Key Wrap 256 bits, tel que spécifié dans le RFC 3394.

Distinct du chiffrement basé sur le contrôleur, l'espace système sur les processeurs de stockage (SP) est chiffré à l'aide d'une fonction de chiffrement (dm_crypt) qui est native de la distribution Linux. Les partitions spécifiques sur le disque système sont chiffrées par défaut, sauf si le chiffrement n'est pas activé sur le système au moment de la fabrication. Pour ces partitions système qui ne sont pas chiffrées, certaines données non chiffrées, telles que les vidages de diagnostics, peuvent être présentes. En outre, il se peut qu'il y ait de petites quantités de données utilisateur non chiffrées en raison de l'écriture des supports de diagnostic sur la partition système. Toutes les données écrites sur la baie à l'aide des protocoles d'E/S standard (iSCSI, FC) sont chiffrées. Tout ce qui est fourni dans la baie au moyen du chemin de contrôle n'est pas chiffré par cette solution ; toutefois, les informations sensibles (par exemple, les mots de passe) sont chiffrées par un autre mécanisme (comme si elles figuraient sur des baies sans chiffrement).

Un nouveau composant, appelé Key Manager, est chargé de générer, de stocker et de gérer les clés de chiffrement pour le système. Le magasin de clés, qui est généré pour stocker les clés de chiffrement, réside sur une LUN gérée dans un espace privé du système. Les clés sont générées ou supprimées suite aux notifications d'ajout ou de suppression d'un pool de stockage. Les sauvegardes de clés sont effectuées automatiquement par le système. En outre, les modifications apportées à la configuration du système, qui entraînent des modifications apportées au magasin de clés, génèrent des alertes d'information qui recommandent la création de sauvegardes de clés. Lorsqu'une opération entraînant une modification du magasin de certificats se produit, une alerte s'affiche en permanence.

Une fonction d'audit distincte est fournie pour les opérations de clés générales qui permettent de suivre l'établissement, la suppression, la sauvegarde et les modifications de restauration de toutes les clés, ainsi que l'ajout SLIC.

Pour obtenir des informations complémentaires sur la fonctionnalité Data at Rest Encryption, consultez *Unity : Livre blanc Data-at-Rest Encryption*.

Activation de la fonction

D@RE est une fonctionnalité sous licence La licence doit être installée lors de la configuration initiale de votre système. une fois activée, l'opération de chiffrement ne peut pas être annulée.

L'opération de chiffrement entraîne la création de clés de chiffrement des données. Le chiffrement de toutes les données utilisateur commence alors. Les clés de chiffrement sont stockées dans un fichier de magasin de clés. Le fichier de magasin de clés qui est généré, réside sur une LUN gérée dans un espace privé du système.

Il est vivement recommandé de sauvegarder le fichier de magasin de clés généré à un autre emplacement qui est externe au système et où le magasin de clés peut être conservé en toute sécurité et secrètement. Si le magasin de certificats du système est corrompu, le système ne fonctionnera pas. Le système passe en mode maintenance. Seul le système d'exploitation est initialisé. Ainsi les tentatives d'accès au système via Unisphere renverront une erreur indiquant que le magasin de clés est à l'état inaccessible. Dans ce cas, le fichier de magasin de clés de sauvegarde et un engagement de service sont requis pour la résolution.

État du chiffrement

L'état suivant de la fonction D@RE peut être affiché via Unisphere ou une commande CLI :

- Mode de chiffrement : type de chiffrement en cours d'utilisation, par exemple le chiffrement basé sur le contrôleur.
- État de chiffrement : basé sur l'état de chiffrement réel :
  - Non pris en charge, le chiffrement de l'espace système sur les processeurs de stockage est désactivé.
  - Sans licence, la licence Data at Rest Encryption pas été installée sur le système.
  - Chiffré, le chiffrement est terminé.
  - Pas de chiffrement, le chiffrement basé sur le contrôleur (CBE) est désactivé.
  - Nettoyage : processus d'écriture de données aléatoires dans l'espace inutilisé des disques ou remise à zéro des disques non liés pour effacer les données résiduelles de l'utilisation précédente.

    Remarque

    Pour les disques Flash SAS 2, la suppression du mappage est utilisée pour nettoyer les disques plutôt que la remise à zéro. Pour obtenir des informations complémentaires sur la fonctionnalité Data at Rest Encryption, consultez *EMC Unity : Livre blanc Data at Rest Encryption* disponible sur le Support en ligne (https://support.emc.com).
  - Chiffrement, le chiffrement est en cours d'exécution.
- État KMIP, si KMIP est activé ou désactivé.

Pour afficher l'état de la fonction D@RE dans Unisphere, sélectionnez**Paramètres** > **Gestion** > **Chiffrement**. L'état du chiffrement s'affiche sous **Gérer le chiffrement**.

Remarque

Vous pouvez également utiliser la commande CLI `uemcli -u <username> -p <password> /prot/encrypt show -detail` pour consulter l'état des fonctions (Mode de chiffrement, État du chiffrement, Pourcentage chiffré, État de sauvegarde du magasin de clés et État KMIP). Vous pouvez également utiliser cette commande CLI pour afficher l'état du magasin de clés et pour déterminer si des interventions de l'utilisateur sont nécessaires. Reportez-vous au *Guide d'utilisation de l'interface de ligne de commande Unisphere* pour plus d'informations sur ces commandes CLI.

Gestion de clés externe

La prise en charge de la gestion de clés externe est assurée par l'utilisation du protocole KMIP (Key Management Interoperability Protocol). KMIP définit la façon dont un client fonctionne avec un gestionnaire de clés externe.

Remarque

La gestion de clés externe n'est prise en charge qu'avec les serveurs de gestion des clés qui ont implémenté le protocole KMIP développé par OASIS. Si un serveur KMIP KeySecure Gemalto est utilisé, le gestionnaire des clés sur le système de stockage requiert un nom d'utilisateur et un mot de passe pour être configuré sur le serveur.

L'activation et la configuration de la prise en charge de KMIP sur le système de stockage dépend du chiffrement activé sur le système de stockage. Lorsque le chiffrement est activé et KMIP est activé, la clé de démarrage est migrée à partir du système de stockage vers un gestionnaire de clés externe et la copie locale est supprimée. En outre, l'ancien emplacement des clés stockées localement est reprogrammé et ne peut pas être ouvert une fois que les clés ont migré. Il est recommandé de générer une nouvelle sauvegarde de fichier du magasin de certificats.

Un rôle d'utilisateur d'administrateur ou d'administrateur de sécurité est nécessaire pour configurer la gestion de clés externe. Pour configurer la gestion de clés externe, sélectionnez **Paramètres** > **Gestion** > **Chiffrement** et, sous **Gestion du chiffrement** > **Gestion des clés externe**, sélectionnez **Configurer**. Fournissez les informations requises dans la boîte de dialogue qui s'affiche pour configurer les propriétés du serveur de gestion de clés et pour ajouter le serveur KMIP au cluster de serveurs KMIP. La boîte de dialogue permet également d'importer et de gérer les certificats adéquats de l'autorité de certification (AC) et du client, et de vérifier la configuration. La configuration requiert deux certificats :

- Le certificat AC au format PEM
- Un fichier PKCS #12 protégé par mot de passe et contenant le certificat client

Une copie de la configuration du serveur KMIP, comprenant les données de configuration du serveur et les certificats, est stockée en local dans des emplacements sécurisés du système de stockage, ainsi que sur les disques back-end du système pour assurer la redondance.

Remarque

Reportez-vous à la Matrice de support simplifiée pour le système de stockage sur le site Web de support pour obtenir des informations sur la compatibilité et l'interopérabilité liées aux serveurs KMIP.

Les certificats sont téléchargés sur le processeur de stockage actif. Au moment du démarrage, chaque fois qu'un problème de certificat est signalé, le système rétablit les

certificats à partir de sa copie locale du lockbox et effectue une nouvelle tentative. Si le test échoue à nouveau, le système passe en mode maintenance. Si une différence est trouvée, le contenu du lockbox sur le back-end est mis à jour.

Remarque

Sinon, utilisez la commande de l'interface de ligne de commande (CLI) `uemcli -u<username> -p<password> /prot/encrypt/kmip -set -username <value> {-passwd <value> | -passwdSecure} -port <value> [-timeout <value>] -server <value>` pour configurer KMIP. Utilisez la commande CLI `uemcli -u<username> -p<password> /sys/cert [ -type { CA | Server | Client | TrustedPeer } ] [ -service {Mgmt_LDAP | Mgmt_KMIP | VASA_HTTP } [ -scope <value> ] ] [ -id <value> ]` pour importer des certificats de l'autorité de certification et du client. Utilisez la commande CLI `uemcli -u<username> -p<password> /prot/encrypt/kmip -verify` pour vérifier la configuration. Reportez-vous au *Guide d'utilisation de l'interface de ligne de commande Unisphere* pour plus d'informations sur ces commandes CLI.

S'il existe un problème ou qu'une modification inattendue de la configuration ou de l'état du protocole KMIP se produit, le système ne peut pas confirmer que la configuration ou l'état est correct et démarre en mode maintenance. Le système ne peut pas revenir en mode normal avant la résolution du problème. Le script de maintenance `svc_kmip` peut servir à restaurer la configuration correcte du serveur KMIP et, si nécessaire, les certificats Unity afin que le système puisse revenir en mode normal.

NOTE

Le script de maintenance `svc_kmip` est utilisé uniquement pour la restauration et ne peut pas être utilisé pour définir la configuration KMIP et l'activer sur un nouveau système. Pour plus d'informations sur ce script de maintenance, consultez les *Notes techniques sur les commandes de maintenance*.

Sauvegarder le fichier de magasin de clés

Les modifications apportées à la configuration du système qui modifient le magasin de clés génèrent des alertes d'information persistantes qui recommandent de créer des sauvegardes des clés. Une nouvelle alerte est générée uniquement après la récupération du magasin de clés à partir du système pour la sauvegarde.

Remarque

Il est vivement recommandé de sauvegarder le fichier de magasin de clés généré à un autre emplacement qui est externe au système et où le magasin de clés peut être conservé en toute sécurité et secrètement. Si les fichiers du magasin de clés résidant sur le système deviennent corrompus et inaccessibles, le système passe en mode maintenance. Dans ce cas, le fichier de magasin de clés de sauvegarde et un engagement de service sont requis pour la résolution.

Un rôle utilisateur d'administrateur ou d'administrateur de sécurité est nécessaire pour sauvegarder le fichier de magasin de clés. Pour sauvegarder le fichier de magasin de clés qui est à un emplacement externe au système où le magasin de clés peut être conservé en toute sécurité et secrètement, sélectionnez**Paramètres** > **Gestion** > **Chiffrement** et, sous**Gérer le chiffrement** > **Magasin de clés**,

sélectionnez**Sauvegarder le fichier du magasin de clés**. La boîte de dialogue qui s'affiche vous dirige dans la procédure de sauvegarde du fichier de magasin de clés généré.

Remarque

Vous pouvez aussi utiliser la commande CLI `uemcli -u<username> -p<password> -download encryption -type backupKeys` pour sauvegarder le fichier de magasin de clés à un emplacement externe au système où le magasin de clés peut être conservé en toute sécurité et secrètement. Reportez-vous au *Guide d'utilisation de l'interface de ligne de commande Unisphere* pour plus d'informations sur cette commande CLI.

Consignation de l'audit Data at Rest Encryption

La fonction D@RE fournit une fonction d'audit distincte qui prend en charge la consignation des opérations du magasin de clés suivantes :

- Activation de la fonction
- Création de clés
- Destruction de clés
- Sauvegarde du magasin de clés
- Chiffrement du disque terminé
- Ajout de SLIC

Le log d'audit pour les opérations de magasin de clés est stocké dans l'espace privé sur le système. Pour télécharger le log d'audit complet et les informations de checksum ou les informations d'une année ou d'un mois spécifique, sélectionnez**Paramètres** > **Gestion** > **Chiffrement** et, sous **Gérer le chiffrement** > **Log d'audit**, sélectionnez**Télécharger l'Audit log et le fichier checksum**. Pour télécharger un fichier checksum nouvellement généré pour le fichier log d'audit qui a été extrait précédemment, sélectionnez **Paramètres** > **Gestion** > **Chiffrement** et, sous **Gérer le chiffrement** > **Audit Log**, sélectionnez**Télécharger Chksum**. Le nom de fichier que vous indiquez doit correspondre exactement au fichier auditlog qui a été récupéré précédemment.

Remarque

Vous pouvez aussi utiliser la commande CLI `uemcli -u<username> -p<password> -download encryption -type auditLog -entries <all or YYYY-MM>` pour télécharger le log d'audit complet et les informations de checksum, ou bien un log d'audit partiel, respectivement. Reportez-vous au *Guide d'utilisation de l'interface de ligne de commande Unisphere* pour plus d'informations sur cette commande CLI.

Opérations de remplacement à chaud

Lorsqu'un système est déjà configuré avec des clés DEK pour tous les disques du système qui appartiennent à des pools provisionnés, les disques qui ne figurent pas actuellement dans un pool provisionné sont considérés comme des disques non liés. Le retrait des disques non liés ou des disques non liés devenus défectueux n'affecte pas le magasin de clés et ne nécessite donc pas de fichier de sauvegarde ou de fichier de clés. De même, le remplacement d'un disque non lié n'affecte pas le magasin de clés et ne nécessite donc pas de fichier de sauvegarde ou de fichier de clés.

Remarque

Les disques non liés sont remplacés par les données par défaut pour supprimer les données préexistantes.

Lorsqu'un système est déjà configuré avec des clés DEK pour tous les disques du système qui appartiennent à des pools provisionnés, ces disques sont considérés comme des disques non liés. Si un disque lié est retiré ou qu'il est défaillant et qu'un disque de secours remplace en permanence le disque retiré ou défectueux au bout de cinq minutes, une clé DEK est générée pour le disque de secours et la reconstruction commence. La clé DEK provenant du disque retiré est supprimée immédiatement du magasin de clés. L'état de modification du magasin de clés est défini par le gestionnaire de clés à ce stade et déclenche une alerte pour sauvegarder le magasin de clés, car des clés DEK ont été modifiées dans ce dernier.

Si le disque retiré est réintroduit n'importe où dans le système avant l'expiration de la période de cinq minutes, une reconstruction n'est pas nécessaire et aucune modification n'est effectuée dans le magasin de clés. La clé DEK reste la même, car elle n'est pas associée au slot mais au disque. En outre, aucune alerte d'état de modification du magasin de clés n'est générée.

Remarque

Si le nettoyage ou la destruction du disque retiré est nécessaire, l'opération doit être effectuée indépendamment.

Ajout d'un disque à un système de stockage avec chiffrement activé

Le fait d'insérer un ou plusieurs nouveaux disques dans le système ne déclenche pas la génération d'une nouvelle clé DEK pour chaque disque. Cette opération ne se produira pas pour un nouveau disque tant que le disque est provisionné dans un pool. L'état de modification du magasin de clés est défini par le gestionnaire de clés à ce stade et déclenche une alerte pour sauvegarder le magasin de clés, car des clés DEK ont été modifiées dans ce dernier.

Lorsque vous ajoutez un nouveau disque à un système de stockage, ce disque est considéré comme non lié. Les disques non liés sont remplacés par les données par défaut pour supprimer les données préexistantes. Seul l'espace adressable du disque est remplacé. Toutes les données en texte clair résiduelles qui peuvent être masquées dans des emplacements illisibles du disque ne sont pas remplacées.

NOTE

Si l'accès potentiel aux données qui restent de l'utilisation précédente d'un disque est incompatible avec votre règle de sécurité, vous devez nettoyer indépendamment ce disque avant de l'insérer dans le système de stockage avec le chiffrement activé.

Suppression d'un disque à partir d'un système de stockage avec chiffrement activé

Lorsqu'un système est déjà configuré avec des clés DEK pour tous les disques du système qui appartiennent à des pools provisionnés, ces disques sont considérés comme des disques non liés. Si un disque lié est retiré et n'est pas remplacé au bout de cinq minutes, la clé DEK de ce disque n'est pas supprimée du magasin de clés. La clé reste valide jusqu'à ce que le pool provisionné soit supprimé ou qu'un nouveau disque soit inséré. Si le disque retiré est réintroduit n'importe où dans le système avant l'expiration de la période de cinq minutes, une reconstruction n'est pas nécessaire,

comme dans le cas d'un disque de remplacement, et aucune modification n'est effectuée dans le magasin de clés. La clé DEK reste la même, car elle n'est pas associée au slot mais au disque. En outre, aucune alerte d'état de modification du magasin de clés n'est générée.

Remarque

Si le nettoyage ou la destruction du disque retiré est nécessaire, l'opération doit être effectuée indépendamment.

Remplacement d'un châssis et des processeurs de stockage dans un système de stockage avec chiffrement activé

Le magasin de clés généré est lié au matériel du système de stockage. Un engagement de service est nécessaire pour remplacer un châssis et des processeurs de stockage à partir d'un système de stockage avec chiffrement activé.

Paramètres de sécurité des données

Le Tableau 16 à la page 74 présente les fonctions de sécurité disponibles pour les types de stockages des systèmes de stockage pris en charge.

Tableau 16 Fonctions de sécurité

Type de stockage	Port	Protocole	Paramètres de sécurité
Stockage iSCSI	3260	TCP	• Un contrôle d'accès au niveau de l'hôte iSCSI (initiateur) est disponible via Unisphere (et permet aux clients d'accéder au stockage principal, aux snapshots ou aux deux). • L'authentification CHAP est prise en charge de sorte que les serveurs iSCSI (cibles) du système de stockage puissent authentifier les hôtes iSCSI (initiateurs) qui tentent d'accéder au stockage iSCSI. • L'authentification CHAP mutuelle est également prise en charge pour que les hôtes iSCSI (initiateurs) puissent authentifier les serveurs iSCSI du système de stockage.
Stockage SMB	445	TCP, UDP	• L'authentification pour les actions de domaine et d'administration est assurée via les comptes d'utilisateur et de groupe Active Directory. • Les contrôles d'accès aux fichiers et aux partages sont assurés par l'intermédiaire des services d'annuaire Windows. La liste de contrôle d'accès (ACL) aux partages SMB peut également être configurée via une interface SMI-S. • Les signatures de sécurité sont prises en charge au moyen de la fonction de signature SMB. • Le chiffrement SMB est assuré via SMB 3.0 et Windows 2012 pour les hôtes compatibles SMB.

Tableau 16 Fonctions de sécurité (suite)

Type de stockage	Port	Protocole	Paramètres de sécurité
			• La prise en charge des services de rétention au niveau des fichiers (en option) est assurée via un module complémentaire.
Stockage NFS	2049	TCP	• Le contrôle d'accès aux partages s'effectue au moyen de Unisphere. • Prise en charge des méthodes de contrôle d'accès et d'authentification NFS identifiées dans NFS versions 3 et 4. • La prise en charge des services de rétention au niveau des fichiers (en option) est assurée via un module complémentaire.
KDC	88		• Key Distribution Center Serveur Kerberos qui fournit des tickets Kerberos pour se connecter aux services Kerberos.
Sauvegarde et restauration			• La sécurité NDMP peut être mise en œuvre sur la base de secrets partagés NDMP.

CHAPITRE 6

Maintenance de sécurité

Ce chapitre décrit diverses fonctions de maintenance de sécurité accès implémentées sur le système de stockage.

Les thèmes abordés sont les suivants :

Maintenance sécurisée

Le système de stockage offre les fonctions de sécurité ci-après pour les tâches de maintenance et de mise à jour à distance :

- Activation des licences
- Mise à niveau des logiciels
- Hot fixes de logiciels

Mise à jour des licences

La fonction de mise à jour des licences permet aux utilisateurs d'obtenir et d'installer des licences pour des fonctions spécifiques du système de stockage. Le Tableau 17 à la page 78 présente les fonctions de sécurité associées à la fonction de mise à jour des licences.

Tableau 17 Fonctions de sécurité associées à la mise à jour des licences

Processus	Sécurité
Obtention de licences via le site Web de support en ligne EMC	L'acquisition de licences s'effectue dans une session authentifiée sur le site Web de support en ligne EMC.
Réception des fichiers de licences	Les licences sont envoyées à l'adresse e-mail spécifiée dans une transaction authentifiée sur le site Web de support en ligne EMC.
Téléchargement et installation de licences sur le système de stockage par l'intermédiaire du client Unisphere	• Les téléchargements de fichiers de licences sur le système de stockage s'effectuent dans les sessions Unisphere authentifiées par HTTPS. • Le système de stockage valide les fichiers de licence reçus au moyen de signatures numériques. Chaque fonction sous licence est validée par une signature unique dans le fichier de licences.

Mise à niveau des logiciels

La fonction de mise à jour logicielle du système de stockage permet aux utilisateurs d'obtenir et d'installer des mises à jour/mises à niveau des logiciels exécutés sur le système de stockage. Le Tableau 18 à la page 78 présente les fonctions de sécurité associées à la fonction de mise à niveau du logiciel du système de stockage.

Tableau 18 Fonctions de sécurité associées à la mise à niveau logicielle

Processus	Description
Téléchargement de logiciels du système de stockage à partir du site Web de support en ligne EMC	L'acquisition de licences s'effectue dans une session authentifiée sur le site Web de support en ligne EMC.

Tableau 18 Fonctions de sécurité associées à la mise à niveau logicielle (suite)

Processus	Description
Téléchargement des logiciels du système de stockage	Le téléchargement des logiciels sur le système de stockage s'exécute dans une session Unisphere authentifiée par HTTPS.

EMC Secure Remote Services pour votre système de stockage

La fonctionnalité EMC Secure Remote Services (ESRS) permet à votre fournisseur de services autorisé d'accéder à distance à votre système de stockage à l'aide d'un tunnel sécurisé et chiffré. Pour l'accès sortant, le réseau IP de gestion du système de stockage doit autoriser le trafic HTTPS sortant et entrant. Le tunnel sécurisé établi par ESRS entre le périphérique du système de stockage et les systèmes autorisés sur le réseau du Centre de support peut également permettre de transférer des fichiers provenant du système de stockage ou de les retransférer vers le réseau du Centre de support.

Deux options de maintenance à distance sont disponibles afin d'envoyer les informations du système de stockage au Centre de support pour le dépannage à distance :

- Services ESRS centralisés Virtual Edition (VE)
- Integrated ESRS (déploiements physiques uniquement)

Centralized EMC Secure Remote Services

Centralized ESRS s'exécute sur un serveur de passerelle. Lorsque vous sélectionnez cette option, votre système de stockage est ajouté aux autres systèmes de stockage dans un cluster ESRS. Le cluster se trouve derrière une seule connexion sécurisée (centralisée) commune entre les serveurs du Centre de support et ESRS Gateway hors baie. ESRS Gateway est le point unique d'entrée et de sortie pour toutes les activités ESRS basées sur IP pour les systèmes de stockage associés à la passerelle.

ESRS Gateway est une application de solution de support à distance qui est installée sur un ou plusieurs serveurs dédiés fournis par le client. ESRS Gateway fonctionne comme un courtier en communication entre les systèmes de stockage associés, les serveurs proxy (facultatifs) et Policy Manager (facultatif), ainsi que le Centre de support. Les connexions à Policy Manager et aux serveurs proxy associés sont configurées via l'interface ESRS Gateway, avec les fonctions d'état d'ajout (inscription), de modification, de suppression (annulation de l'inscription) et d'interrogation que les clients ESRS peuvent utiliser pour s'enregistrer dans ESRS Gateway.

Pour plus d'informations sur ESRS Gateway et Policy Manager, accédez à la page produit EMC Secure Remote Services du Support en ligne EMC (https://support.emc.com).

Integrated EMC Secure Remote Services (déploiements physiques uniquement)

Remarque

La disponibilité de cette fonction dépend de votre mise en œuvre.

Integrated ESRS s'exécute directement sur votre système de stockage. Lorsque vous sélectionnez cette option, votre système de stockage configure une connexion

sécurisée entre lui-même et les serveurs du Centre de support. L'option de service à distance intégré peut être configurée comme étant uniquement sortante ou sortante/entrante, ce qui est la valeur par défaut. La configuration sortante uniquement permet la connectivité du service à distance pour le transfert distant du système de stockage vers le Centre de support. La configuration sortante/entrante permet la connectivité du service à distance pour le transfert à distance et le transfert à distance depuis le Centre de support avec le système de stockage. Lorsque l'option de configuration sortante/entrante est sélectionnée, la connexion du système de stockage à un Policy Manager facultatif et à tous les serveurs proxy associés doit être configurée via Unisphere ou l'interface de ligne de commande.

CHAPITRE 7

Paramètres d'alerte de sécurité

Ce chapitre décrit les différentes méthodes disponibles pour avertir les administrateurs des alertes survenues sur le système de stockage.

Les thèmes abordés sont les suivants :

Paramètres d'alerte

Les alertes du système de stockage signalent aux administrateurs les événements exploitables survenant sur le système de stockage. Les événements du système de stockage peuvent être signalés par différentes méthodes, décrites dans le Tableau 19 à la page 82.

Tableau 19 Paramètres d'alerte

Type d'alerte	Description
Notification visuelle	Affiche des messages contextuels à caractère informatif dans l'interface et en temps réel pour indiquer l'existence de conditions d'alerte. Ces messages fournissent des informations de base sur la condition d'alerte. Vous pouvez obtenir des informations supplémentaires dans **Paramètres** > **Alertes** > **Spécifier les alertes par e-mail et la configuration SMTP**. **Remarque** Les notifications d'alerte visuelles du système de stockage ne sont pas configurables. En outre, le système de stockage ne dispose pas d'une option d'authentification sur un serveur de messagerie SMTP. Si votre serveur de messagerie requiert que tous les clients s'authentifient pour relayer un e-mail, le système de stockage ne peut pas envoyer d'alertes par e-mail via ce serveur de messagerie.
Notification par e-mail	Permet de spécifier une ou plusieurs adresses e-mail auxquelles envoyer les messages d'alerte. Les paramètres suivants peuvent être configurés : • adresses e-mail auxquelles envoyer les alertes du système de stockage ; • Niveau de gravité (critique, erreur, avertissement, avis ou informations) requis pour la notification par e-mail. **Remarque** Pour que la notification d'alerte par e-mail du système de stockage fonctionne, vous devez configurer un serveur SMTP cible pour le système de stockage.
Traps SNMP	Transfère les informations d'alerte aux hôtes désignés (destinations de trap) qui jouent le rôle de référentiels pour les informations d'alerte générées par le système de stockage. Vous pouvez configurer les traps SNMP à l'aide de Unisphere. Les paramètres sont notamment les suivants : • Adresse IP d'une destination de trap SNMP réseau • Paramètres de sécurité facultatifs pour la transmission de données de trap ▪ Protocole d'authentification : algorithme de hachage utilisé pour les traps SNMP (SHA ou MD5) ▪ Protocole de confidentialité : Algorithme de chiffrement utilisé pour les traps SNMP (DES ou AES) ▪ Version : Version utilisée pour les traps SNMP (v2c ou v3) ▪ Communauté : Chaîne de communauté SNMP (applicable uniquement à la destination SNMP v2c) L'aide en ligne de Unisphere fournit des informations complémentaires à ce sujet.
Services à distance sécurisés EMC (ESRS)	ESRS fournit une connexion IP permettant au Support EMC de recevoir les messages d'alerte et les fichiers d'erreur en provenance du système de stockage, et de procéder à un dépannage à distance, garantissant ainsi une résolution rapide et efficace des problèmes.

Tableau 19 Paramètres d'alerte (suite)

Type d'alerte	Description
	Remarque Disponible avec l'EE version 4.0 ou supérieure. Pour que le service ESRS fonctionne, vous devez l'activer sur le système de stockage.

Configuration des paramètres d'alerte

Vous pouvez configurer les paramètres d'alerte utilisés par le système de stockage pour la notification par e-mail et les traps SNMP.

Configuration des paramètres d'alerte pour les notifications par e-mail

Dans Unisphere :

Procédure

1. Sélectionnez **Paramètres** > **Alertes** > **E-mail et SMTP**.
2. Dans la section **Spécifier les alertes par e-mail et la configuration SMTP** sous **Envoyer des alertes par e-mail à la liste d'adresses e-mail suivante**, configurez les adresses e-mail auxquelles envoyer des notifications d'alerte.
3. Sous **Niveau de gravité des alertes à envoyer:**, choisissez l'une des options suivantes pour définir le niveau de gravité auquel un événement doit correspondre pour que des e-mails d'alerte soient générés :
   - Critique
   - Alertes d'erreur et au-dessus
   - Alertes d'avertissement et au-dessus
   - Alertes de notification et au-dessus
   - Alertes d'information et au-dessus

   Remarque

   Pour que le mécanisme d'alerte par e-mail du système de stockage fonctionne, un serveur SMTP cible doit être configuré pour le système de stockage.
4. Sous **Définir les paramètres réseau SMTP:**, configurez le serveur cible SMTP.

Configuration des paramètres d'alerte pour les traps SNMP

Dans Unisphere :

Procédure

1. Sélectionnez **Paramètres** > **Alertes** > **SNMP**.
2. Dans la section **Gérer les alertes SNMP** sous **Envoyer des alertes via des traps SNMP à ces destinations:**, configurez les informations suivantes pour les destinations de trap SNMP :

- Nom du réseau ou adresse IP
- Protocole d'authentification SNMP à utiliser
- Protocole de confidentialité à utiliser
- Version SNMP à utiliser
- Chaîne de communauté (applicable à la destination SNMP v2c uniquement)

3. Sous **Niveau de gravité des alertes à envoyer:**, choisissez l'une des options suivantes pour définir le niveau de gravité auquel un événement doit correspondre pour que des traps SNMP soient générées :
   - Critique
   - Alertes d'erreur et au-dessus
   - Alertes d'avertissement et au-dessus
   - Alertes de notification et au-dessus
   - Alertes d'information et au-dessus

CHAPITRE 8

Autres paramètres de sécurité

Ce chapitre contient des informations supplémentaires permettant de garantir un fonctionnement sécurisé du système de stockage.

Les thèmes abordés sont les suivants :

À propos des exigences STIG

Les exigences STIG (Security Technical Implementation Guide) définissent les normes de configuration et de maintenance dans le cadre des déploiements informatiques requises par le programme IA (Information Assurance) du Département de la Défense des États-Unis. Ces directives sont conçues pour améliorer les paramètres de sécurité et les options de configuration avant que les systèmes ne soient connectés à un réseau. Vous trouverez plus d'informations sur les différentes exigences STIG à l'adresse suivante http://iase.disa.mil/stigs/index.html.

Certaines étapes de renforcement en vue de répondre aux exigences STIG sont activées en exécutant des scripts de maintenance. La commande de maintenance `svc_stig` active ou désactive le mode STIG sur un système Unity (déploiements physiques uniquement) et indique l'état du mode STIG. Cette commande de maintenance fournit un mécanisme simple et automatisé pour appliquer ces modifications. Ces modifications peuvent également être annulées, s'il existe une exigence permettant de le faire à une date ultérieure (par exemple, pour résoudre un problème opérationnel).

Remarque

Alors que les modifications apportées par le mode STIG aux options de configuration et de gestion peuvent être annulées, tous les paramètres associés ne sont pas restaurés à leurs valeurs par défaut. Certains paramètres, tels que les autorisations et les modifications de privilèges apportées aux systèmes de fichiers au niveau de l'environnement d'exploitation, sont conservés.

Le système de stockage conservera le mode STIG de manière permanente grâce à la mise à niveau du logiciel.

Gérer le mode STIG (déploiements physiques uniquement)

Lorsque le mode STIG est activé via la commande de maintenance `svc_stig`, l'état de chaque mode STIG appliqué (catégorie I ou Catégorie II ou les deux) s'affiche. Vous pouvez spécifier les catégories applicables, mais si vous utilisez `svc_stig -e` sans spécifier d'options spécifiques, les modes STIG CAT I et CAT II sont appliqués par défaut. Lorsque la catégorie CAT II est activée, l'interface de service SSH du système de stockage et Unisphere affichent une bannière de connexion DoD pour les sessions interactives.

Pour renforcer votre système de stockage, suivez ces trois étapes dans l'ordre :

1. Activez le mode STIG. Ce processus applique les modifications au SP passif et le redémarre. Une fois le redémarrage complètement terminé, le SP passif devient actif. Les modifications sont ensuite appliquées au précédent SP actif avant de procéder à son redémarrage.
2. Activez le mode FIPS 140-2. Ce processus entraîne le redémarrage des SP. Pour plus d'informations sur le mode FIPS 140-2, reportez-vous à la section Prise en charge de la gestion pour FIPS 140-2 à la page 64.
3. Activez les paramètres du compte utilisateur STIG. Pour plus d'informations sur les paramètres de compte utilisateur STIG, reportez-vous à la section Gérer les paramètres de compte utilisateur en mode STIG (déploiements physiques uniquement) à la page 88.

Pour désactiver le renforcement de votre système de stockage, suivez ces trois étapes dans l'ordre :

1. Désactivez les paramètres du compte utilisateur STIG.
2. Désactivez le mode FIPS 140-2.
3. Désactivez le mode STIG.

Exemples d'utilisation

```
Usage: svc_stig [<qualifiers>] where the qualifiers are:

  -h|--help             : Display this message
  -d|--disable       [options] : Disable STIGs
  -e|--enable        [options] : Enable STIGs
  -s|--status        [options] : Get status for STIGs

This script enables, disables, and provides current status for each
catgory of STIGs.

See the help text below for more information on options.

Refer to the system documentation for a complete description of
STIGs
supported.

-d|--disable:
  Used to Disable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : disable a specific category of STIGs

-e|--enable:
  Used to Enable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : enable a specific category of STIGs

-s|--status:
  Used to show the current status (enabled or disabled) for all
STIGs
  (no option specified).
  Options:

    -c|--cat [X]    : show status for a specific Category of STIGs
    -b|--boolean-format : show boolean status for a specific
Category of STIGs
```

Exemple 1 Activer le mode STIG

```
12:51:21 service@OB-M1204-spb spb:~> svc_stig -e
################################################################################
############
WARNING:
WARNING: This action will cause a reboot of the system!!
WARNING:
################################################################################
############

################################################################################
############
INFO:
INFO: Both Storage Processors will reboot in sequence, starting
with peer SP.
```

Exemple 1 Activer le mode STIG (suite)

```
INFO: When primary SP comes back from reboot, the process will
automatically
INFO: restart to finish applying. Monitor status with 'svc_stig -
s'. If status
INFO: does not change to expected value within 30 minutes, contact
service
INFO: provider.
INFO:
################################################################
###########
Enter "yes" if want to proceed with this action:
```

Exemple 2 Affiche l'état du mode STIG

```
13:25:15 service@OB-M1204-spa spa:~> svc_stig -s
STIG CATEGORY 1: ENABLED
STIG CATEGORY 2: ENABLED
```

Gérer les paramètres de compte utilisateur en mode STIG (déploiements physiques uniquement)

Un utilisateur disposant d'un rôle d'administrateur ou d'administrateur de la sécurité a la possibilité d'activer, de désactiver, d'afficher et de configurer les paramètres associés aux comptes utilisateur. Les paramètres s'appliquent à tous les comptes utilisateur, sauf spécification contraire. Lorsque les paramètres du compte utilisateur sont activés sans spécifier de valeur particulière pour chaque paramètre, la valeur par défaut STIG est automatiquement appliquée. Lorsque les paramètres du compte utilisateur sont désactivés, chaque paramètre retrouve sa valeur initiale avant l'activation de la fonctionnalité. Les fonctionnalités suivantes pour les paramètres de compte utilisateur ne sont applicables qu'aux systèmes sur lesquels le mode STIG est activé :

- Autres exigences en matière de mot de passe
- Exigences inhérentes aux échecs de connexion
- Période de blocage
- Délai d'inactivité de la session
- Activer le blocage administrateur par défaut

Voici un récapitulatif des limites de la fonctionnalité de configuration du compte utilisateur :

- La fonctionnalité est uniquement disponible via les commandes UEMCLI `/user/account/settings set` **et** `/user/account/settings show`.
- Seul un utilisateur doté du rôle d'administrateur ou d'administrateur de la sécurité peut exécuter cette commande.
- Le mot de passe du compte d'administrateur par défaut n'expire jamais.
- La commande renvoie une erreur si elle est utilisée lorsque le mode STIG n'est pas activé.

- Cette fonctionnalité doit être activée séparément après l'activation du mode STIG.
- Cette fonctionnalité doit être désactivée séparément avant la désactivation du mode STIG.

Autres exigences en matière de mot de passe

D'autres exigences en matière de mot de passe sont ajoutées pour les comptes utilisateur créés ou modifiés après l'activation du mode STIG :

- Taille minimale de mot de passe
- Nombre de mots de passe
- Période de validité du mot de passe

Le paramètre Taille minimale de mot de passe (`-passwdMinSize`) désigne la taille minimale que les mots de passe des comptes utilisateur locaux doivent avoir lors de la création d'un compte utilisateur ou lors de la modification d'un mot de passe. La taille minimale du mot de passe peut être configurée pour être comprise entre 8 et 40 caractères. La valeur par défaut lorsque les paramètres du compte utilisateur sont activés sans spécifier la taille minimale du mot de passe est de 15 caractères. Lorsque les paramètres du compte utilisateur sont désactivés, la taille minimale du mot de passe est définie à 8 caractères. Toute modification apportée à ce paramètre n'affecte pas les comptes utilisateur locaux ayant été créés avant la modification, sauf si le mot de passe est modifié.

Le paramètre Nombre de mots de passe (`-passwdCount`) représente le nombre de mots de passe ne pouvant pas être réutilisés pour les comptes utilisateur locaux. Le nombre de mots de passe peut être configuré pour être compris entre 3 et 12 mots de passe. La valeur par défaut lorsque les paramètres du compte utilisateur sont activés sans spécifier le nombre de mots de passe est de 5 mots de passe. Lorsque les paramètres de compte utilisateur sont désactivés, le nombre de mots de passe est défini à 3 mots de passe. Ce paramètre a une incidence sur tous les comptes utilisateur locaux existants et nouveaux.

Le paramètre Période de validité du mot de passe (`-passwdPeriod`) désigne la période en jours avant expiration des comptes utilisateur locaux. La période de validité du mot de passe peut être configurée pour être comprise entre 1 et 180 jours, la valeur -noPasswdPeriod signifiant qu'un mot de passe n'expirera jamais. La valeur par défaut lorsque les paramètres du compte utilisateur sont activés sans spécifier de période de validité du mot de passe est de 60 jours. Lorsque les paramètres de compte utilisateur sont désactivés, le champ de la période de validité du mot de passe est vide. Ce paramètre a une incidence sur tous les comptes utilisateur locaux existants et nouveaux. Toutefois, ce paramètre ne s'applique pas au compte utilisateur administrateur par défaut pour lequel le mot de passe n'expire jamais.

État d'expiration du mot de passe

Un utilisateur doté d'un rôle d'administrateur ou d'administrateur de la sécurité peut consulter le paramètre d'expiration du mot de passe de tous les comptes utilisateur locaux. Ce paramètre ne peut pas être défini. Il peut uniquement être affiché lorsque l'option `-detail` est spécifiée dans la commande UEMCLI `/user/account/settings show`.

L'état d'expiration du mot de passe pour un compte utilisateur apparaît sous l'une des valeurs suivantes :

- s.o. : S'affiche lorsqu'un mot de passe est défini pour ne jamais expirer, lorsque le compte utilisateur est de type LDAP ou lorsque les paramètres de compte utilisateur sont désactivés.
- nb jours restants : S'affiche lorsque les paramètres du compte utilisateur sont activés et que la période de validité du mot de passe est configurée sur une valeur supérieure à 0.

- expiré : S'affiche lorsque le mot de passe du compte utilisateur a expiré.

Exigences inhérentes aux échecs de connexion

Les exigences inhérentes aux échecs de connexion suivantes sont ajoutées aux comptes utilisateur locaux après l'activation du mode STIG :

- Nombre maximal de connexions ayant échoué
- Échec de la période de connexion

Le nombre maximal autorisé d'échecs de connexion consécutifs pour les comptes utilisateur locaux peut être configuré pour être compris entre 1 et 10 échecs de connexion consécutifs. La valeur par défaut lorsque les paramètres du compte utilisateur sont activés sans spécifier le nombre maximal d'échecs de connexion est de 3 échecs de connexion consécutifs. Lorsque les paramètres de compte utilisateur sont désactivés, aucune valeur n'est définie pour le nombre maximal d'échecs de connexion consécutifs.

Remarque

Les paramètres de la période d'échec de connexion (`-failedLoginPeriod`) et de la période de blocage (`-lockoutPeriod`) doivent être spécifiés par une valeur lorsque le paramètre du nombre maximal d'échecs de connexion (`-maxFailedLogins`) est spécifié. La valeur `-noMaxFailedLogins` signifie qu'il n'y a pas de nombre maximum autorisé d'échecs de connexions consécutifs. En outre, `-noFailedLoginPeriod` et `-noLockoutPeriod` doivent être spécifiés lorsque `-noMaxFailedLogins` est défini. Pour en savoir plus sur ces paramètres, reportez-vous à la section Désactivation/réactivation du nombre d'échecs de connexion à la page 91.

Le paramètre de période d'échec de connexion représente la période en secondes pendant laquelle le nombre d'échecs de connexion fait l'objet d'un suivi pour les comptes utilisateur locaux. La période peut être configurée pour être comprise entre 1 et 3 600 secondes. La valeur par défaut lorsque les paramètres de compte utilisateur sont activés sans spécifier la période d'échec de connexion est de 900 secondes. Lorsque les paramètres de compte utilisateur sont désactivés, le champ de la période d'échec de connexion est vide.

Remarque

Les paramètres de la période d'échec de connexion (`-maxFailedLogins`) et de la période de blocage (`-lockoutPeriod`) doivent être spécifiés par une valeur lorsque le paramètre de la période d'échec de connexion (`-failedLoginPeriod`) est spécifié. La valeur `-noFailedLoginPeriod` signifie que le nombre d'échecs de connexion consécutifs ne fait pas l'objet d'un suivi au cours d'une période donnée. En outre, `-noMaxFailedLogins` et `-noLockoutPeriod` doivent être spécifiés lorsque `-noFailedLoginPeriod` est défini. Pour en savoir plus sur ces paramètres, reportez-vous à la section Désactivation/réactivation du nombre d'échecs de connexion à la page 91.

Période de blocage

Le paramètre de période de blocage représente la période en secondes pendant laquelle le compte utilisateur local est bloqué lorsque le nombre maximal d'échecs de connexion consécutifs a été atteint durant la période d'échec de connexion. La période peut être configurée pour être comprise entre 1 et 86 400 secondes. La valeur par défaut lorsque les paramètres de compte utilisateur sont activés sans spécifier la période de blocage est de 3 600 secondes. Lorsque les paramètres de compte utilisateur sont désactivés, le champ de la période de blocage est vide.

Remarque

Les paramètres du nombre maximum d'échecs de connexion (`-maxFailedLogins`) et de la période d'échec de connexion (`-failedLoginPeriod`) doivent être spécifiés par une valeur lorsque le paramètre de la période de blocage (`-lockoutPeriod`) est spécifié. La valeur `-noLockoutPeriod` signifie que le compte ne sera pas bloqué parce qu'il a atteint la limite maximale d'échecs de connexion durant la période d'échec de connexion. En outre, `-noMaxFailedLogins` et `-noFailedLoginPeriod` doivent être spécifiés lorsque `-noLockoutPeriod` est défini. Pour en savoir plus sur ces paramètres, reportez-vous à la section Désactivation/réactivation du nombre d'échecs de connexion à la page 91.

Désactivation/réactivation du nombre d'échecs de connexion

Un utilisateur doté du rôle d'administrateur ou d'administrateur de la sécurité peut choisir de désactiver toutes les restrictions de connexion en définissant simultanément les paramètres `-noMaxFailedLogins`, `-noFailedLoginPeriod` et `-noLockoutPeriod` en une seule commande, par exemple :

```
uemcli -d 10.0.0.1 -u Local/admin - p MyPassword456 ! /User/Account/
Settings définir - noMaxFailedLogins - noFailedLoginPeriod -
noLockoutPeriod
```

⚠ ATTENTION

Il n'est pas recommandé d'exécuter cette commande en mode STIG. Tant que ce paramètre est activé, une attaque du mot de passe par force brute peut se produire car aucune vérification n'est effectuée.

Pour réactiver toutes les restrictions de connexion, définissez simultanément des valeurs aux paramètres `-maxFailedLogins`, `-failedLoginPeriod` et `-lockoutPeriod` en une seule commande, par exemple :

```
uemcli -d 10.0.0.1 -u Local/admin -p MyPassword456! /user/account/
settings set -maxFailedLogins 3 -failedLoginPeriod 900 -lockoutPeriod
3600
```

Délai d'inactivité de la session

Le paramètre Délai d'inactivité de la session représente la période en secondes pendant laquelle la session d'un utilisateur peut être inactive avant la fin automatique de la session. La période peut être configurée pour être comprise entre 1 et 3 600 secondes. La valeur par défaut lorsque les paramètres du compte utilisateur sont activés sans spécifier de délai d'inactivité de la session est de 600 secondes. Lorsque les paramètres de compte utilisateur sont désactivés, le champ du délai d'inactivité de la session est vide. Ce paramètre s'applique aux comptes utilisateur locaux et LDAP.

Remarque

La valeur `-noSessionIdleTimeout` signifie que la session ne va pas expirer en raison de l'inactivité.

Activer le blocage administrateur par défaut

Le paramètre Activer le blocage administrateur par défaut indique si les fonctionnalités de verrouillage de compte manuel et automatique s'appliqueront au compte d'administrateur par défaut local. Ce paramètre peut être configuré pour être soit `yes` ou `no`. La valeur par défaut est `no` lorsque les paramètres de compte utilisateur sont

activés sans spécifier ce paramètre. La valeur `no` signifie que les fonctionnalités de verrouillage manuel et automatique du compte ne s'appliquent pas au compte utilisateur administrateur local par défaut.

Verrouillage/déverrouillage manuel du compte (déploiements physiques uniquement)

Un utilisateur doté du rôle d'administrateur a la possibilité de verrouiller/déverrouiller manuellement les comptes utilisateur. Une fois qu'un compte utilisateur est verrouillé manuellement, l'utilisateur ne peut pas s'authentifier même si les informations d'identification sont valides. En outre, le compte utilisateur reste verrouillé jusqu'à ce qu'un administrateur le déverrouille manuellement.

Voici un récapitulatif des limites de la fonctionnalité de verrouillage/déverrouillage manuel :

- La fonctionnalité est uniquement disponible via l'interface UEMCLI, `/user/account/ -id <administrator_id> set -locked {yes|no}`.
- Seul un utilisateur doté du rôle d'administrateur peut exécuter cette commande.
- Le compte administrateur par défaut ne peut pas être verrouillé/déverrouillé.
- Un utilisateur ne peut pas verrouiller/déverrouiller ses propres comptes.
- La commande renvoie une erreur si elle est utilisée lorsque le mode STIG n'est pas activé.

Contrôles de sécurité physique (déploiements physiques uniquement)

Le lieu d'installation du système de stockage doit être choisi et, si nécessaire, adapté de sorte que sa sécurité physique soit garantie. Il convient notamment de veiller à ce que les portes et verrous soient en nombre suffisant, à limiter l'accès physique au système aux seules personnes autorisées et à contrôler cet accès, à doter le système d'une source d'alimentation fiable, et à respecter les meilleures pratiques en matière de câblage.

En outre, les éléments et composants suivants du système de stockage nécessitent une vigilance particulière :

- Bouton de réinitialisation des mots de passe : réinitialise temporairement les mots de passe par défaut du compte de maintenance et du compte administrateur par défaut du système de stockage jusqu'à ce qu'un administrateur réinitialise les mots de passe.
- Connecteur de port de service Ethernet du SP : permet l'accès authentifié via une connexion par port de service Ethernet du SP.

Protection antivirus

Le système de stockage prend en charge CAVA (Common AntiVirus Agent). CAVA, composant de Common Event Enabler (CEE), offre une solution antivirus aux clients utilisant un système de stockage. Il emploie un protocole SMB standard dans un environnement Microsoft Windows Server. CAVA utilise un logiciel antivirus tiers pour identifier et éliminer les virus connus avant qu'ils infectent les fichiers du système de stockage. Le programme d'installation CEE (qui contient celui de CAVA) et les notes

de mise à jour CEE sont disponibles via le Support en ligne sous **Support par produit** pour la gamme Unity, Unity VSA, Unity hybride ou Unity 100 % Flash dans **Téléchargements** > **Version complète**.

ANNEXE A

Suites de chiffrement TLS

Cette annexe répertorie les suites de chiffrement TSL prises en charge par le système de stockage.

Ce document traite des points suivants :

Suites de chiffrement TLS pris en charge

Une suite de chiffrement définit un ensemble de technologies permettant de sécuriser vos communications TLS :

- Algorithme d'échange de clé (comment la clé secrète utilisée pour chiffrer les données est communiquée entre le client et le serveur). Exemples : Clé RSA ou Diffie-Hellman (DH)
- Méthode d'authentification (comment les hôtes peuvent authentifier l'identité des hôtes distants). Exemples : Certificat RSA, certificat DSS ou aucune authentification
- Méthode de chiffrement (comment chiffrer les données). Exemples : AES (256 ou 128 bits)
- Algorithme de hachage (assurer les données en fournissant un moyen de déterminer si les données ont été modifiées). Exemples : SHA-2 ou SHA-1

Les suites de chiffrement prises en charge combinent tous ces éléments.

La liste suivante affiche les noms OpenSSL des suites de chiffrement TLS pour le système de stockage et les ports associés.

Tableau 20 Suites de chiffrement TSL par défaut/prises en charge sur le système de stockage

Suites de chiffrement	Protocoles	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444

Tableau 20 Suites de chiffrement TSL par défaut/prises en charge sur le système de stockage (suite)

Suites de chiffrement	Protocoles	Ports
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989

ANNEXE B

Configuration LDAP

Cette annexe décrit comment configurer le système Unity pour qu'il se connecte à un serveur LDAP pour l'authentification et comment attribuer des rôles aux utilisateurs et groupes LDAP.

Ce document traite des points suivants :

À propos de la configuration LDAP

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole d'application pour l'interrogation et la modification de services d'annuaire s'exécutant sur des réseaux TCP/IP. Il aide à centraliser la gestion des opérations d'autorisation et d'authentification réseau. L'intégration des utilisateurs de Unisphere à un environnement LDAP existant offre un moyen de contrôler l'accès de gestion en fonction de comptes utilisateur et de groupes définis à l'aide de l'annuaire LDAP.

Avant de configurer LDAP, vous devez configurer le système Unity pour qu'il se connecte à un serveur DNS. Cette action est requise pour résoudre l'adresse IP et le nom d'hôte complet pour chaque serveur LDAP configuré.

Les entités en réseau qui échangent des données s'authentifient les unes les autres à l'aide de certificats. Pour que des communications sécurisées aient lieu entre deux entités en réseau, une entité doit accorder sa confiance au certificat de l'autre entité (acceptation). Unisphere utilise le protocole SSL/TLS et la norme de certificat X.509 pour sécuriser les communications entre les clients (systèmes de stockage) et les serveurs (LDAP). Le système Unity nécessite le téléchargement du fichier de chaîne de certificats, afin de vérifier correctement le certificat de serveur reçu du serveur LDAP lors de l'établissement de la session TLS.

Une fois les paramètres LDAP du système configurés pour le système Unity, vous pouvez exécuter des fonctions de gestion utilisateur, telles que l'attribution d'autorisations d'accès à Unisphere sur la base d'utilisateurs et de groupes existants, dans le contexte d'une structure d'annuaire LDAP déterminée.

Suivez cette séquence d'étapes pour configurer LDAP sur un système Unity :

1. Configurez le serveur DNS

   Remarque

   requis uniquement lorsque les noms d'hôte sont utilisés pour les adresses IP LDAP ou lorsque la fonctionnalité LDAP dynamique est utilisée. Dans le cas contraire, cette étape est facultative.

2. Configurer le serveur LDAP.
3. Vérifiez la connexion du serveur LDAP.
4. Configurez LDAPS pour le serveur LDAP.
5. Vérifiez la connexion au serveur LDAP à l'aide du protocole LDAPS.
6. Configurez les utilisateurs et les groupes LDAP

Remarque

L'*Aide en ligne Unisphere* fournit plus d'informations sur LDAP et DNS et les étapes pour configurer le système Unity afin de se connecter à un serveur LDAP et un serveur DNS, et comment assigner des rôles et gérer des utilisateurs et groupes LDAP.

Configurer le serveur DNS

Le DNS doit être configuré avant de configurer le serveur LDAP pour résoudre les adresses du serveur LDAP. Cela est nécessaire pour résoudre l'adresse IP et le nom d'hôte complet pour que chaque serveur LDAP soit résolu.

Pour configurer le DNS, procédez ainsi :

Procédure

1. Dans Unisphere, cliquez sur l'icône en forme d'engrenage pour afficher la page **Paramètres**.
2. Dans le panneau de gauche, sous **Gestion**, cliquez sur **Serveur DNS**.

   La page **Gérer les serveurs du nom de domaine** apparaît.
3. En fonction de votre configuration de site, procédez de l'une des façons suivantes :
   - Si le système est configuré pour récupérer les adresses du serveur DNS à partir d'une source distante, sélectionnez **Obtenir automatiquement une adresse de serveur DNS**.
   - Sélectionnez **Configurer manuellement une adresse de serveur DNS** et entrez au moins une adresse IP pour un serveur DNS sur lequel le serveur LDAP est configuré. Si les serveurs LDAP sont configurés manuellement à l'aide d'adresses IP, les serveurs LDAP doivent se trouver à la fois dans des zones de recherche directe et inversée sur le serveur DNS.
4. Une fois que les adresses du serveur DNS sont configurées, cliquez sur **Appliquer** pour enregistrer la configuration du serveur DNS.

Configurer un serveur LDAP

La configuration du serveur LDAP consiste à spécifier les informations de configuration nécessaires pour se connecter au serveur LDAP.

Pour configurer LDAP, procédez ainsi :

Procédure

1. Dans Unisphere, cliquez sur l'icône en forme d'engrenage pour afficher la page **Paramètres**.
2. Dans le panneau de gauche, sous **Utilisateurs et groupes**, cliquez sur **Services d'annuaire**.

   La page **Configurer les informations d'identification du serveur LDAP** s'affiche.
3. Pour le **Nom du domaine**, tapez le nom de domaine du serveur d'authentification LDAP.

   Le nom de domaine doit être renseigné lorsque la configuration du serveur LDAP est créée. Après cela, il est grisé parce qu'il ne peut pas être modifié sans supprimer et recréer la configuration du serveur LDAP.
4. Pour le **Nom unique**, saisissez le nom unique de l'utilisateur LDAP disposant de privilèges d'administrateur.

   Le nom unique doit être spécifié dans l'un des formats suivants :
   - Format de notation LDAP (par exemple `cn=Administrator,cn=Users,dc=mycompany,dc=com`)
   - <*user*>@<*domain*> format (par exemple, `Administrator@mycompany.com`)
   - <*domain*>/<*user*> format (par exemple, `mycompany.com/Administrator`)
5. Pour le **Mot de passe**, tapez le mot de passe de l'utilisateur spécifié dans **Nom unique**.

6. Si le serveur LDAP utilise un port différent pour LDAP par rapport au numéro de port par défaut 389, remplacez le port par le numéro de port requis.

   Par exemple, spécifiez le port 3268 pour LDAP avec l'authentification au niveau de la forêt. (`nsroot.net` au lieu de `nam.nsroot.net` avec LDAP permet aux clients d'interroger l'intégralité de la forêt Active Directory (AD) (port 3268) plutôt que simplement le domaine AD (port TCP 389). En outre, l'association de rôle AD est basée sur les périmètres de groupes pour les groupes locaux de domaine et les groupes universels. Cela permet aux utilisateurs finaux de faire une recherche dans AD avec le périmètre approprié comme cela est nécessaire et pour éviter les recherches de groupe inutiles.) Il est fortement recommandé de configurer et vérifier LDAP avant de configurer LDAP sécurisé (LDAPS). Ceci réduit au minimum tout dépannage qui peut être nécessaire lors de l'activation de LDAPS.

7. Dans **Adresse du serveur**, exécutez l'une des opérations suivantes :

   - Pour ajouter manuellement une adresse de serveur, cliquez sur **Ajouter** pour afficher la boîte de dialogue **Serveur LDAP**, entrez l'adresse IP ou le nom d'hôte complet, puis cliquez sur **OK**. Pour supprimer une adresse de serveur, sélectionnez l'adresse dans la zone de texte et cliquez sur **Supprimer**.
   - Pour récupérer automatiquement les adresses du serveur DNS, cliquez sur **Découverte automatique**.

8. Si le serveur LDAP dispose d'un chemin de recherche différent de la valeur par défaut `cn=Users,dc=` pour l'utilisateur ou le groupe, ou les deux, cliquez sur **Avancé**.

   La boîte de dialogue **Avancé** s'affiche.

9. Dans la fenêtre **Avancé**, mettez à jour les chemins de recherche ou d'autres champs si nécessaire, puis cliquez sur **OK** pour enregistrer les modifications de configuration avancées.

   Par exemple, si vous configurez l'authentification au niveau de la forêt, sélectionnez **Avancé** pour accéder à la fenêtre **Avancé** et spécifiez **`userPrincipalName`** dans le champ **Attribut ID utilisateur**. Si le serveur LDAP a un chemin de recherche autre que celui par défaut (cn=Users,dc=) pour les utilisateurs, les groupes ou les deux, accédez à la fenêtre **Paramètres avancés** pour mettre à jour les chemins de recherche ou d'autres propriétés si nécessaire.

10. Une fois que toutes les informations de configuration LDAP sont spécifiées, cliquez sur **Appliquer** pour enregistrer la configuration.

    Si **Découverte automatique** a été sélectionnée pour récupérer automatiquement les adresses du serveur DNS, les adresses de serveur obtenues à partir de DNS sont affichées en grisé dans **Adresse du serveur**.

À effectuer

Une fois la configuration du serveur LDAP enregistrée et pour éviter tout risque d'indisponibilité des données, la configuration doit être vérifiée pour confirmer que les connexions au serveur LDAP seront réussies.

Vérifier la configuration LDAP

Remarque

Pour éviter tout risque d'indisponibilité des données, vous devez vérifier la connexion LDAP après chaque modification de la configuration LDAP.

Pour vérifier la réussite de la connexion au serveur LDAP, procédez comme suit :

Procédure

1. Cliquez sur **Vérifier la connexion** sur la page **Configurer les informations d'identification du serveur LDAP**.

   Si la configuration est valide, une connexion sera établie avec le serveur LDAP et une coche verte apparaîtra avec le texte **Connexion vérifiée**.
2. Si la vérification échoue, les étapes suivantes sont recommandées pour résoudre le problème d'échec :
   a. Vérifiez les informations de configuration **Configurer les informations d'identification du serveur LDAP**, en particulier le **Nom unique** (nom d'utilisateur), le **Mot de passe** et l'**Adresse du serveur** (adresse IP ou nom d'hôte).
   b. Vérifiez que le serveur LDAP est en ligne.
   c. Vérifiez qu'il n'y a pas de problème de réseau, comme des règles de pare-feu qui pourraient bloquer l'accès au port LDAP, la configuration du routeur réseau qui empêcherait la connexion, etc.

Configurer LDAP sécurisé

La configuration de LDAP sécurisé (LDAPS) requiert les éléments suivants :

- Configurer le protocole LDAPS et le port
- Configurer la chaîne de certificats

Lorsque LDAPS est configuré, le système Unity se connecte au serveur LDAP à l'aide de TLS. Le système Unity nécessite le téléchargement du fichier de chaîne de certificats, afin de vérifier correctement le certificat de serveur reçu du serveur LDAP lors de l'établissement de la session TLS.

Le format du fichier de certificat à télécharger est le suivant :

- Le fichier de certificat doit se terminer par une extension de fichier `cer`. Exemple : `LdapServerChain.cer`
- Tous les certificats du fichier de certificat à télécharger doivent être au format PEM. Les certificats formatés PEM sont des textes ASCII qui commencent par `-----BEGIN CERTIFICATE-----` et finissent par `-----END CERTIFICATE-----`.
- Le certificat du serveur LDAP doit avoir le Nom du serveur, tel qu'il est spécifié dans la configuration LDAP, dans le champ Objet ou Nom alternatif de l'objet du certificat. Ceci est nécessaire pour vérifier que le certificat provient du serveur LDAP désiré.
- Si le certificat du serveur LDAP est auto-signé, seul le certificat du serveur est requis.
- Si le certificat du serveur LDAP est signé par une autorité de certification, la chaîne de certificats, jusqu'à l'autorité de certification racine, doit figurer dans le fichier de certificat à télécharger dans l'ordre suivant :

1. Certificat de l'autorité de certification intermédiaire (le cas échéant).
2. ...
3. Certificat de l'autorité de certification racine.
4. S'il y a plusieurs certificats dans le fichier à télécharger, il doit y avoir une nouvelle ligne entre chaque certificat.

Pour configurer LDAPS, procédez ainsi :

Procédure

1. Cochez la case **Utiliser le protocole LDAPS** à la page **Configurer les informations d'identification du serveur LDAP**.

   Le **port** passe automatiquement à 636, qui est le numéro de port LDAPS par défaut. Si le serveur LDAP utilise un port différent pour LDAPS, remplacez le port par le numéro de port requis. Par exemple, spécifiez le port 3269 pour LDAPS avec l'authentification au niveau de la forêt. (`nsroot.net` au lieu de `nam.nsroot.net` avec LDAPS permet aux clients d'interroger l'intégralité de la forêt AD (port 3269) plutôt que simplement le domaine AD (port TCP 636). En outre, l'association de rôle AD est basée sur les périmètres de groupes pour les groupes locaux de domaine et les groupes universels. Cela permet aux utilisateurs finaux de faire une recherche dans AD avec le périmètre approprié comme cela est nécessaire et pour éviter les recherches de groupe inutiles.) En outre, **Télécharger le certificat** devient actif lorsque la case à cocher **Utiliser le protocole LDAPS** est sélectionnée.
2. Cliquez sur **Télécharger le certificat**.

   La boîte de dialogue **Télécharger le fichier** s'affiche.
3. Cliquez sur **Choisir un fichier**.
4. Naviguez jusqu'au fichier de certificat souhaité, sélectionnez le fichier et cliquez sur **Démarrer le téléchargement**.
5. Une fois le chargement du fichier terminé, cliquez sur **Appliquer** pour enregistrer les modifications de configuration.

À effectuer

Vous devez vérifier la configuration après avoir configuré LDAP et téléchargé le fichier de certificat du serveur.

Vérifier la configuration LDAPS

Remarque

Pour éviter tout risque d'indisponibilité des données, vous devez vérifier la connexion LDAP après chaque modification de la configuration LDAP.

Pour vérifier la configuration LDAPS, exécutez la commande suivante :

Procédure

1. Cliquez sur **Vérifier la connexion** sur la page **Configurer les informations d'identification du serveur LDAP**.

   Si la configuration est valide, une connexion sera établie avec le serveur LDAP et une coche verte apparaîtra avec le texte **Connexion vérifiée**.
2. Si la vérification échoue, les étapes suivantes sont recommandées pour résoudre le problème d'échec :

a. Vérifiez les informations de configuration **Configurer les informations d'identification du serveur LDAP**, en particulier le numéro de port.

b. Vérifiez que le serveur LDAP est en ligne et configuré pour LDAPS.

c. Vérifiez que les certificats du fichier de certificat téléchargé sont valides, par exemple, qu'ils n'ont pas expiré et se trouvent dans le bon ordre.

d. Vérifiez que le **Nom du serveur** configuré se trouve dans le champ Objet ou Nom alternatif de l'objet du certificat du serveur LDAP.

e. Vérifiez qu'il n'y a pas de problème de réseau, comme des règles de pare-feu qui pourraient bloquer l'accès au port LDAPS, etc.

À effectuer

Lorsque le serveur LDAP est configuré, un ou plusieurs utilisateurs ou groupes LDAP doivent être ajoutés au système Unity pour mapper les utilisateurs (ou groupes) aux rôles. Sinon, l'authentification LDAP réussira lors de la connexion, mais la connexion échouera car aucun rôle ne pourra être assigné à l'utilisateur.

Configurer un utilisateur LDAP

La procédure de création d'un groupe LDAP sur le système Unity est la même que la création d'un utilisateur LDAP, sauf que le groupe LDAP doit également être créé sur le serveur LDAP, et les utilisateurs LDAP ajoutés en tant que membres de ce groupe. La création d'un groupe LDAP présente l'avantage d'un groupe LDAP configuré sur le système Unity, puis attribué à plusieurs utilisateurs LDAP.

Pour créer un utilisateur ou un groupe LDAP, procédez comme suit :

Remarque

Le serveur LDAP doit être configuré avant qu'un utilisateur ou un groupe LDAP puisse être créé.

Procédure

1. Dans Unisphere, cliquez sur l'icône en forme d'engrenage pour afficher la page **Paramètres**.
2. Dans le panneau de gauche, sous **Utilisateurs et groupes**, cliquez sur **Gestion des utilisateurs**.

   La page **Gérer les utilisateurs et les groupes** s'affiche.
3. Cliquez sur l'icône Ajouter (signe plus).

   L'assistant **Créer un utilisateur ou un groupe** s'affiche.
4. Exécutez l'une des opérations suivantes :
   - Cliquez **Utilisateur LDAP**.
   - Cliquez sur **Groupe LDAP**.
5. Cliquez sur **Suivant**.

   La page **Informations LDAP** s'affiche avec l'autorité LDAP affichée sur la page.
6. Pour **l'utilisateur LDAP**, tapez le nom d'utilisateur répertorié dans le serveur LDAP.
7. Cliquez sur **Suivant**.

   La page **Rôle** s'affiche.

8. Cliquez sur le bouton radio du rôle à assigner.
9. Cliquez sur **Suivant**.

   La page **Résumé** apparaît.
10. Après avoir vérifié que le nom d'utilisateur ou de groupe LDAP et le rôle sont corrects, cliquez sur **Terminer** pour terminer la transaction ou sur **Précédent** pour modifier la configuration de l'utilisateur.

    Lorsque la création de l'utilisateur ou du groupe a réussi, la page **Résultats** s'affiche.
11. Cliquez sur **Fermer** pour fermer l'assistant **Créer un utilisateur ou un groupe**.

    L'utilisateur ou le groupe LDAP qui vient d'être ajouté apparaîtra dans la liste d'utilisateurs de la page **Gérer des utilisateurs et des groupes**.