Dell EMC Data Protection Advisor

Version 18.1

Guide d'installation et d'administration

302-004-935

REV 02

DELL EMC

Publié en Juillet 2018

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

FIGURES

TABLEAUX

Préface

En vue d'améliorer la qualité de sa gamme de produits, EMC publie régulièrement des révisions de ses matériels et logiciels. 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 EMC.

Remarque

Les informations figurant dans ce document sont exactes à la date de publication. Consultez le Support en ligne EMC (https://support.emc.com) afin de vous assurer que vous utilisez la version la plus récente de ce document.

Objectif

Ce document explique comment installer DPA et configurer DPA pour surveiller un environnement de protection des données. Ce document décrit également les fonctions d'administration, notamment la création d'utilisateurs et de rôles, la mise à jour des paramètres système, la création de politiques et la résolution des problèmes associés aux collections de données.

Certification ISO 9001

Le système de gestion régissant la conception et le développement de ce produit est certifié ISO 9001:2015.

Audience

Ce document est destiné aux administrateurs système. Les lecteurs de ce document doivent être familiarisés avec les tâches suivantes :

- Identifier les différents composants matériels et logiciels qui composent l'environnement de sauvegarde et de réplication.
- Suivre les procédures pour configurer les opérations de sauvegarde et de réplication.
- Suivre les instructions pour rechercher les problèmes et implémenter des solutions.

Historique des révisions

Le tableau ci-dessous présente l'historique des révisions de ce document.

Tableau 1 Historique des révisions

Révision	Date	Description
01	6 juillet 2018	Première publication de ce document pour DPA18.1
02	13 juillet 2018	Mise à jour des sections suivantes : Mise à niveau des agents DPA à la page 72

Documentation connexe

La documentation DPA comprend les publications suivantes :

- *Data Protection Advisor Custom Reporting Guide*
- *Guide de référence pour la collecte des données de Data Protection Advisor*
- *Guide d'administration et d'installation de Data Protection Advisor*
- *Notes techniques de Data Protection Advisor*
- *Aide en ligne de Data Protection Advisor*
- *Guide produit de Data Protection Advisor*
- *Notes de mise à jour de Data Protection Advisor*
- *Data Protection Advisor Report Reference Guide*
- *Guide de programmation pour l'utilisation de l'API REST Data Protection Advisor*
- *Guide de configuration et de sécurité de Data Protection Advisor*
- *Guide de compatibilité de Data Protection Advisor*
- *Autre documentation technique et livres blancs*

Conventions utilisées dans ce document pour certains points particuliers
EMC utilise les conventions suivantes pour attirer l'attention du lecteur sur certains points particuliers :

NOTE

Indique des pratiques n'impliquant aucune blessure.

Remarque

Fournit des informations importantes, mais non vitales.

Tableau 2 Conventions de style

Gras	Utilisé pour les noms d'éléments d'interface, tels que les noms de boutons, de champs, d'onglets, de chemins de menus (tout ce qui nécessite une sélection ou un clic de la part de l'utilisateur)
Italique	Utilisé pour les titres complets de publications référencées dans le texte
`Monospace`	Utilisé pour : • code système ; • sortie du système, telle qu'un message d'erreur ou un script ; • noms de chemin, noms de fichier, invites et syntaxe ; • commandes et options.
Monospace italique	Utilisé pour les variables
`Monospace gras`	Utilisé pour les entrées utilisateur
[ ]	Des crochets entourent les valeurs facultatives.
|	Une barre verticale indique des sélections alternatives : la barre signifie « ou »
{ }	Les accolades entourent le contenu que l'utilisateur doit spécifier, c'est-à-dire x, y ou z.
...	Les points de suspension indiquent des informations non essentielles omises dans l'exemple

Obtenir de l'aide

Pour plus d'informations sur le support, les produits et les licences EMC, procédez comme suit :

Informations sur les produits

Pour toute information sur la documentation, les notes de mise à jour, les mises à jour logicielles ou les produits EMC, consultez le Support en ligne d'EMC à l'adresse : https://support.emc.com.

Support technique

Rendez-vous sur le site de support en ligne EMC https://support.emc.com et choisissez **Centre de service** . Plusieurs options pour contacter le support technique EMC sont disponibles sur ce site Web. Notez que 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 EMC.

Communautés en ligne

Consultez le site EMC Community Network à l'adresse https://community.emc.com pour contacter vos homologues, discuter, découvrir les solutions et obtenir de l'assistance sur les produits. Communiquez en ligne et de façon interactive avec des clients, des partenaires et des professionnels certifiés au sujet de tous les produits EMC.

Vos commentaires

Vos suggestions nous aident à améliorer la précision, l'organisation et la qualité globale des publications utilisateur. Nous vous invitons à envoyer votre avis sur ce document à l'adresse suivante DPAD.Doc.Feedback@emc.com.

CHAPITRE 1

Préparation de l'installation de DPA

Le présent chapitre contient les sections suivantes :

Présentation

Tous les déploiements de DPA incluent les installations suivantes :

- Serveur datastore DPA et agent DPA sur un hôte
- Serveur d'applications DPA et agent DPA sur un autre hôte

Lors de l'installation de DPA, l'assistant d'installation vous guide pas à pas dans la mise en œuvre de ces composants.

L'installation des serveurs d'applications DPA et de datastore sur un seul hôte n'est pas prise en charge. Vous pouvez installer plusieurs serveurs d'applications sur le même serveur datastore. Chaque serveur d'applications supplémentaire sera installé sur son propre hôte et ces serveurs seront installés en tant que cluster DPA. Vous pouvez installer des agents DPA supplémentaires pour la surveillance du système et la collecte des données à distance. La réplication du datastore est prise en charge par DPA pour permettre la réplication continue, sécurisée et fiable. DPA peut ainsi conserver un réplica, ou Slave, du datastore primaire, ou Master, à des fins de résilience, en cas de point unique de défaillance.

Configuration système requise

DPA exige la configuration système minimale suivante : *Guide de compatibilité de Data Protection Advisor* fournit une liste complète de la configuration système requise.

Plates-formes de serveur DPA

Les serveurs DPA ne prennent en charge que des systèmes d'exploitation 64 bits. Consultez votre responsable de compte afin de déterminer le dimensionnement approprié pour votre environnement.

Mémoire requise

- 16 Go de RAM/4 cœurs pour le serveur de datastore DPA
- 16 Go de RAM/4 cœurs pour le serveur d'applications DPA

Exigences en matière de disque dur :

- 18 Go de stockage sur disque rattaché localement pour le serveur d'applications
- 20 Go de stockage sur disque rattaché localement pour le serveur de datastore
- 3 Go d'espace libre sont requis pour la mise à niveau de la base de données

Remarque

Les systèmes colocalisés de datastore et d'application ne sont pas pris en charge dans les systèmes de production. Bien que le programme d'installation comprenne une option de système conjoint, lorsqu'elle est sélectionnée, une boîte de dialogue indiquant qu'elle n'est pas prise en charge dans les systèmes de production s'affiche.

- Le serveur d'applications DPA et les serveurs datastore DPA ne doivent pas être utilisés pour exécuter d'autres applications. Les ressources de l'hôte du serveur d'applications DPA et de l'hôte du datastore DPA doivent être dédiées à DPA.

- Si vous exécutez DPA dans un environnement virtualisé, le CPU et la mémoire alloués doivent être réservés aux serveurs DPA
- Le programme d'installation DPA dispose d'une limite souple de 7892 Mo et d'une limite stricte de 5844 Mo. La limite souple permet la poursuite de l'installation, mais pas la limite stricte.
- Le dimensionnement et le réglage automatiques de l'utilisation des ressources internes DPA s'effectuent au cours de l'installation. Si des ressources (CPU, mémoire, etc.) sont utilisées par d'autres applications durant l'installation, les performances de DPA peuvent être affectées.
- Systèmes d'exploitation :
  - Prise en charge des systèmes d'exploitation 64 bits uniquement
  - Microsoft Windows Server 2008 R2, 2012, 2012 R2 (x64 uniquement), 2016
  - Red Hat Linux ES/AS 6.0, 6.2, 6.4 (64 bits), 6.5, 6.8, 7, 7.1, 7.2, 7.3, 7.4 (64 bits)
    Exécutez l'agent de mise à jour (up2date) pour vous assurer que les derniers correctifs du système d'exploitation sont installés
  - SUSE Linux 12 x86 (64 bits)

  Exécutez l'agent de mise à jour (up2date) pour vous assurer que les derniers correctifs du système d'exploitation sont installés

  Pour améliorer les performances, libaio doit être installé sur le système et disponible dans `LD_LIBRARY_PATH`.

Stockage de datastore

Pour des raisons de performances, nous déconseillons l'installation du serveur datastore DPA sur des systèmes de fichiers NAS, tels que des partages CIFS ou NFS. En effet, la bande passante de ces systèmes de fichiers risque d'être insuffisante pour gérer les E/S requises.

Bien que la structure du système de fichiers standard datastore convienne pour la plupart des déploiements, vous pouvez distribuer différents systèmes de fichiers sur des systèmes de fichiers distincts, afin d'optimiser les performances lors de l'installation, dans les options d'installation avancées.

Autorisations

Afin d'éviter l'échec de l'installation, assurez-vous de disposer des autorisations suivantes avant d'installer le logiciel :

- Windows :
  - Les privilèges d'administrateur (au niveau du domaine ou local avec accès complet)
  - Si le contrôle des comptes utilisateur (UAC) est activé, utilisez Run As Administrator
- UNIX et Linux :
  - Utilisateur root
  - Si vous utilisez un logiciel de sécurité pour la gestion des accès au compte root, assurez-vous que les autorisations vous permettront de créer de nouveaux

utilisateurs une fois que vous serez utilisateur root. Ces autorisations doivent inclure la possibilité de créer des répertoires personnels par défaut pour le compte à créer.

Synchronisation de l'heure NTP

Il est recommandé de disposer du protocole NTP (Network Time Protocol) pour synchroniser le serveur DPA et les hôtes d'Agent DPA. Cela garantit la collecte précise et cohérente de données.

Le processus d'authentification de l'utilisateur DPA nécessite que les heures sur l'horloge du système sur la machine client et sur le serveur soient synchronisées à une minute près.

Points à prendre en compte pour l'installation

L'assistant d'installation DPA affiche les options avancées pour la configuration de la réplication du datastore avec les datastores maîtres et esclaves, et la configuration des objets d'application en cluster. Si vous utilisez l'une des options ou les deux, veillez à :

- Planifiez la topologie de déploiement finale avant de commencer l'installation.
- Prédéterminez tous les hôtes et toutes adresses IP et tenez-les à disposition.

Si vous prévoyez une installation avancée, contactez votre responsable de compte pour obtenir de l'aide sur la conception d'une solution d'architecture avancée.

Configuration de la mémoire virtuelle d'infrastructure et du CPU

Si vous prévoyez de déployer DPA dans une infrastructure virtualisée, procédez comme suit :

Procédure

- Assurez-vous que la mémoire allouée est réservée exclusivement pour chaque machine virtuelle.
- Placez l'application DPA et les VM datastore dans un pool de ressources où le partage d'allocation de ressources est défini sur High. Vous pouvez également sélectionner High Share Allocation pour chaque VM.
- Sélectionnez Thick Provision Eager Zeroed pour les disques du datastore. L'allocation de disques en provisionnement Thick avec mise à zéro rapide entraîne une allocation de l'ensemble de l'espace en amont. Le fichier disque est mis à zéro avant que le système soit mis à disposition pour utilisation.

Ressource de stockage du système d'exploitation

Réglage général

Au cours de l'installation, le programme d'installation règle le service de datastore DPA en fonction de l'environnement hôte sur lequel il est déployé. Ce réglage suppose que l'hôte est dédié à DPA et prend en compte des ressources comme l'espace disque, la mémoire totale et les cœurs CPU. Si, pendant la durée de vie du service de datastore DPA, l'une de ces ressources physiques augmente ou diminue, exécutez la commande dpa datastore tune sur l'hôte du datastore. Pour plus d'informations, reportez-vous à la section dpa datastore tune à la page 162.

Problèmes matériels avec le réglage

Pour les déploiements dans lesquels des performances optimales sont essentielles, le type et la qualité du matériel utilisé pour le serveur hôte du datastore ont un impact considérable sur les performances du service de datastore.

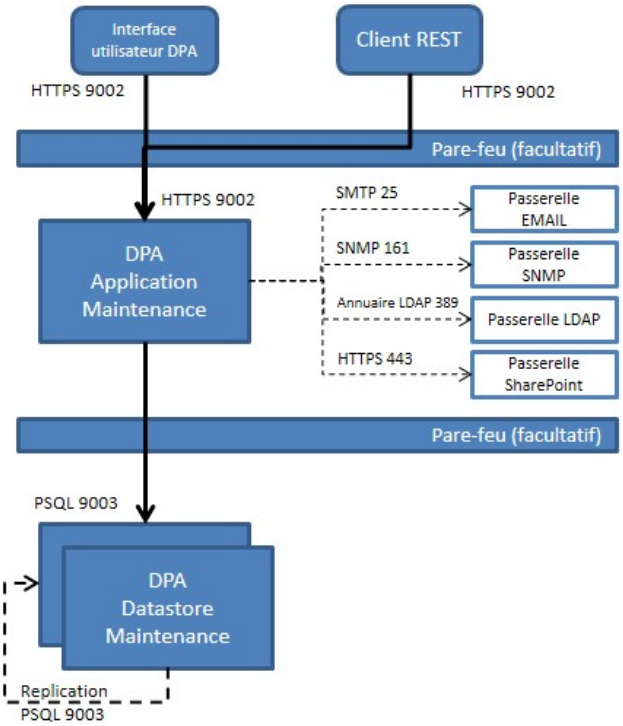
Généralement, plus votre système comporte de mémoire RAM et de piles de disques, meilleures sont les performances. En effet, la mémoire RAM supplémentaire permet de limiter les accès aux disques. En outre, les piles supplémentaires permettent de répartir les opérations de lecture et d'écritures sur plusieurs disques, ce qui améliore le rendement et réduit l'encombrement des têtes de lecture des disques.

En environnement de production, les services DPA Application et DPA Datastore doivent être installés sur des machines distinctes. Ainsi, le service de datastore bénéficie de plus de matériel, et le cache sur disque du système d'exploitation contient plus de données du datastore (et non des données d'autres applications ou des données système).

Paramètres de communication dans DPA

Pour assurer la communication entre le serveur DPA et les agents DPA, configurez les pare-feu du réseau de façon à autoriser la communication sur ces ports, comme illustré dans la figure suivante. La configuration d'un pare-feu supplémentaire peut être nécessaire pour autoriser la communication sur d'autres ports, selon ce que vous souhaitez surveiller. Par exemple, si vous surveillez Avamar, ouvrez le port 5555 entre le serveur Avamar et l'agent DPA. Pour plus d'informations, reportez-vous à la section « Découverte de l'environnement dans DPA ».

Figure 1 Ports et protocoles DPA



Remarque

*Il peut y avoir un ou plusieurs collecteurs et serveurs d'applications.

Dans l'illustration ci-dessus, les flèches montrent le chemin que suit la communication. L'agent DPA initie la connexion avec le serveur d'applications DPA sur le port 9002. Pour les pare-feu, cela dépend de l'endroit d'où part la connexion, de quel port elle part, et sur quel port d'écoute elle aboutit. DPA La communication entre l'agent et le serveur d'applications DPA passe par les TCP 9002 et 3741. Les communications entre l'agent et le serveur DPA sont sécurisées, chiffrées et compressées.

Les tableaux ci-dessous indiquent les ports supplémentaires requis sur les hôtes de déploiement, pour permettre à DPA de fonctionner correctement. Les ports répertoriés doivent accepter les connexions et autoriser les réponses de n'importe quelle connexion établie. Certains fournisseurs réseau décrivent ce type de connexion comme bidirectionnelle, et ces périphériques de sécurité réseau doivent refléter cela.

Paramètres des ports DPA

Les tableaux ci-dessous présentent les ports requis par DPA afin de fonctionner correctement. Selon les systèmes surveillés, des ports supplémentaires peuvent être nécessaires pour les Agents DPA. *Guide d'administration et d'installation de Data Protection Advisor* indique la configuration requise pour l'installation.

Tableau 3 Paramètres des ports d'application DPA

Port	Description	Sens du trafic
25	Port TCP utilisé pour le service SMTP	Connexion sortante au serveur SMTP.
80	Port TCP utilisé pour le service SharePoint	Connexion sortante vers le serveur SharePoint.
161	Port UDP utilisé pour le service SNMP	Connexion sortante vers les périphériques SNMP.
389/636 (sur SSL)	Port TCP utilisé pour l'intégration avec LDAP	Connexion sortante au serveur LDAP.
3741	Port TCP utilisé pour les communications d'agents DPA.	Connexion sortante aux agents DPA
4447	Port TCP utilisé pour les communications entre les services	Connexion entrante
4712	Port TCP utilisé pour les communications entre les services	Connexion localhost
4713	Port TCP utilisé pour les communications entre les services	Connexion localhost
5445	Port TCP utilisé pour les communications entre les services	Connexion localhost
5455	Port TCP utilisé pour les communications entre les services	Connexion localhost
8090	Port TCP utilisé pour les communications entre les services	Connexion localhost
9002	Port TCP utilisé pour le service HTTPS.	Connexion entrante sur SSL à partir de clients de l'interface utilisateur, de la CLI et de l'API REST.
9003	Port TCP utilisé pour les communications de datastore DPA.	Connexion sortante au datastore DPA.

Tableau 3 Paramètres des ports d'application DPA (suite)

Port	Description	Sens du trafic
9005	Port TCP utilisé pour la gestion de Jboss	Connexion localhost
9999	Port TCP utilisé pour la gestion de Jboss	Connexion localhost

Tableau 4 Paramètres de port de datastore DPA

Port	Description	Sens du trafic
3741	Port TCP utilisé pour les communications d'agents DPA.	Connexion entrante à partir du serveur d'applications DPA.
9002	Port TCP utilisé pour le service HTTPS.	Connexion sortante sur SSL sur le serveur d'applications DPA.
9003	Port TCP utilisé pour les communications de datastore DPA.	Connexion entrante à partir du serveur d'applications DPA.

Tableau 5 Paramètres de port de l'Agent DPA

Port	Description	Sens du trafic
3741	Port TCP utilisé pour les communications d'agents DPA.	Connexion entrante à partir du serveur d'applications DPA.
9002	Port TCP utilisé pour le service HTTPS.	Connexion sortante sur SSL sur le serveur d'applications DPA.

Tableau 6 Paramètres de port du cluster DPA

Port	Description	Sens du trafic
25	Port TCP utilisé pour le service SMTP	Connexion sortante au serveur SMTP.
80	Port TCP utilisé pour le service SharePoint	Connexion sortante vers le serveur SharePoint.
161	Port UDP utilisé pour le service SNMP	Connexion sortante vers les périphériques SNMP.
389/636 (sur SSL)	Port TCP utilisé pour l'intégration avec LDAP	Connexion sortante au serveur LDAP.
3741	Port TCP utilisé pour les communications d'agents DPA.	Connexion sortante aux agents DPA

Tableau 6 Paramètres de port du cluster DPA (suite)

Port	Description	Sens du trafic
4447	Port TCP utilisé pour les communications entre les services	Connexion entrante
4712	Port TCP utilisé pour les communications entre les services	Connexion localhost
4713	Port TCP utilisé pour les communications entre les services	Connexion localhost
5445	Port TCP utilisé pour les communications entre les services	Connexion bidirectionnelle du cluster
5455	Port TCP utilisé pour les communications entre les services	Connexion bidirectionnelle du cluster
7500	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster
7600	Multidiffusion sur TCP	Connexion entrante du cluster
8090	Port TCP utilisé pour les communications entre les services	Connexion localhost
9002	Port TCP utilisé pour le service HTTPS.	Connexion entrante sur SSL à partir de clients de l'interface utilisateur, de la CLI et de l'API REST.
9003	Port TCP utilisé pour les communications de datastore DPA.	Connexion sortante au datastore DPA.
9005	Port TCP utilisé pour la gestion de Jboss	Connexion localhost
9876	Multidiffusion sur TCP	Connexion bidirectionnelle du cluster
9999	Port TCP utilisé pour la gestion de Jboss	Connexion localhost
23364	Multidiffusion sur TCP	Connexion bidirectionnelle du cluster
45688	Multidiffusion sur TCP	Connexion bidirectionnelle du cluster
45689	Multidiffusion sur TCP	Connexion bidirectionnelle du cluster
45700	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster

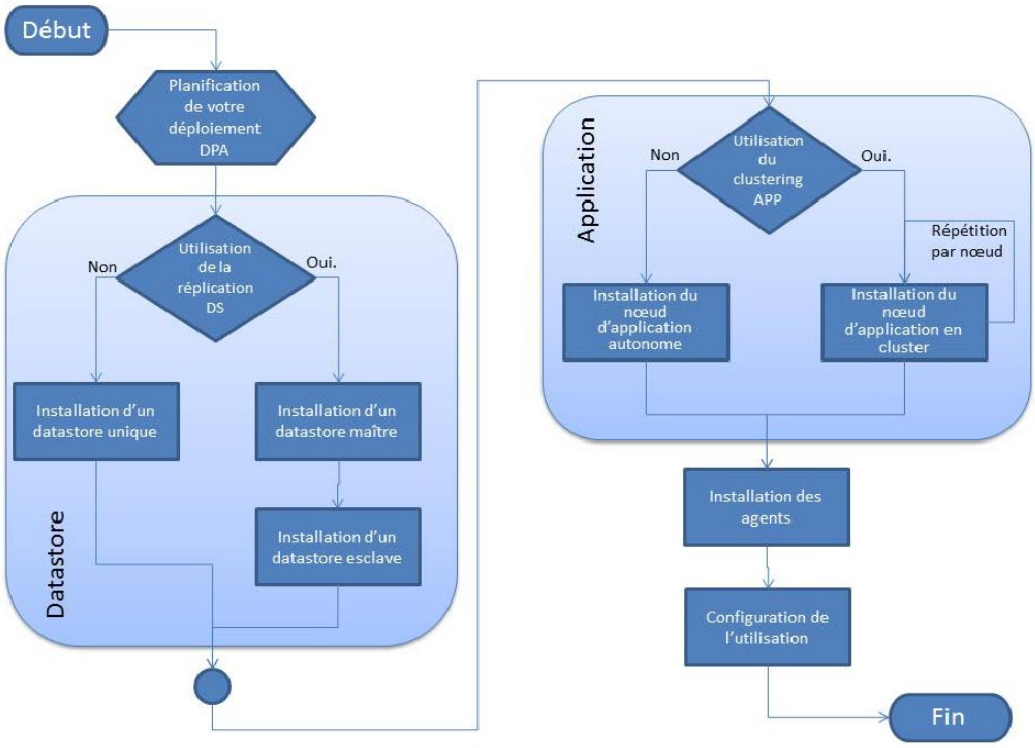
Tableau 6 Paramètres de port du cluster DPA (suite)

Port	Description	Sens du trafic
54200	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster
54201	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster
55200	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster
55201	Multidiffusion sur UDP	Connexion bidirectionnelle du cluster
57600	Multidiffusion sur TCP	Connexion bidirectionnelle du cluster

Présentation de l'installation et de la configuration

Le workflow d'installation de DPA fournit un workflow global des tâches pour l'installation de DPA avec diverses configurations.

Figure 2 Workflow d'installation d'DPA



La présentation de l'installation et de la configuration répertorie les tâches à effectuer pour installer DPA et paramétrer la surveillance des données.

Tableau 7 Présentation de l'installation et de la configuration

Action	Commentaires
Configuration de l'ordinateur hôte	
Définir au moins deux hôtes pour l'installation du serveur DPA : Un pour le serveur d'applications DPA initial et l'autre pour le serveur de datastore. Un hôte distinct est nécessaire pour le datastore et le serveur d'applications, afin que le système d'exploitation sur chaque serveur puisse gérer correctement les exigences de performances d'E/S d'un service et les exigences de RAM et de mémoire cache d'un autre service, sans que les deux services n'entrent en concurrence pour l'utilisation des ressources.	DPA ne doit pas être installé sur des serveurs qui exécutent déjà d'autres applications. Pour une installation dans un environnement de production, vous devez disposer d'un hôte pour le service d'application et d'un autre hôte pour le service de datastore. Nous recommandons d'utiliser un serveur dédié avec au moins 2 Go d'espace temporaire. Pour plus d'informations, consultez le Guide de compatibilité.
Définir un hôte pour l'installation de l'agent DPA (facultatif).	Si à la fois le serveur DPA et le ou les hôtes découverts s'exécutent sous Windows, il n'est pas nécessaire d'installer un agent sur l'hôte découvert. Cependant, nous vous recommandons d'utiliser l'agent installé sur les hôtes du serveur DPA, uniquement pour surveiller celui-ci. Si vous effectuez la découverte de clients d'hôtes Windows alors que le serveur DPA réside sur un hôte Linux, au moins un agent DPA doit être installé sur un agent Windows.
Assurez-vous que DPA et tous ses composants sont configurés comme étant des exceptions pour tous les logiciels antivirus.	S'ils ne sont pas définis comme exceptions, il peut arriver que des composants de DPA soient arrêtés ou que des fichiers associés soient mis en quarantaine par les logiciels antivirus.
Si vous installez plusieurs serveurs d'applications DPA (en cluster), provisionnez l'infrastructure réseau ainsi qu'un répertoire partagé.	• Attribuez un VLAN dédié à l'utilisation des serveurs d'applications DPA. Si aucun VLAN dédié n'est disponible, demandez à votre administrateur réseau une adresse de groupe multidiffusion UDP pouvant être utilisée pour le cluster DPA. • Pour augmenter la résilience et la qualité de service, prévoyez d'utiliser un répartiteur matériel d'équilibrage de charge pour servir de passerelle vers les serveurs d'applications DPA. • Configurez un répertoire partagé auquel tous les serveurs d'applications pourront accéder. DPA utilisera ce dossier partagé pour écrire les rapports planifiés et autres fichiers temporaires auxquels tous les

Tableau 7 Présentation de l'installation et de la configuration (suite)

Action	Commentaires
	serveurs d'applications ont besoin d'accéder.
Vérifier les exigences relatives à VMware ou Hyper-V.	DPA est certifié pour un fonctionnement sur une machine virtuelle Linux ou Windows dans un environnement VMware ou Hyper-V. Pour plus d'informations, consultez le Guide de compatibilité logicielle.
Configurer la mémoire virtuelle d'infrastructure et le CPU	Pour plus d'informations, reportez-vous à la section Configuration de la mémoire virtuelle d'infrastructure et du CPU à la page 18.
Ouvrir ou désactiver les pare-feu pour que la communication puisse s'effectuer entre les serveurs DPA.	Si vous souhaitez utiliser une communication sécurisée pour vous connecter au serveur d'applications sur le port 9002, assurez-vous que les paramètres TLS (Transport Layer Security) sont activés pour la communication sécurisée dans les paramètres de votre navigateur. En cas d'installation sur des serveurs DPA, les pare-feu logiciels ou du système d'exploitation peuvent être désactivés, ou des ports peuvent être ouverts pour permettre la communication entre le serveur d'applications DPA, le serveur datastore DPA et les agents DPA, avant d'installer les composants DPA. En général, le réseau sur lequel les serveurs DPA et les agents DPA résidents sont sécurisés et protégés par un pare-feu réseau. Cela signifie que vous pouvez désactiver les pare-feu logiciels ou du système d'exploitation. Si vous choisissez de laisser les pare-feu logiciels ou du système d'exploitation actifs, vous devez ouvrir ou déverrouiller les ports requis. Pour plus d'informations, reportez-vous à la section Paramètres de communication dans DPA à la page 19. Si vous êtes sous Linux, exécutez les commandes suivantes pour désactiver le pare-feu et vous assurer qu'il reste désactivé après démarrage ou redémarrage : • Exécutez **`iptables stop`**. • Configurez l'utilitaire `chkconfig` sur **`iptables off`**.
Installer le système d'exploitation hôte et tous les correctifs requis sur le ou les serveurs DPA et l'hôte de l'agent.	Le Guide de compatibilité logicielle répertorie les architectures et les correctifs requis.

Tableau 7 Présentation de l'installation et de la configuration (suite)

Action	Commentaires
Installer tous les logiciels requis sur l'hôte de l'agent une fois que la dernière version du serveur d'applications DPA est prête.	Pour la surveillance à distance d'applications ou de services, il vous faudra peut-être installer des logiciels complémentaires sur l'hôte de l'agent. Par exemple, le client NetWorker doit être installé sur l'hôte de l'agent si l'agent est utilisé ultérieurement pour la surveillance à distance de NetWorker. Pour plus d'informations, reportez-vous à la rubrique Découverte de l'environnement dans DPA à la page 167
Si le DNS n'est pas activé dans l'environnement, ajoutez l'adresse IP et le nom de domaine complet (FQDN) du serveur SharePoint dans le fichier hosts du serveur d'applications DPA.	L'intégration de DPA et de SharePoint nécessite l'adresse IP et le nom de domaine complet pour publier des rapports sur SharePoint et configurer le port de SharePoint. Le port SharePoint est configurable. Si aucun port n'est spécifié, le port par défaut est 80. Vous pouvez définir le port en utilisant une URL standard dans le champ URL existant dans la boîte de dialogue des paramètres de SharePoint. Paramètres système à la page 95, tableau des paramètres SharePoint, fournit des informations à ce sujet.
Si vous utilisez l'authentification utilisateur LDAP sur votre serveur DPA, rassemblez les informations nécessaires à la configuration	Pour configurer l'authentification utilisateur LDAP, vous avez besoin des informations suivantes : • Nom ou adresse IP du serveur LDAP • Utiliser SSL ? • Port du serveur LDAP • LDAP Version • Nom unique du répertoire de base • Attribut d'identification
Télécharger et enregistrer les fichiers binaires DPA	Pour télécharger les fichiers binaires du serveur DPA et de l'agent, accédez à la section des téléchargements DPA de http://support.emc.com. Enregistrez les fichiers binaires du serveur DPA et de l'agent localement.
Récupérer et enregistrer vos licences DPA	
Sauvegarder les fichiers de licence requis sur votre machine locale pour y accéder plus facilement au cours de l'installation. L'assistant d'installation DPA vous invite à rechercher le fichier de licence lors de l'installation de la licence.	Vous devez connaître l'adresse IP du serveur datastore principal. Pour plus d'informations sur l'obtention des licences DPA ou des types de licence DPA disponibles et requises, contactez votre responsable de compte.

Tableau 7 Présentation de l'installation et de la configuration (suite)

Action	Commentaires
• Pour les nouvelles installations non migrées, vous devez obtenir des licences DPA pour tous les composants que vous souhaitez surveiller. • Pour les installations 5.x migrées, les licences existantes seront migrées. • La licence CLP est requise pour la nouvelle fonctionnalité DPA et accroît la capacité sur une instance DPA. Si vous n'ajoutez pas de capacité ou n'optez pas pour la fonctionnalité de la nouvelle version de DPA, l'importation de licences CLP n'est pas nécessaire. Si vous migrez DPA de la version 5.x à DPA, les licences existantes font l'objet d'une migration en même temps que la configuration et les données. Si vous n'ajoutez pas de capacité ou si vous n'utilisez pas de nouvelles fonctionnalités avec des licences WLS existantes, celles-ci ne peuvent coexister avec des licences de type CLP si elles ont été importées avant ces dernières. Pour plus d'informations, reportez-vous à la section Coexistence de licences CLP et WLS dans DPA à la page 80.	Une licence DPA est requise pour gérer DPA après l'installation. DPA est fourni avec une licence d'évaluation de 90 jours. La licence d'évaluation est créée au moment de l'installation de DPA et est valable durant 90 jours maximum. Elle permet d'accéder à toutes les fonctions. Si vous importez une licence au cours de cette période d'évaluation de 90 jours, la licence d'évaluation est supprimée et votre accès aux fonctions de DPA dépend de la licence que vous avez importée. Pour obtenir des informations sur les licences DPA requises ou sur l'achat de licences pour votre installation DPA, contactez votre responsable de compte.
Fournir les licences Solutions Enabler (SE).	• Il est nécessaire de disposer d'au moins un volume système (gatekeeper) par adaptateur HBA Symmetrix. • Un hôte Solutions Enabler peut découvrir toutes les baies VNX/CLARiiON en utilisant une adresse IP. Pour la découverte VNX/CLARiiON, nous recommandons l'installation de Solutions Enabler sur le serveur DPA. • Le *guide de compatibilité logicielle* décrit les versions de Solutions Enabler requises pour la découverte de baies de stockage.
Installez DPA	
Installez le logiciel DPA.	Installez le serveur et l'agent DPA selon les instructions d'installation. Pour plus d'informations, reportez-vous à Installation du service de datastore à la page 32, Installation du service d'application à la page 34 et Installation de l'agent DPA à la page 57.
Configuration de la découverte de baies hôtes et des hôtes Solutions Enabler	

Tableau 7 Présentation de l'installation et de la configuration (suite)

Action	Commentaires
Configurer la découverte de baies Symmetrix et VNX/CLARiiON	Pour plus d'informations, reportez-vous à la section Configuration des baies de stockage pour l'analyse de la réplication à la page 206. Les opérations de cette section s'appliquent uniquement si vous surveillez une baie de stockage, une base de données ou un ordinateur Microsoft Exchange Server dans le cadre d'une analyse de réplication.
Indiquer l'hôte Solutions Enabler utilisé pour la découverte des baies de stockage Symmetrix ou VNX/CLARiiON.	Le *guide de compatibilité logicielle* décrit les versions de Solutions Enabler requises pour la découverte de baies de stockage, ainsi que les logiciels à installer sur l'hôte Solutions Enabler. L'hôte doit être en mesure de communiquer avec la baie Symmetrix par le biais d'une connexion SAN. Le port TCP 443 ou 2163 doit être activé sur l'hôte pour la connexion VNX/CLARiiON.
Configuration de l'environnement pour la surveillance de la protection des données	
S'assurer que les ports requis sont ouverts entre l'hôte de l'agent DPA et le serveur ou les périphériques surveillés et que la communication est possible par le biais du protocole choisi.	Le Paramètres de communication dans DPA à la page 19 dresse la liste des protocoles et des ports DPA par défaut requis pour la communication entre l'agent et le périphérique ou le serveur surveillé.
S'assurer que les données d'identification DPA utilisées pour se connecter au périphérique ou au serveur surveillé sont suffisantes ou que vous disposez des nouvelles données d'identification.	Le Autorisations à la page 17 répertorie les paramètres par défaut pour les données d'identification DPA installées avec DPA.
Configurer la surveillance de RecoverPoint (si nécessaire).	Les exigences relatives à l'hôte de l'agent RecoverPoint et à l'hôte d'application sont répertoriées dans le Surveillance de RecoverPoint à la page 206
Découvrir et configurer l'importation de l'hôte d'application (en cas de surveillance de Microsoft Exchange ou d'une base de données).	• Si un agent distant est utilisé pour l'importation des hôtes, le serveur DPA doit être en mesure de résoudre l'hôte de l'agent. • Pour plus d'informations si la découverte de l'application est effectuée sans agent, reportez-vous à la section Configuration pour l'analyse de réplication à la page 204.
Définition des règles de protection des données	
Préparer la configuration des règles sur lesquelles DPA s'appuiera pour surveiller la conformité.	Dans le cadre de l'analyse de réplication, les règles de protection des données comportent les informations suivantes :

Tableau 7 Présentation de l'installation et de la configuration (suite)

Action	Commentaires
	• Type de réplication (SRDF/S, SRDF/A, MirrorView, RecoverPoint, etc.). • Réplication à un point dans le temps ou continue. • Destination de la cible de réplication. Pour le reporting sur la protection de données, les règles sont les suivantes : • Règles de refacturation : pour l'analyse des coûts financiers d'opérations de protection des données. • Règles de rétention : pour l'analyse de la conformité avec les cibles de protection des données de l'objectif de temps de restauration (RTO) et de l'objectif de point de restauration (RPO). Pour plus d'informations, reportez-vous à la section Stratégies à la page 226.

CHAPITRE 2

Installation de DPA

Le présent chapitre contient les sections suivantes :

Installation du serveur DPA

L'installation du serveur DPA comprend deux étapes :

1. installation du service de datastore
2. installation du service d'application

Clustering des applications à la page 37 fournit des informations sur l'installation avec le clustering. Réplication de datastore à la page 49 fournit des informations sur l'installation avec la réplication du datastore.

Si le service d'application est installé avant le service datastore, l'installation du service d'application échoue. Si vous rencontrez des difficultés lors de l'installation, reportez-vous à la section Dépannage à la page 263.

Les procédures décrites dans cette section s'appliquent aux nouvelles installations. Pour les mises à niveau à partir d'anciennes versions prises en charge de DPA antérieures à DPA18.1, ainsi que pour installer la version 18.1, consultez Mises à niveau. Les notes de mise à jour DPA fournissent des informations sur les mises à niveau prises en charge.

Le programme d'installation de DPA s'exécute sous Windows et Linux, à condition que votre installation Linux prenne en charge l'exécution d'une interface utilisateur. Les procédures suivantes décrivent une installation dans un environnement Windows 64 bits.

Installation du service de datastore

Cette procédure inclut la mise en œuvre pour une installation normale de datastore sans clustering ni réplication du datastore.

Avant de commencer

- Connectez-vous en tant qu'administrateur local ou administrateur de domaine avec un accès local intégral.
- Si UAC est activé sur un hôte Windows, exécutez le programme d'installation via Exécuter en tant qu'administrateur.
- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Si vous effectuez l'installation sur UNIX/Linux, assurez-vous que vous vous êtes connecté en tant qu'utilisateur root. Des problèmes peuvent survenir au niveau du serveur de datastore si l'installation est effectuée après un passage au mode utilisateur root par l'intermédiaire de certains logiciels de sécurité de type SU (par exemple, à l'aide de la commande `sesu`).
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Si vous effectuez l'installation sur Linux IPv6, assurez-vous de disposer de l'ID de l'interface IPv6 du serveur de datastore. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du datastore. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur la machine de l'agent Linux et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

```
fe80::9c9b:36f:2ab:d7a2%2
```

Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) et celles placées après font référence à l'ID de l'interface (dans cet exemple, `2`).

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Si vous n'effectuez pas d'installation avancée, cliquez sur **Next**, puis suivez les consignes de l'assistant d'installation.

   Pour effectuer une installation avancée, cochez la case Show Advanced Installation Options dans l'écran Advanced Installation, puis cliquez sur Next et suivez les consignes de l'assistant d'installation.

   Les options avancées sont les suivantes :

   - **Do not register DPA services** : empêche l'enregistrement du service de datastore auprès du gestionnaire du système d'exploitation. Cette option évite un démarrage du service de datastore après le redémarrage de l'hôte. Vous devez utiliser l'interface de ligne de commande DPA pour installer le service avec le système d'exploitation.
   - **Do not start DPA services** : empêche le démarrage des services de datastore après l'installation. Il est nécessaire d'utiliser l'interface de ligne de commande DPA pour démarrer le service.
   - **Install with advanced datastore layout** : configure le service de datastore avec les systèmes de fichiers requis répartis sur différents disques afin d'optimiser les performances.
6. Lorsque vous y êtes invité, sélectionnez le dossier d'installation.

   Sélectionnez l'emplacement par défaut ou accédez à un autre emplacement de dossier.
7. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**.

   L'installation commence.

   S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.
8. À l'invite, sélectionnez les adresses IP que le datastore doit écouter pour repérer les connexions en provenance du ou des serveurs d'applications DPA.
9. À l'invite, saisissez l'adresse IP du serveur d'applications DPA qui va utiliser le datastore de l'étape 8, puis cliquez sur **Add** et **Next**.
10. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

    Notez les points suivants concernant le mot de passe du datastore :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.

- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial
- La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

11. Saisissez le mot de passe de l'agent DPA lorsque vous y êtes invité :

    Notez les points suivants concernant le mot de passe de l'agent :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
      - Un minimum de 1 lettre majuscule et 1 lettre minuscule
      - Un minimum de 1 caractère numérique
      - Un minimum de 1 caractère spécial
    - La commande dpa agent --set-credentials permet de réinitialiser le mot de passe de l'agent DPA. dpa agent --set-credentials fournit plus d'informations.

12. Une fois terminée l'installation du serveur de datastore DPA, cliquez sur **Done**.

Installation du service d'application

Cette procédure inclut la mise en œuvre pour une installation normale du service d'application sans clustering ni réplication du datastore.

Avant de commencer

- Pour garantir une communication sécurisée entre le serveur DPA et l'agent, définissez le mot de passe d'inscription de l'agent à l'aide de la commande de CLI `dpa app agentpwd` sur l'hôte de serveur d'applications DPA. Vous devez également définir ce mot de passe sur tous les hôtes d'agents DPA. dpa application agentpwd fournit des informations à ce sujet. Puis, redémarrez le service d'application. Veillez à configurer ce mot de passe pour chaque agent.
- Copiez le fichier binaire d'installation de l'agent sur le serveur ou sur votre machine locale.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous que l'option de service de datastore est sélectionnée et que le service de datastore est en cours d'exécution.
- Si l'installation a été effectuée avec les options avancées sur Linux IPv6, et que l'agent souhaite parler à un autre serveur d'applications ou répartiteur de charge, par exemple, dans le cas d'un cluster, assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du serveur d'applications. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr`

`show` sur le serveur d'applications et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

```
fe80::9c9b:36f:2ab:d7a2%2
```

Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications ou du répartiteur de charge auquel l'agent souhaite se connecter (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) ; celles placées après font référence à l'ID de l'interface du serveur d'applications en cours (`2` dans cet exemple).

- Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE.

Le processus d'installation du service d'application est similaire à celui du service de datastore.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Si vous n'effectuez pas d'installation avancée, cliquez sur **Next**, puis suivez les consignes de l'assistant d'installation.

   Les options avancées sont les suivantes :

   - **Do not register DPA services** : empêche l'enregistrement du service de datastore auprès du gestionnaire de service du système d'exploitation. Cette option évite un démarrage des services DPA après le redémarrage de l'hôte.
   - **Do not start DPA services** : empêche le démarrage des services DPA après l'installation. Il est nécessaire d'utiliser l'interface de ligne de commande DPA pour démarrer le service.
   - **Install the DPA services as clusterable** : configure le service DPA pour identifier et rejoindre tout cluster DPA actuel.

     La suite de l'installation se déroule comme pour le datastore.
6. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**. L'installation commence.

   S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.

Remarque

Une erreur d'échec de connexion au datastore peut se produire si les pare-feu nécessaires pour communiquer entre le serveur d'applications et le datastore ne sont pas ouverts. Paramètres de communication dans DPA à la page 19 fournit des informations à ce sujet.

7. Dans l'étape **Connect to Remote DPA Datastore**, saisissez l'adresse IP du serveur de datastore DPA préalablement installé.

   L'installation reprend.

8. À l'invite, spécifiez le nom ou l'adresse IP de l'hôte du serveur d'applications DPA avec lequel l'agent DPA va communiquer. Par défaut, l'Agent communique avec le serveur d'applications local avec l'adresse IP 127.0.0.1. Dans une configuration en cluster, fournissez l'adresse IP du répartiteur d'équilibrage de charge placé devant les serveurs d'applications. Cliquez sur **Next**.

   L'installation du service d'application DPA est maintenant terminée.

9. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

   Notez les points suivants concernant le mot de passe du datastore :

   - Les mots de passe vides ne sont pas pris en charge.
   - La longueur minimale est de 9 caractères.
   - Les critères suivants sont obligatoires :
     - Un minimum de 1 lettre majuscule et 1 lettre minuscule
     - Un minimum de 1 caractère numérique
     - Un minimum de 1 caractère spécial
   - Le dpa application dspassword configure le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa application dspassword à la page 149.

10. Lorsque vous y êtes invité, indiquez le mot de passe administrateur.

    Notez les points suivants concernant le mot de passe d'administrateur :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
      - Un minimum de 1 lettre majuscule et 1 lettre minuscule
      - Un minimum de 1 caractère numérique
      - Un minimum de 1 caractère spécial
    - La commande dpa app adminpassword peut être utilisée pour réinitialiser le mot de passe de l'administrateur DPA et pour activer le compte administrateur DPA lorsque le service de datastore DPA est opérationnel. dpa application adminpassword à la page 146 fournit plus d'informations à ce sujet.

11. Cliquez sur **Done**.

Une fois l'installation terminée, démarrez le serveur DPA et attribuez-lui une licence. Pour plus d'informations, reportez-vous à la section Procédure qui suit l'installation de DPA à la page 65.

Clustering des applications

DPA peut être défini dans une configuration en cluster avec plusieurs serveurs d'applications DPA fonctionnant avec un seul serveur de datastore DPA. Le clustering permet aux serveurs d'applications de démarrer de façon dynamique, de partager la charge applicative avec d'autres serveurs d'applications et d'être interrompus au fur et à mesure que la demande diminue.

Les serveurs d'applications en cluster offrent plusieurs avantages :

- résilience accrue
- équilibrage de la charge applicative lorsqu'elle est placée derrière un répartiteur de charge que vous fournissez ;
- possibilité de faire évoluer le déploiement DPA rapidement ;
- gestion des ressources écologique et flexible ;
- réduction des points uniques de défaillance.

Lorsque plusieurs serveurs d'applications sont configurés dans un cluster, vous pouvez démarrer et arrêter des serveurs d'applications individuels basés sur la charge. Par exemple, vous pouvez démarrer des serveurs supplémentaires pour le reporting de fin de mois ou d'autres périodes de forte utilisation. Vous pouvez ajouter de nouveaux serveurs aux clusters en cours d'exécution pour améliorer les performances en fonction de la charge.

Assurez-vous que tous les nœuds de cluster utilisent le même type IP d'adressage IP : les adresses IPv4 ou IPv6.

Vous pouvez configurer le clustering d'applications :

- lors d'une nouvelle installation ; Installer le service d'application maître avec clustering à la page 41 et Installation du service d'application esclave avec le clustering à la page 45 fournissent des informations.
- au cours d'une mise à niveau ; Mise à niveau des clusters existants à la page 74 et Mise à niveau avec la réplication de datastore et les clusters existants à la page 76 fournissent des informations supplémentaires.
- après l'installation et la configuration ; Ajout d'un serveur d'applications à un cluster après le déploiement DPA à la page 133 fournit plus d'informations.

Restrictions et recommandations pour la mise en cluster

Tenez compte des restrictions et des recommandations suivantes lorsque vous configurez des clusters :

- DPA prend en charge un maximum de quatre nœuds dans un cluster :
  - un maître
  - trois esclaves
- Chaque cluster de serveurs d'applications doit se trouver dans son propre LAN/VLAN
  - L'extension des réseaux LAN est impossible.

    - La mise en cluster est basée sur le protocole de diffusion UDP.
- Les clusters peuvent communiquer entre réseaux LAN avec le datastore.
- Un répartiteur physique d'équilibrage de charge doit être placé devant le cluster de serveurs d'applications pour gérer la charge entre les objets du serveur d'applications DPA. L'utilisation des répartiteurs d'équilibrage de charge du logiciel n'est pas recommandée.
- Toute configuration accessible via la console Web DPA est enregistrée dans le datastore et est accessible à l'échelle du cluster. Toute opération de configuration qui nécessite l'utilisation de l'utilitaire d'exécution dpa, telle que « dpa application promote », s'effectue localement sur l'objet sur lequel elle a été exécutée. Ajout d'un serveur d'applications à un cluster après le déploiement DPA à la page 133 et Commandes d'application dpa à la page 146 fournissent des informations sur la commande dpa application promote.
- Si vous mettez en œuvre le clustering des serveurs d'applications, assurez-vous d'avoir bien effectué la configuration du cluster avant d'activer le chiffrement sur les serveurs d'applications.

Installation du service de datastore avec clustering

Cette procédure inclut la mise en œuvre d'un cluster avec un répartiteur de charge, un datastore, un serveur d'applications maître et un ou plusieurs serveurs d'applications.

Avant de commencer

- Connectez-vous en tant qu'administrateur local ou administrateur de domaine avec un accès local intégral.
- Si UAC est activé sur un hôte Windows, exécutez le programme d'installation via Exécuter en tant qu'administrateur.
- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Si vous effectuez l'installation sur UNIX/Linux, assurez-vous que vous vous êtes connecté en tant qu'utilisateur root. Des problèmes peuvent survenir au niveau du serveur de datastore si l'installation est effectuée après un passage au mode utilisateur root par l'intermédiaire de certains logiciels de sécurité de type SU (par exemple, à l'aide de la commande `sesu`).
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous de créer un répertoire partagé commun pour les rapports qui est accessible depuis les nœuds d'application. Par exemple, sur Windows Cluster Datastore1 `\\WinClusterDS1\cluster_share`. Le répertoire partagé doit disposer d'autorisations de lecture/écriture pour les utilisateurs de ClusterApp1 et ClusterApp2 qui possèdent le service DPA.
- Assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Si vous effectuez l'installation sur Linux IPv6, assurez-vous de disposer de l'ID de l'interface IPv6 du serveur de datastore. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du datastore. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur la machine de l'agent Linux et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

```
fe80::9c9b:36f:2ab:d7a2%2
```

Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) et celles placées après font référence à l'ID de l'interface (dans cet exemple, `2`).

- Vérifiez que tous les ordinateurs sont sur la même carte réseau dans vCenter.
- Si vous installez la réplication du datastore :
  - Planifiez la topologie de déploiement finale avant de commencer l'installation. Des ressources supplémentaires sont disponibles sur EMC Community Network (ECN), et fournissent des recommandations ainsi que les bonnes pratiques pour planifier votre déploiement.
  - Prédéterminez tous les hôtes et toutes adresses IP et tenez-les à disposition.
  - Assurez-vous que le serveur de datastore ou le serveur d'applications dans son ensemble, y compris les nœuds de cluster, utilise le même type IP d'adressage IP : les adresses IPv4 ou IPv6.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Si vous n'effectuez pas d'installation avancée, cliquez sur **Next**, puis suivez les consignes de l'assistant d'installation.

   Pour effectuer une installation avancée, cochez la case Show Advanced Installation Options dans l'écran Advanced Installation, puis cliquez sur Next et suivez les consignes de l'assistant d'installation.

   Les options avancées sont les suivantes :

   - **Do not register DPA services** : empêche l'enregistrement du service de datastore auprès du gestionnaire du système d'exploitation. Cette option évite un démarrage du service de datastore après le redémarrage de l'hôte. Vous devez utiliser l'interface de ligne de commande DPA pour installer le service avec le système d'exploitation.
   - **Do not start DPA services** : empêche le démarrage des services de datastore après l'installation. Il est nécessaire d'utiliser l'interface de ligne de commande DPA pour démarrer le service.
   - **Install with advanced datastore layout** : configure le service de datastore avec les systèmes de fichiers requis répartis sur différents disques afin d'optimiser les performances.

     Le fait de sélectionner Advanced Installation Options vous permet également de configurer la réplication du datastore et de sélectionner par la suite un rôle de réplication pour ce serveur, dans le programme d'installation.
6. Lorsque vous y êtes invité, sélectionnez le dossier d'installation.

   Sélectionnez l'emplacement par défaut ou accédez à un autre emplacement de dossier.
7. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**.

   L'installation commence.

S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.

8. Dans la fenêtre **Datastore Listening Addresses**, spécifiez les adresses IP que le service de datastore doit écouter pour repérer les connexions à partir des services d'application DPA.
9. Dans la fenêtre **Configure Datastore Access**, saisissez les adresses IP des serveurs d'applications DPA qui utiliseront le datastore, puis cliquez sur **Add** et **Next**.

   Saisissez les adresses IP pour chaque serveur d'applications DPA dans la configuration en cluster.

10. Dans la fenêtre **Datastore Agent Address**, spécifiez l'adresse de substitution pour l'agent de datastore comme adresse IP du répartiteur de charge.
11. Si vous configurez la réplication du datastore, sélectionnez **Enable datastore replication** > **puis le rôle de réplication pour ce serveur** > **SLAVE**. Cliquez sur **Next**.
    a. Indiquez l'adresse IP ou le nom de domaine complet du serveur de datastore maître.
    b. Lorsque vous y êtes invité dans la fenêtre **Configure Agent**, saisissez le nom de domaine complet ou l'adresse IP du service d'application DPA avec lequel/laquelle l'agent DPA installé doit communiquer.

       Par défaut, l'agent communique avec le serveur d'applications spécifié précédemment dans l'assistant.

    c. Si vous travaillez dans un environnement Linux IPv6, saisissez le nom de domaine complet/l'adresse IP du répartiteur de charge au format suivant : `IPV6Address%Interface_Id`

       Cliquez sur **Next**.
12. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

    Notez les points suivants concernant le mot de passe du datastore :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
      - Un minimum de 1 lettre majuscule et 1 lettre minuscule
      - Un minimum de 1 caractère numérique
      - Un minimum de 1 caractère spécial
    - La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

13. Une fois terminée l'installation du serveur de datastore DPA, cliquez sur **Done**.
14. À l'invite de commande, exécutez la commande `dpa svc status` pour vérifier que le service de datastore est en cours d'exécution.
15. Définissez la taille du pool de connexions à la base de données dans tous les nœuds du datastore. Exécutez :

 # dpa ds tune --connections xxx <RAM>GB où *xxx* représente environ 250 pour chaque serveur d'applications et *RAM* représente la quantité de RAM. Par exemple, vous utiliseriez *xxx* 500 pour un cluster à deux nœuds.

Si le cluster est activé pour la réplication de datastore, exécutez cette commande pour tous les datastores esclaves.

Installer le service d'application maître avec clustering

Avant de commencer

- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous que le service datastore est actif.
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Si l'installation a été effectuée avec les options avancées sur Linux IPv6, et que l'agent souhaite parler à un autre serveur d'applications ou répartiteur de charge, par exemple, dans le cas d'un cluster, assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du serveur d'applications. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur le serveur d'applications et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications ou du répartiteur de charge auquel l'agent souhaite se connecter (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) ; celles placées après font référence à l'ID de l'interface du serveur d'applications en cours (`2` dans cet exemple).
- Planifiez la topologie de déploiement finale avant de commencer l'installation. Des ressources supplémentaires sont disponibles sur EMC Community Network (ECN), et fournissent des recommandations ainsi que les bonnes pratiques pour planifier votre déploiement.
- Prédéterminez tous les hôtes et toutes les adresses IP et tenez-les à disposition, y compris l'adresse IP configurée pour le répartiteur d'équilibrage de charge qui sera placé devant les serveurs d'applications.
- Assurez-vous que tous les nœuds de cluster utilisent le même type IP d'adressage IP : les adresses IPv4 ou IPv6.
- Spécifiez un répertoire commun qui est partagé par tous les nœuds. Il s'agit de l'emplacement du dossier dans lequel les rapports générés par le nœud d'application DPA sont stockés.
- Si vous installez le clustering de serveurs d'applications sous UNIX, veillez à spécifier le répertoire partagé commun dans un répertoire local mappé vers un partage réseau NFS ou CIFS UNIX.
  - Vérifiez que vous avez créé un nom d'utilisateur dans tous les nœuds d'application au sein du cluster avec les mêmes ID d'utilisateur et ID de groupe. Lors de l'installation, vous êtes invité à vous connecter avec un nom

d'utilisateur et un mot de passe UNIX valides. Les utilisateurs du système comme ftpuser et bin ne peuvent pas être utilisés.

- Assurez-vous de disposer d'un accès en lecture et en écriture sur le répertoire partagé que vous avez spécifié.
- Veillez à valider le chemin s'il est rattaché à un partage réseau.

- Si vous installez le clustering de serveurs d'applications sous Windows, veillez à spécifier le répertoire partagé commun comme un chemin UNC (Windows *Universal Naming Convention*).
  - Veillez à valider le chemin spécifié.
  - Configurez et accordez un accès en lecture et en écriture à un compte utilisateur (nom d'utilisateur et mot de passe) pour le partage que vous avez spécifié ci-dessus. Ce compte utilisateur doit disposer de droits **Log on as a service** de Windows actifs.
- Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE.

Le processus d'installation du service d'application est similaire à celui du service de datastore.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next.**
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Assurez-vous que **Show Advanced Installation Options** est activé, puis cliquez sur **Next**.

   Les options avancées sont les suivantes :

   - **Do not register DPA services** : empêche l'enregistrement du service de datastore auprès du gestionnaire de service du système d'exploitation. Cette option évite un démarrage des services DPA après le redémarrage de l'hôte.
   - **Do not start DPA services** : empêche le démarrage des services DPA après l'installation. Il est nécessaire d'utiliser l'interface de ligne de commande DPA pour démarrer le service.
   - **Install the DPA services as clusterable** : configure le service DPA pour identifier et rejoindre tout cluster DPA actuel.

     Pour ajouter un objet d'application à un cluster, sélectionnez Install the DPA services as clusterable et suivez les consignes de l'assistant d'installation.

     Lorsque vous êtes invité à indiquer un emplacement commun pour les rapports des serveurs d'applications, veillez à spécifier un répertoire commun qui est partagé par tous les nœuds. Un répertoire partagé pour stocker les rapports est requis lorsque vous exécutez plusieurs nœuds d'application.

Si vous effectuez l'installation sur UNIX, le programme d'installation vous invite à spécifier le nom d'utilisateur d'un compte associé à un utilisateur valide qui dispose d'un accès en lecture et en écriture au partage spécifié dans la section « Avant de commencer ».

Si vous effectuez l'installation sur Windows, veillez à configurer le dossier UNC partagé et commun requis et saisissez le nom d'utilisateur et le mot de passe de domaine disposant d'un accès au répertoire spécifié. Pour plus d'informations, reportez-vous à la section « Avant de commencer ».

La suite de l'installation se déroule comme pour le datastore.

6. Dans la fenêtre **Application Advanced Options**, assurez-vous que **Install the DPA services as clusterable** est activé, puis cliquez sur **Next**.
7. Dans la fenêtre Identify the DPA Datastore to connect to, spécifiez l'adresse IP du datastore, puis cliquez sur **Next**.
8. Dans la fenêtre **Application Cluster Address**, sélectionnez l'adresse IP que le serveur d'applications souhaite écouter et cliquez sur **Next**.
9. Dans la fenêtre **Application Cluster Options**, sélectionnez le rôle d'application **Master** dans le menu déroulant, puis cliquez sur **Next**.
10. Dans la fenêtre **Choose a Folder**, spécifiez le dossier partagé que vous souhaitez utiliser pour le reporting, puis cliquez sur **Next**.
11. Dans la fenêtre **Usernamer**, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur qui sera désormais propriétaire du service DPA. Cliquez sur le bouton **Next**.

    Assurez-vous que l'utilisateur dispose d'autorisations de lecture/écriture sur le dossier partagé spécifié dans l'étape 11.

    Si c'est un domaine, le nom d'utilisateur doit être au format suivant : <Domain \User>. S'il se n'agit pas d'un domaine, le nom d'utilisateur doit être au format : <HOSTNAME\User>.
12. Dans la fenêtre **Enter Alternative Agent Address**, spécifiez l'adresse d'agent de substitution comme adresse IP du répartiteur de charge, puis cliquez sur **Next**.
13. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**. L'installation commence.

    S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.

Remarque

Une erreur d'échec de connexion au datastore peut se produire si les pare-feu nécessaires pour communiquer entre le serveur d'applications et le datastore ne sont pas ouverts. Paramètres de communication dans DPA à la page 19 fournit des informations à ce sujet.

---

14. Dans l'étape **Connect to Remote DPA Datastore**, saisissez l'adresse IP du serveur de datastore DPA préalablement installé.

    L'installation reprend.
15. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

    Notez les points suivants concernant le mot de passe du datastore :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial
- La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

16. Lorsque vous y êtes invité, indiquez le mot de passe administrateur.

    Notez les points suivants concernant le mot de passe d'administrateur :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
      - Un minimum de 1 lettre majuscule et 1 lettre minuscule
      - Un minimum de 1 caractère numérique
      - Un minimum de 1 caractère spécial
    - La commande dpa app adminpassword peut être utilisée pour réinitialiser le mot de passe de l'administrateur DPA et pour activer le compte administrateur DPA lorsque le service de datastore DPA est opérationnel. dpa application adminpassword à la page 146 fournit plus d'informations à ce sujet.

17. Cliquez sur **Done**.

    Une fois l'installation terminée, démarrez le serveur DPA et attribuez-lui une licence. Procédure qui suit l'installation de DPA à la page 65 fournit plus d'informations à ce sujet.

18. À l'invite de commande, exécutez la commande `dpa app con` pour vérifier la configuration du serveur d'applications.

    Vous remarquerez peut-être qu'après avoir exécuté la commande `dpa app con`, l'adresse de liaison est définie sur 0.0.0.0. DPA procède ainsi pour autoriser toutes les adresses de connexion.

    Le résultat doit indiquer que le mode de fonctionnement est cluster et que le rôle du cluster est Maître.

19. Si vous ajoutez une adresse multidiffusion au cluster, reléguez le cluster sur autonome, puis passez-le en nœud du cluster :

    Si vous n'ajoutez pas d'adresse multidiffusion au cluster, passez à l'étape 19.

    a. À l'invite de commande, exécutez la commande `dpa app stop` pour arrêter le serveur d'applications.

    b. Exécutez la commande `dpa app demote` pour reléguer le nœud en nœud autonome.

    c. Exécutez la commande `dpa app promote` afin de promouvoir le nœud d'application en cluster. Assurez-vous d'inclure l'adresse de liaison, l'adresse

multidiffusion et le chemin d'accès du dossier partagé. Veillez également à spécifier le rôle.

20. À l'invite de commande, exécutez la commande `dpa app start` pour démarrer le service d'application.
21. Vérifiez la justesse de l'installation et de la configuration dans le fichier `server.log` pour le message `DPA master started successfully`.

Installation du service d'application esclave avec le clustering

Avant de commencer

- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous que le service datastore est actif.
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Si l'installation a été effectuée avec les options avancées sur Linux IPv6, et que l'agent souhaite parler à un autre serveur d'applications ou répartiteur de charge, par exemple, dans le cas d'un cluster, assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du serveur d'applications. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur le serveur d'applications et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications ou du répartiteur de charge auquel l'agent souhaite se connecter (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) ; celles placées après font référence à l'ID de l'interface du serveur d'applications en cours (`2` dans cet exemple).
- Planifiez la topologie de déploiement finale avant de commencer l'installation. Des ressources supplémentaires sont disponibles sur EMC Community Network (ECN), et fournissent des recommandations ainsi que les bonnes pratiques pour planifier votre déploiement.
- Prédéterminez tous les hôtes et toutes les adresses IP et tenez-les à disposition, y compris l'adresse IP configurée pour le répartiteur d'équilibrage de charge qui sera placé devant les serveurs d'applications.
- Assurez-vous que tous les nœuds de cluster utilisent le même type IP d'adressage IP : les adresses IPv4 ou IPv6.
- Spécifiez un répertoire commun qui est partagé par tous les nœuds. Il s'agit de l'emplacement du dossier dans lequel les rapports générés par le nœud d'application DPA sont stockés.
- Si vous installez le clustering de serveurs d'applications sous UNIX, veillez à spécifier le répertoire partagé commun dans un répertoire local mappé vers un partage réseau NFS ou CIFS UNIX.

- Vérifiez que vous avez créé un nom d'utilisateur dans tous les nœuds d'application au sein du cluster avec les mêmes ID d'utilisateur et ID de groupe. Lors de l'installation, vous êtes invité à vous connecter avec un nom d'utilisateur et un mot de passe UNIX valides. Les utilisateurs du système comme ftpuser et bin ne peuvent pas être utilisés.
- Assurez-vous de disposer d'un accès en lecture et en écriture sur le répertoire partagé que vous avez spécifié.
- Veillez à valider le chemin s'il est rattaché à un partage réseau.

- Si vous installez le clustering de serveurs d'applications sous Windows, veillez à spécifier le répertoire partagé commun comme un chemin UNC (Windows *Universal Naming Convention*).
  - Veillez à valider le chemin spécifié.
  - Configurez et accordez un accès en lecture et en écriture à un compte utilisateur (nom d'utilisateur et mot de passe) pour le partage que vous avez spécifié ci-dessus. Ce compte utilisateur doit disposer de droits **Log on as a service** de Windows actifs.
- Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE.

Le processus d'installation du service d'application est similaire à celui du service de datastore.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next.**
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Assurez-vous que **Show Advanced Installation Options** est activé, puis cliquez sur **Next**.

   Les options avancées sont les suivantes :

   - **Do not register DPA services** : empêche l'enregistrement du service de datastore auprès du gestionnaire de service du système d'exploitation. Cette option évite un démarrage des services DPA après le redémarrage de l'hôte.
   - **Do not start DPA services** : empêche le démarrage des services DPA après l'installation. Il est nécessaire d'utiliser l'interface de ligne de commande DPA pour démarrer le service.
   - **Install the DPA services as clusterable** : configure le service DPA pour identifier et rejoindre tout cluster DPA actuel.

     Pour ajouter un objet d'application à un cluster, sélectionnez Install the DPA services as clusterable et suivez les consignes de l'assistant d'installation.

     Lorsque vous êtes invité à indiquer un emplacement commun pour les rapports des serveurs d'applications, veillez à spécifier un répertoire commun qui est partagé par tous les nœuds. Un répertoire partagé pour

stocker les rapports est requis lorsque vous exécutez plusieurs nœuds d'application.

Si vous effectuez l'installation sur UNIX, le programme d'installation vous invite à spécifier le nom d'utilisateur d'un compte associé à un utilisateur valide qui dispose d'un accès en lecture et en écriture au partage spécifié dans la section « Avant de commencer ».

Si vous effectuez l'installation sur Windows, veillez à configurer le dossier UNC partagé et commun requis et saisissez le nom d'utilisateur et le mot de passe de domaine disposant d'un accès au répertoire spécifié. Pour plus d'informations, reportez-vous à la section « Avant de commencer ».

La suite de l'installation se déroule comme pour le datastore.

6. Dans la fenêtre **Application Advanced Options**, assurez-vous que **Install the DPA services as clusterable** est activé, puis cliquez sur **Next**.
7. Dans la fenêtre Identify the DPA Datastore to connect to, spécifiez l'adresse IP du datastore, puis cliquez sur **Next**.
8. Dans la fenêtre **Application Cluster Address**, sélectionnez l'adresse IP que le serveur d'applications souhaite écouter et cliquez sur **Next**.
9. Dans la fenêtre **Application Cluster Options**, sélectionnez le rôle d'application **Slave** dans le menu déroulant et cliquez sur **Next**.
10. Dans la fenêtre **Application Cluster Option**, spécifiez l'adresse IP du nœud maître ou le nom de domaine complet avec lequel l'esclave doit communiquer, puis cliquez sur **Next**.
11. Dans la fenêtre **Usernamer**, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur qui sera désormais propriétaire du service DPA. Cliquez sur le bouton **Next**.

    Assurez-vous que l'utilisateur dispose d'autorisations de lecture/écriture sur le dossier partagé spécifié dans l'étape 10.

    Si c'est un domaine, le nom d'utilisateur doit être au format suivant : <Domain \User>. S'il se n'agit pas d'un domaine, le nom d'utilisateur doit être au format : <HOSTNAME\User>.
12. Dans la fenêtre **Enter Alternative Agent Address**, spécifiez l'adresse d'agent de substitution comme adresse IP du répartiteur de charge, puis cliquez sur **Next**.
13. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**. L'installation commence.

    S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.

Remarque

Une erreur d'échec de connexion au datastore peut se produire si les pare-feu nécessaires pour communiquer entre le serveur d'applications et le datastore ne sont pas ouverts. Paramètres de communication dans DPA à la page 19 fournit des informations à ce sujet.

---

14. Dans l'étape **Connect to Remote DPA Datastore**, saisissez l'adresse IP du serveur de datastore DPA préalablement installé.

    L'installation reprend.

15. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

    Notez les points suivants concernant le mot de passe du datastore :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
        - Un minimum de 1 lettre majuscule et 1 lettre minuscule
        - Un minimum de 1 caractère numérique
        - Un minimum de 1 caractère spécial
    - La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

16. Lorsque vous y êtes invité, indiquez le mot de passe administrateur.

    Notez les points suivants concernant le mot de passe d'administrateur :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
        - Un minimum de 1 lettre majuscule et 1 lettre minuscule
        - Un minimum de 1 caractère numérique
        - Un minimum de 1 caractère spécial
    - La commande dpa app adminpassword peut être utilisée pour réinitialiser le mot de passe de l'administrateur DPA et pour activer le compte administrateur DPA lorsque le service de datastore DPA est opérationnel. dpa application adminpassword à la page 146 fournit plus d'informations à ce sujet.

17. Cliquez sur **Done**.

    Une fois l'installation terminée, démarrez le serveur DPA et attribuez-lui une licence. Procédure qui suit l'installation de DPA à la page 65 fournit plus d'informations à ce sujet.

18. À l'invite de commande, exécutez la commande `dpa app con` pour vérifier la configuration du serveur d'applications.

    Le résultat doit indiquer que le mode de fonctionnement est cluster et que le rôle du cluster est Slave.

19. Si vous ajoutez une adresse multidiffusion au cluster, reléguez le cluster sur autonome, puis passez-le en nœud du cluster :

    Si vous n'ajoutez pas d'adresse multidiffusion au cluster, passez à l'étape 19.

    a. À l'invite de commande, exécutez la commande `dpa app stop` pour arrêter le serveur d'applications.

    b. Exécutez la commande `dpa app demote` pour reléguer le nœud en nœud autonome.

    c. Exécutez la commande `dpa app promote` afin de promouvoir le nœud d'application en cluster. Assurez-vous d'inclure l'adresse de liaison, l'adresse multidiffusion et le chemin d'accès du dossier partagé. Assurez-vous

également que vous spécifiez le rôle d'esclave et l'adresse IP du nœud principal. Par exemple :

```
dpa app promote --bind 10.10.211.212 --multicast 210.1.2.33 --
role SLAVE 10.10.211.213 --path \\WinClusterDS1\cluster_share
```

20. À l'invite de commande, exécutez la commande `dpa app start` pour démarrer le service d'application.
21. Vérifiez la justesse de l'installation et de la configuration dans le fichier `server.log` pour le message `DPA slave started successfully`.

Réplication de datastore

La réplication du datastore DPA permet d'effectuer des réplications continues, sécurisées et fiables pour que DPA puisse conserver une copie, ou *Slave*, du datastore principal, ou *Master*, à des fins de résilience, en cas de point unique de défaillance. Vous pouvez ajouter des esclaves supplémentaires en cascade à la configuration maître/esclave standard, si nécessaire.

Dans l'éventualité d'une défaillance du datastore maître, il est possible de mettre à jour l'esclave pour qu'il adopte le rôle de maître avec la commande manuelle de basculement sur incident. Les serveurs d'application sont alors configurés pour utiliser ce nouveau maître. La durée de la reconfiguration et celle du démarrage des services datastore et d'application DPA sont normalement similaires. Pour plus d'informations, reportez-vous à la section Réalisation d'un basculement sur incident du serveur datastore à la page 139.

Il ne peut exister qu'un seul datastore maître par déploiement. Tous les datastores sont maîtres lors de l'installation. La réplication est activée dès lors qu'un datastore esclave peut communiquer avec le datastore maître. La réplication des données débute au démarrage d'un serveur d'application.

Vous pouvez configurer la réplication du datastore :

- au cours d'une nouvelle installation, Installing the Master Datastore Service with Datastore Replication et Installing the Slave Datastore Service with Datastore Replication fournissent des informations.
- au cours d'une mise à niveau ; Mise à niveau avec activation de la réplication du datastore pour DPA 6.3 et les versions plus récentes à la page 75 et Mise à niveau avec la réplication de datastore et les clusters existants à la page 76 fournissent des informations.
- après l'installation et le déploiement ; Configuration de la réplication du datastore après déploiement à la page 137 fournit plus d'informations.

Assurez-vous que tous les nœuds du datastore utilisent le même type d'IP pour l'adressage IP, c'est-à-dire soit des adresses IPv4, soit des adresses IPv6.

Configuration de la réplication du datastore

Procédure

1. Configurez le datastore esclave, pendant ou après l'installation.
2. Configurez le datastore maître, pendant ou après l'installation.
3. Installez si besoin le serveur d'applications et démarrez-le.

Installer le service de datastore maître avec la réplication du datastore

Cette procédure inclut la mise en œuvre de l'installation d'un datastore maître avec réplication du datastore.

Avant de commencer

- Connectez-vous en tant qu'administrateur local ou administrateur de domaine avec un accès local intégral.
- Si UAC est activé sur un hôte Windows, exécutez le programme d'installation via Exécuter en tant qu'administrateur.
- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Si vous effectuez l'installation sur UNIX/Linux, assurez-vous que vous vous êtes connecté en tant qu'utilisateur root. Des problèmes peuvent survenir au niveau du serveur de datastore si l'installation est effectuée après un passage au mode utilisateur root par l'intermédiaire de certains logiciels de sécurité de type SU (par exemple, à l'aide de la commande `sesu`).
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Si vous effectuez l'installation sur Linux IPv6, assurez-vous de disposer de l'ID de l'interface IPv6 du serveur de datastore. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du datastore. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur la machine de l'agent Linux et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) et celles placées après font référence à l'ID de l'interface (dans cet exemple, `2`).
- Planifiez la topologie de déploiement de réplication de datastore finale avant de commencer l'installation. Des ressources supplémentaires sont disponibles sur EMC Community Network (ECN), et fournissent des recommandations ainsi que les bonnes pratiques pour planifier votre déploiement.
- Prédéterminez tous les hôtes et toutes adresses IP et tenez-les à disposition.
- Assurez-vous que le serveur de datastore ou le serveur d'applications dans son ensemble, y compris les nœuds de cluster, utilise le même type IP d'adressage IP : les adresses IPv4 ou IPv6.
- Assurez-vous que le serveur d'applications sélectionné est le même que celui qu'utilise le datastore maître.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.

5. Cochez la case **Show Advanced Installation Options** dans l'écran **Advanced Installation**, puis cliquez sur **Next**.
6. Sélectionnez **Install with advanced datastore layout**, puis cliquez sur **Next**.
7. Lorsque vous y êtes invité, sélectionnez le dossier d'installation.

   Sélectionnez l'emplacement par défaut ou accédez à un autre emplacement de dossier.
8. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**.

   L'installation commence.

   S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.
9. Dans la fenêtre **Datastore Listening Addresses**, spécifiez les adresses IP que le service de datastore doit écouter pour repérer les connexions à partir des services d'application DPA.
10. Dans la fenêtre **Configure Datastore Access**, saisissez les adresses IP des serveurs d'applications DPA qui utiliseront le datastore, puis cliquez sur **Add** et **Next**.

    Saisissez les adresses IP pour chaque serveur d'applications DPA dans la configuration en cluster.
11. Dans la fenêtre **Datastore Agent Address**, spécifiez l'adresse de substitution pour l'agent de datastore comme adresse IP du répartiteur de charge.
12. Sélectionnez **Enable datastore replication** > **puis le rôle de réplication pour ce serveur** > **SLAVE**. Cliquez sur **Next**.
    a. Indiquez l'adresse IP ou le nom de domaine complet du serveur de datastore maître.
    b. Lorsque vous y êtes invité dans la fenêtre **Configure Agent**, saisissez le nom de domaine complet ou l'adresse IP du service d'application DPA avec lequel/laquelle l'agent DPA installé doit communiquer.

       Par défaut, l'agent communique avec le serveur d'applications spécifié précédemment dans l'assistant.
    c. Si vous utilisez des serveurs d'applications DPA en cluster, spécifiez le nom de domaine complet/l'adresse IP du répartiteur de charge. Indiquez l'adresse IPV6 du serveur d'applications/répartiteur de charge au format suivant : `IPV6Address%Interface_Id`

       La valeur par défaut du nom de domaine complet/adresse IP reste vide dans le cas d'un cluster et lorsque vous utilisez un serveur d'applications Linux IPv6 ou des serveurs d'applications DPA en cluster, car la valeur IPV6%Interface_Id doit être saisie manuellement. Dans tous les autres cas, le nom de domaine complet/l'adresse IP est automatiquement défini(e) sur la valeur par défaut de l'adresse IP du serveur d'applications.

       Cliquez sur **Next**.
13. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

    Notez les points suivants concernant le mot de passe du datastore :

    - Les mots de passe vides ne sont pas pris en charge.

- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial
- La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

14. Une fois terminée l'installation du serveur de datastore DPA, cliquez sur **Done**.
15. À l'invite de commande, exécutez la commande `dpa svc status` pour vérifier que le service de datastore est en cours d'exécution.
16. Définissez la taille du pool de connexions à la base de données dans tous les nœuds du datastore. Exécutez :

    `# dpa ds tune --connections xxx <RAM>GB` où *xxx* représente environ 250 pour chaque serveur d'applications et *RAM* représente la quantité de RAM. Par exemple, vous utiliseriez *xxx* 500 pour un cluster à deux nœuds.

    Si le cluster est activé pour la réplication de datastore, exécutez cette commande pour tous les datastores esclaves.

Installer le service de datastore esclave avec la réplication du datastore

Cette procédure inclut la mise en œuvre de l'installation d'un datastore esclave avec réplication du datastore.

Avant de commencer

- Connectez-vous en tant qu'administrateur local ou administrateur de domaine avec un accès local intégral.
- Si UAC est activé sur un hôte Windows, exécutez le programme d'installation via Exécuter en tant qu'administrateur.
- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Si vous effectuez l'installation sur UNIX/Linux, assurez-vous que vous vous êtes connecté en tant qu'utilisateur root. Des problèmes peuvent survenir au niveau du serveur de datastore si l'installation est effectuée après un passage au mode utilisateur root par l'intermédiaire de certains logiciels de sécurité de type SU (par exemple, à l'aide de la commande `sesu`).
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Si vous effectuez l'installation sur Linux IPv6, assurez-vous de disposer de l'ID de l'interface IPv6 du serveur de datastore. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du datastore. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur la machine de l'agent Linux et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

```
fe80::9c9b:36f:2ab:d7a2%2
```

Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) et celles placées après font référence à l'ID de l'interface (dans cet exemple, `2`).

- Planifiez la topologie de déploiement de réplication de datastore finale avant de commencer l'installation. Des ressources supplémentaires sont disponibles sur EMC Community Network (ECN), et fournissent des recommandations ainsi que les bonnes pratiques pour planifier votre déploiement.
- Prédéterminez tous les hôtes et toutes adresses IP et tenez-les à disposition.
- Assurez-vous que le serveur de datastore ou le serveur d'applications dans son ensemble, y compris les nœuds de cluster, utilise le même type IP d'adressage IP : les adresses IPv4 ou IPv6.
- Assurez-vous que le serveur d'applications sélectionné est le même que celui qu'utilise le datastore maître.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran Installation Options, sélectionnez l'option d'installation du service de datastore, puis cliquez sur **Next**.
5. Cochez la case **Show Advanced Installation Options** dans l'écran **Advanced Installation**, puis cliquez sur **Next**.
6. Sélectionnez **Install with advanced datastore layout**, puis cliquez sur **Next**.
7. Lorsque vous y êtes invité, sélectionnez le dossier d'installation.

   Sélectionnez l'emplacement par défaut ou accédez à un autre emplacement de dossier.
8. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**.

   L'installation commence.

   S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.
9. Dans la fenêtre **Datastore Listening Addresses**, spécifiez les adresses IP que le service de datastore doit écouter pour repérer les connexions à partir des services d'application DPA.
10. Dans la fenêtre **Configure Datastore Access**, saisissez les adresses IP des serveurs d'applications DPA qui utiliseront le datastore, puis cliquez sur **Add** et **Next**.

    Saisissez les adresses IP pour chaque serveur d'applications DPA dans la configuration en cluster.
11. Dans la fenêtre **Datastore Agent Address**, spécifiez l'adresse de substitution pour l'agent de datastore comme adresse IP du répartiteur de charge.
12. Sélectionnez **Enable datastore replication** > **puis le rôle de réplication pour ce serveur** > **SLAVE**. Cliquez sur **Next**.
    a. Indiquez l'adresse IP ou le nom de domaine complet du serveur de datastore maître.

b. Lorsque vous y êtes invité dans la fenêtre **Configure Agent**, saisissez le nom de domaine complet ou l'adresse IP du service d'application DPA avec lequel/laquelle l'agent DPA installé doit communiquer.

   Par défaut, l'agent communique avec le serveur d'applications spécifié précédemment dans l'assistant.

c. Si vous utilisez des serveurs d'applications DPA en cluster, spécifiez le nom de domaine complet/l'adresse IP du répartiteur de charge. Indiquez l'adresse IPV6 du serveur d'applications/répartiteur de charge au format suivant : **`IPV6Address%Interface_Id`**

   La valeur par défaut du nom de domaine complet/adresse IP reste vide dans le cas d'un cluster et lorsque vous utilisez un serveur d'applications Linux IPv6 ou des serveurs d'applications DPA en cluster, car la valeur IPV6%Interface_Id doit être saisie manuellement. Dans tous les autres cas, le nom de domaine complet/l'adresse IP est automatiquement défini(e) sur la valeur par défaut de l'adresse IP du serveur d'applications.

   Cliquez sur **Next**.

13. Une fois terminée l'installation du serveur de datastore DPA, cliquez sur **Done**.
14. À l'invite de commande, exécutez la commande `dpa svc status` pour vérifier que le service de datastore est en cours d'exécution.
15. Définissez la taille du pool de connexions à la base de données dans tous les nœuds du datastore. Exécutez :

    `# dpa ds tune --connections xxx <RAM>GB` où *xxx* représente environ 250 pour chaque serveur d'applications et *RAM* représente la quantité de RAM. Par exemple, vous utiliseriez *xxx* 500 pour un cluster à deux nœuds.

    Si le cluster est activé pour la réplication de datastore, exécutez cette commande pour tous les datastores esclaves.

Installation du service d'applications avec la réplication du datastore

Cette procédure d'installation du service d'application est incluse par souci d'exhaustivité. Il n'existe aucune mise en œuvre particulière du service d'application pour la réplication de datastore.

Avant de commencer

- Copiez le fichier binaire d'installation sur le serveur ou sur votre machine locale.
- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Présentation de l'installation et de la configuration à la page 24 fournit plus d'informations à ce sujet.
- Assurez-vous que l'option de service de datastore est sélectionnée et que le service de datastore est en cours d'exécution.
- En cas d'installation sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Si l'installation a été effectuée avec les options avancées sur Linux IPv6, et que l'agent souhaite parler à un autre serveur d'applications ou répartiteur de charge, par exemple, dans le cas d'un cluster, assurez-vous de disposer de l'adresse IP du serveur d'applications avec lequel l'agent souhaite communiquer. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation du serveur d'applications. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr`

`show` sur le serveur d'applications et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

```
fe80::9c9b:36f:2ab:d7a2%2
```

Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications ou du répartiteur de charge auquel l'agent souhaite se connecter (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) ; celles placées après font référence à l'ID de l'interface du serveur d'applications en cours (`2` dans cet exemple).

- Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE.

Le processus d'installation du service d'application est similaire à celui du service de datastore.

Procédure

1. Double-cliquez sur le fichier binaire DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Faites défiler le contrat jusqu'à la fin pour activer l'option permettant d'accepter les termes du contrat de licence. Cliquez sur **Next.**
4. Dans l'écran **Installation Options**, sélectionnez l'option d'installation du service d'application, puis cliquez sur **Next**.
5. Si vous n'effectuez pas d'installation avancée, cliquez sur **Next**, puis suivez les consignes de l'assistant d'installation.
6. Consultez le récapitulatif avant installation, notamment les informations sur l'espace disque requis, puis cliquez sur **Install**. L'installation commence.

   S'il n'y a pas suffisamment d'espace disque, annulez l'installation ou sélectionnez un autre disque pour installer DPA.

   Remarque

   Une erreur d'échec de connexion au datastore peut se produire si les pare-feu nécessaires pour communiquer entre le serveur d'applications et le datastore ne sont pas ouverts. Paramètres de communication dans DPA à la page 19 fournit des informations à ce sujet.

7. Dans l'étape **Connect to Remote DPA Datastore**, saisissez l'adresse IP du serveur de datastore DPA maître préalablement installé.

   L'installation reprend.

8. À l'invite, spécifiez le nom ou l'adresse IP de l'hôte du serveur d'applications DPA avec lequel l'agent DPA va communiquer. Par défaut, l'Agent communique avec le serveur d'applications local avec l'adresse IP 127.0.0.1. Dans une configuration en cluster, fournissez l'adresse IP du répartiteur d'équilibrage de charge placé devant les serveurs d'applications. Cliquez sur **Next**.

   L'installation du service d'application DPA est maintenant terminée.

9. Saisissez le mot de passe du datastore lorsque vous y êtes invité.

   Notez les points suivants concernant le mot de passe du datastore :

   - Les mots de passe vides ne sont pas pris en charge.
   - La longueur minimale est de 9 caractères.
   - Les critères suivants sont obligatoires :
     - Un minimum de 1 lettre majuscule et 1 lettre minuscule
     - Un minimum de 1 caractère numérique
     - Un minimum de 1 caractère spécial
   - La commande dpa datastore dspassword peut être utilisée pour réinitialiser le mot de passe du datastore DPA. Pour plus d'informations, reportez-vous à la section dpa datastore dspassword à la page 156.

10. Définissez le mot de passe d'administrateur.

    Notez les points suivants concernant le mot de passe d'administrateur :

    - Les mots de passe vides ne sont pas pris en charge.
    - La longueur minimale est de 9 caractères.
    - Les critères suivants sont obligatoires :
      - Un minimum de 1 lettre majuscule et 1 lettre minuscule
      - Un minimum de 1 caractère numérique
      - Un minimum de 1 caractère spécial
    - La commande dpa app adminpassword peut être utilisée pour réinitialiser le mot de passe de l'administrateur DPA et pour activer le compte administrateur DPA lorsque le service de datastore DPA est opérationnel. dpa application adminpassword à la page 146 fournit plus d'informations à ce sujet.

11. Cliquez sur **Done**.

    Une fois l'installation terminée, démarrez le serveur DPA et attribuez-lui une licence. Procédure qui suit l'installation de DPA à la page 65 fournit plus d'informations à ce sujet.

Bonnes pratiques de réplication du datastore

Pour répliquer le datastore, respectez les bonnes pratiques suivantes :

- Vous devez redémarrer le service du datastore chaque fois que le rôle change entre le datastore maître et le datastore esclave.
- Utilisez la commande de configuration de la réplication dpa ds rep pour vérifier l'état de la réplication. L'exécution de la commande dpa ds rep sur le datastore maître permet de savoir si la réplication est en cours et de connaître le datastore esclave. Son exécution sur le datastore esclave permet de savoir quel est le datastore maître.
- Avant d'exporter un datastore, vérifiez que vous avez créé un répertoire vide sur le datastore sur lequel vous souhaitez exporter les fichiers du datastore. Par exemple, /tmp/export.

- Les datastores maîtres et esclaves doivent avoir les mêmes caractéristiques de performance et être installés sur la même version de DPA.

Installation de l'agent DPA

Cette section explique comment installer l'agent DPA à l'aide du module d'installation de l'agent seul. Elle concerne les nouvelles installations.

Un agent est automatiquement installé sur les serveurs d'application et de datastore DPA. Par conséquent, n'exécutez pas cette procédure sur les serveurs DPA. Pour les mises à niveau à partir de service packs DPA antérieurs à DPA18.1, ainsi que pour installer les versions les plus récentes de DPA18.1, consultez la section Mises à niveau.

Installation de l'agent DPA

La procédure ci-dessous explique comment installer l'agent DPA dans un environnement Windows.

Avant de commencer

- Assurez-vous que les ports sont ouverts ou désactivés pour la communication entre les serveurs DPA. Pour plus d'informations, reportez-vous à la section Présentation de l'installation et de la configuration à la page 24.
- Assurez-vous de disposer de l'adresse IP du serveur d'applications DPA avec lequel l'agent souhaite communiquer. Si vous effectuez l'installation sur Linux IPv6, assurez-vous de disposer de l'ID de l'interface IPv6 de l'agent. Vous êtes invité à l'indiquer dans la fenêtre **Configure Agent** de l'installation de l'agent. Pour obtenir l'ID d'interface IPv6, exécutez la commande `ip addr show` sur la machine de l'agent Linux et utilisez les résultats pour trouver l'ID de l'interface IPv6. Par exemple :

  ```
  fe80::9c9b:36f:2ab:d7a2%2
  ```

  Où les valeurs placées avant le symbole *%* font référence au protocole IPv6 du serveur d'applications DPA (dans cet exemple, `fe80::9c9b:36f:2ab:d7a2`) et celles placées après font référence à l'ID de l'interface de l'agent (dans cet exemple, `2`).

Procédure

1. Double-cliquez sur le fichier binaire de l'agent DPA pour démarrer l'installation.
2. Cliquez sur **Next**.
3. Lisez et acceptez le contrat de licence utilisateur. Cliquez sur **Next**.
4. Sélectionnez un dossier d'installation et cliquez sur **Next**.
5. Vérifiez le récapitulatif avant installation, puis cliquez sur **Install**.
6. Choisissez les options d'installation de l'Agent :
   - **Do not start DPA Agent service** : cette option empêche le démarrage du service de l'agent DPA après l'installation.

     Si vous sélectionnez cette option, vous devez démarrer manuellement l'agent DPA à partir de la ligne de commande.

     Si vous avez sélectionné Do not start DPA Agent service, cliquez sur **Next**.

     Saisissez le nom de domaine complet ou l'adresse IP du serveur DPA qui communique avec l'agent DPA.

- **L'agent est utilisé pour surveiller la base de données Oracle :** Sélectionnez cette option pour surveiller une base de données Oracle avec l'agent DPA.

  Si vous sélectionnez cette option, naviguez jusqu'au répertoire dans lequel l'agent DPA peut trouver les fichiers des pilotes de périphériques de la base de données Oracle.

7. Cliquez sur **Next**.
8. Dans la fenêtre **Configure Agent**, saisissez le nom de domaine complet ou l'adresse IP du serveur d'applications DPA qui communique avec l'agent DPA.

   Si vous effectuez une installation sur Linux IPv6 et que vous installez des agents Linux, saisissez l'ID d'interface IPv6 de l'agent Linux.

   Cliquez sur **Next**.
9. Définissez le même mot de passe d'agent que celui défini lors de l'installation du datastore DPA :

   Notez les points suivants concernant le mot de passe de l'agent :

   - Les mots de passe vides ne sont pas pris en charge.
   - La longueur minimale est de 9 caractères.
   - Les critères suivants sont obligatoires :
     - Un minimum de 1 lettre majuscule et 1 lettre minuscule
     - Un minimum de 1 caractère numérique
     - Un minimum de 1 caractère spécial
10. Cliquez sur **Done** pour terminer la procédure d'installation.
11. Redémarrez le service Agent.

À effectuer

Suivez les étapes de la section Définition du mot de passe de gestion des licences de l'agent DPA à la page 58.

Définition du mot de passe de gestion des licences de l'agent DPA

Après l'installation de l'agent DPA, définissez le mot de passe de l'agent.

Procédure

1. Exécutez `dpaagent --set-credentials` pour définir le mot de passe de l'agent DPA.

   dpaagent --set-credentials fournit des informations complètes sur la commande.

Configuration de l'agent DPA version 18.1 pour revenir en arrière et collecter les données d'application de sauvegarde

Par défaut, l'agent DPA nouvellement installé commence à collecter des données d'applications de sauvegarde à partir de la date et heure actuelles. Si vous souhaitez consulter les alertes pour les échecs de sauvegardes pendant les jours précédents à des fins d'audit ou autres, ou si pour une raison quelconque, vous souhaitez collecter des jours de données d'application de sauvegarde, vous pouvez configurer l'agent DPA

nouvellement installé de façon à collecter des données pour un nombre d'heures défini par l'utilisateur.

Avant de commencer

Vous devez disposer de DPA18.1 ou une version ultérieure pour cette procédure.

Sous Linux

Procédure

1. Installez l'agent DPA. Ne lancez pas l'agent DPA.
2. Ajoutez les deux lignes suivantes dans le fichier `dpa.config` :

   `VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS`

   `export VARIABLE_NAME`

   Où *VARIABLE_NAME* est le suivant pour ces applications de sauvegarde :

   NetWorker: AGENT_NSR_JOB_STARTTIME

   Avamar : AGENT_AXION_JOB_STARTTIME

   TSM : AGENT_TSM_JOB_STARTTIME

   HPDP : AGENT_DP_JOB_STARTTIME

   CommVault : AGENT_CV_JOB_STARTTIME

   NetBackup : AGENT_NB_JOB_STARTTIME

   ArcServe : AGENT_AS_JOB_STARTTIME

   DB2 : AGENT_DB2_JOB_STARTTIME

   SAP HANA : AGENT_SAP_HANA_JOB_STARTTIME

   RMAN : AGENT_RMAN_JOB_STARTTIME

   MSSQL : AGENT_MSSQLDB_JOB_STARTTIME

   NUMBER_OF_BACKUP_HOURS est le nombre d'heures de sauvegarde avant l'heure actuelle.

   Par exemple, les deux lignes suivantes dans `dpa.config` font que l'agent DPA collecte les données à partir des 14 jours précédents :

   ```
   AGENT_AXION_JOB_STARTTIME=336
   export AGENT_AXION_JOB_STARTTIME
   ```

3. Lancez l'agent DPA.

Pour Windows

Procédure

1. Exportez le registre de clés système vers le chemin de registre `HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT` avec les informations suivantes :

   `VARIABLE_NAME=NUMBER_OF_BACKUP_HOURS`

   Où *VARIABLE_NAME* est le suivant pour ces applications de sauvegarde :

NetWorker: NSR_JOB_STARTTIME

Avamar : AXION_JOB_STARTTIME

TSM : TSM_JOB_STARTTIME

HPDP : DP_JOB_STARTTIME

CommVault : CV_JOB_STARTTIME

NetBackup : NB_JOB_STARTTIME

ArcServe : AS_JOB_STARTTIME

DB2 : DB2_JOB_STARTTIME

SAP HANA : SAP_HANA_JOB_STARTTIME

RMAN : RMAN_JOB_STARTTIME

MSSQL : MSSQLDB_JOB_STARTTIME

NUMBER_OF_BACKUP_HOURS est le nombre d'heures de sauvegarde avant l'heure actuelle.

Par exemple, ajoutez les trois lignes suivantes au contenu du fichier `avamar.reg` et lancez-le à partir de cmd pour une exportation vers le registre, afin que l'agent DPA collecte les données auprès de NetWorker à partir des 14 jours précédents :

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\emc\DPA\AGENT]

NSR_JOB_STARTTIME="336"
```

2. Installez et lancez l'agent DPA.

Installation à l'aide d'une ligne de commande

Utilisez la ligne de commande appropriée.

Avant de commencer

Si vous installez DPA sur un des systèmes d'exploitation UNIX, exécutez la commande `chmod 755` pour modifier l'autorisation d'exécution du fichier binaire.

- Linux

```
DPA-<component>-Linux-<architecture>-<version>.xxx.install.bin
[option]
```

où *option* est l'une des options décrites pour une installation silencieuse ou interactive dans le tableau 7.

Par exemple : **`DPA-Agent-Linux-x86_64-6.5.0.1.bin -i silent -DUSER_INSTALL_DIR="/opt/custom/emc/dpa"`**

- AIX

```
./DPA-<component>-AIX-<architecture>-<version>.bin
```

Par exemple : **./DPA-Agent-AIX-PPC64-6.5.0.1.bin**

- Windows

```
DPA-<component>-Windows-<architecture>-
<version>.xxx.install.exe [option]
```

où *option* est l'une des options décrites pour une installation silencieuse ou interactive dans le tableau 7.

Par exemple : **DPA-Agent-Windows-x86_64-6.5.0.1.exe -i silent -DUSER_INSTALL_DIR="C:\custom\emc\dpa"**

Assurez-vous que vous exécutez les étapes décrites à la section Procédure qui suit l'installation de DPA à la page 65.

Tableau 8 Options de ligne de commande du programme d'installation

Option	Description
-?	Affiche le texte d'aide.
-i [swing | console | silent]	Indique le mode d'interface utilisateur pour le programme d'installation : swing : interface graphique console : console uniquement silent : sans interaction de l'utilisateur
-D <name>="<value>"	Indique les paires nom-valeur du programme d'installation qui peuvent être définies sur la ligne de commande (à l'aide de l'option -D) pour remplacer les valeurs par défaut du programme d'installation ou qui peuvent être insérées dans un fichier de réponses et utilisées avec l'option *-f*. La valeur doit être indiquée entre guillemets. Exemple : -D<*variable name*>="<*value*>" Où : Par exemple : **DPA-Agent-Linux-x86_64-6.5.0.1.bin -i silent -DPort="3740"** Les descriptions <*variable name*> et <*value*> sont incluses dans les tableaux suivants.

Tableau 9 Variables du programme d'installation du datastore

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
USER_INSTALL_DIR	Emplacement d'installation	Chemin d'accès valide	Windows: C:\Program Files\EMC\DPA Linux: /opt/emc/dpa
CHOSEN_INSTALL_SET	Jeu d'installation	DS	s.o.
VAR_INSTALL_SERVICE	Option avancée pour installer le service de datastore	TRUE/FALSE	TRUE
VAR_START_SERVICE	Option avancée pour démarrer/arrêter le service de datastore	TRUE/FALSE	TRUE

Tableau 9 Variables du programme d'installation du datastore (suite)

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
VAR_DATASTORE_DATA_LOCATION	Option avancée de mise en page du datastore pour spécifier le répertoire de données du serveur de datastore afin d'optimiser les performances	Chemin d'accès valide	`$USER_INSTALL_DIR$\services\datastore\`
VAR_DATASTORE_XLOG_LOCATION	Option avancée de mise en page du datastore pour spécifier le répertoire Xlog du serveur de datastore afin d'optimiser les performances	Chemin d'accès valide	`$USER_INSTALL_DIR$\services\datastore\data\`
VAR_USERNAME (LINUX uniquement)	Option avancée pour spécifier un compte utilisateur UNIX existant afin d'installer le service de datastore	Nom d'utilisateur existant	s.o.
VAR_DATASTORE_BIND_ADDRESSES	Adresse IP sur laquelle Postgres doit écouter	Adresse IP valide	s.o.
VAR_DATASTORE_CLIENTS_ADDRESSES	Adresse IP du ou des serveurs d'applications qui se connecteront au service de datastore	Adresses IP valides séparées par une virgule « , »	s.o.
VAR_APOLLO_USER_PASSWORD	DPA Datastore password	[Défini lors de l'installation ou réinitialisé à l'aide de l'interface de ligne de commande DPA.]	s.o.

Tableau 10 Variables de réplication des options avancées du datastore

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
VAR_DATASTORE_REPLICATION	Rôle de la réplication du datastore	MASTER/SLAVE	s.o.
VAR_DATASTORE_REPLICATION_	Adresse IP du maître ou de l'esclave. Si VAR_DATASTORE_REPLICATION_ROLE est défini sur « MASTER », l'adresse IP de l'esclave doit être saisie et inversement lorsque VAR_DATASTORE_REPLICATION_ROLE est défini sur « SLAVE ».	Adresse IP du maître ou de l'esclave	s.o.

Tableau 11 Variables de l'agent de datastore

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
Nom de domaine complet ou adresse IP du serveur DPA VAR_AGENT_APPLICATION _ADDRESS pour gérer l'agent de datastore	Nom de domaine complet ou adresse IP du serveur DPA pour gérer l'agent de datastore Dans le cas de Linux IPv6, <IPv6Address> %<Interface_Id_Of_Datastore_Agent>	Adresse IP ou nom d'hôte valide	Dans le cas où il y a plusieurs serveurs d'applications et lorsque le service de datastore communique avec un ou plusieurs serveurs d'applications Linux IPv6, cette valeur est vide. Sinon, la valeur par défaut est identique à `VAR_DATASTORE_CLIENTS_ADDRESSES`
VAR_AGENT_START_SERVICE	Option avancée pour démarrer/arrêter l'agent de datastore après l'installation	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	Option avancée utilisée par l'agent de datastore pour surveiller Oracle. Chemin d'accès aux fichiers des pilotes de périphériques de la base de données Oracle	Chemin d'accès valide	s.o.

Tableau 12 Variables du programme d'installation de l'application

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
USER_INSTALL_DIR	Emplacement d'installation	Chemin d'accès valide	Windows : `C:\Program Files\EMC\DPA` Linux : `/opt/emc/dpa`
CHOSEN_INSTALL_SET	Jeu d'installation	APP	s.o.
VAR_INSTALL_SERVICE	Option avancée pour installer le service d'application	TRUE/FALSE	TRUE
VAR_START_SERVICE	Option avancée pour démarrer/arrêter le service d'application après l'installation	TRUE/FALSE	TRUE
VAR_APPLICATION_DATASTORE_ADDRESS	Adresse IP du serveur de datastore	Adresse IP valide où le service de datastore est installé et s'exécute	s.o.
VAR_ADMIN_PASSWORD	Mot de passe administrateur associé à l'application DPA	[Défini lors de l'installation ou réinitialisé à l'aide de l'interface de ligne de commande DPA.]	s.o.
VAR_APOLLO_USER_PASSWORD	DPA Datastore password	[Défini lors de l'installation ou réinitialisé à l'aide de l'interface de ligne de commande DPA.]	s.o.

Tableau 13 Variables de l'agent de serveur d'applications

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
VAR_AGENT_APPLICATION_ADDRESS	Nom de domaine complet ou adresse IP du serveur DPA pour gérer l'agent du serveur d'applications	Adresse IP ou nom d'hôte valide	127.0.0.1
VAR_AGENT_START_SERVICE	Option avancée pour démarrer/arrêter l'agent du serveur d'applications après l'installation	TRUE/FALSE	TRUE
AVAR_AGENT_ORACLE_DIRECTORY	Option avancée utilisée par l'agent du serveur d'applications pour surveiller Oracle. Chemin d'accès aux fichiers des pilotes de périphériques de la base de données Oracle	Chemin d'accès valide	s.o.

Tableau 14 Variables des options avancées du cluster du serveur d'applications

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
VAR_APPLICATION_ADDRESS	Adresse IP utilisée par le serveur d'applications pour se présenter aux autres nœuds de l'application DPA.	Adresse IP valide	s.o.
VAR_APPLICATION_CLUSTER_ROLE	Rôle du nœud d'application dans un cluster	MASTER/SLAVE	s.o.
VAR_APPLICATION_MASTER_ADDRESS	Si VAR_APPLICATION_CLUSTER_ROLE="SLAVE", cette valeur doit être saisie.	Adresse IP valide	s.o.
VAR_APPLICATION_REPORT_DIRECTORY	Chemin d'accès au dossier de rapport partagé du réseau	Chemin d'accès valide	s.o.
VAR_APPLICATION_REPORT_USERNAME	Utilisateur qui détient le service d'application et bénéficie du droit d'accès au dossier de rapport partagé	DOMAIN\\Username existant pour Windows Nom d'utilisateur existant pour UNIX	s.o.
VAR_APPLICATION_REPORT_PASSWORD (Windows uniquement)	Mot de passe de l'utilisateur précédent		s.o.

Tableau 15 Variables du programme d'installation de l'agent autonome

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
USER_INSTALL_DIR	Emplacement d'installation	Chemin d'accès valide	Windows : `C:\Program Files\EMC\DPA`

Tableau 15 Variables du programme d'installation de l'agent autonome (suite)

Nom de variable	Description	Valeurs possibles	Valeurs par défaut
			Linux : `/opt/emc/dpa`
VAR_AGENT_APPLICATION_ADDRESS	Nom de domaine complet ou adresse IP du serveur DPA pour gérer le nom d'hôte ou l'adresse IP valide de cet agent	Dans le cas de Linux IPv6, <IPv6Address> %<Interface_Id_Of_Agent>	s.o.
VAR_AGENT_START_SERVICE	Option avancée pour démarrer/arrêter l'agent après l'installation	TRUE/FALSE	TRUE
VAR_AGENT_ORACLE_DIRECTORY	Option avancée utilisée pour surveiller Oracle. Chemin d'accès aux fichiers des pilotes de périphériques de la base de données Oracle	Chemin d'accès valide	s.o.

Procédure qui suit l'installation de DPA

Après l'installation ou la mise à niveau de DPA et l'accès à la console Web DPA, un message s'affiche, indiquant au serveur DPA l'état du processus d'initialisation. Le processus d'initialisation peut durer environ 10 minutes.

Lors de l'initialisation, DPA crée les schémas de base de données, les tableaux, les vues et le datastore DPA. Il crée également les différents rapports système et modèles de tableaux de bord, les utilisateurs du système par défaut, les groupes de règles du moteur d'analyse et divers autres objets d'origine et par défaut. Votre temps de connexion réseau affecte la vitesse à laquelle toutes ces actions sont effectuées. Après l'installation de DPA, veillez à exécuter les étapes suivantes.

Procédure

1. Si vous avez effectué une mise à niveau ou une migration vers la version DPA18.1, videz le cache/l'historique du navigateur avant toute utilisation de DPA18.1.
2. (Facultatif) Procédez comme suit pour vérifier si l'initialisation est toujours en cours ou si elle est terminée :
   a. Si vous avez effectué l'installation sur Linux à un emplacement autre que celui par défaut, déconnectez-vous de la session, puis reconnectez-vous. Vous pouvez également procéder à l'exécution depuis une nouvelle fenêtre de connexion.

      Un nouveau shell est requis pour que les chemins d'accès aux commandes d'exécution soient trouvés avant l'exécution de dpa.sh svc status.

   b. Sur le serveur d'applications DPA, accédez à <install_dir>\services \applications.
   c. Vérifiez les extensions*.deployed, *.isdeploying ou .failed des fichiers *.rar, *.ear et *.war.
      - Si l'extension de ces fichiers est *.isdeploying, cela signifie que l'initialisation du serveur est en cours.

- Si l'extension de ces fichiers est *.deployed, l'initialisation du serveur est terminée et vous pouvez vous connecter à la console Web DPA.
- Si l'extension des fichiers est *.failed, l'initialisation du serveur a échoué. Dans ce cas, contactez le support technique.

3. Démarrez la console Web pour vérifier que DPA a été correctement installé.

   Tous les services de DPA doivent être en cours d'exécution lorsque vous démarrez la console Web. Pour démarrer la console Web, votre navigateur doit être équipé du plugin Adobe Flash.

   a. Ouvrez un navigateur et connectez-vous au serveur DPA par https sur le port 9002. Vérifiez que vous avez désactivé votre bloqueur de fenêtres contextuelles. Par exemple :

      ```
      https://<server_name>:9002
      ```

      Où <*server_name*> est le nom ou l'adresse IP du serveur ou localhost.

      Vous pouvez également utiliser

      ```
      https://<server_name>:9002/flexui url
      ```

      . Si vous souhaitez continuer à utiliser la console web DPA18.1 basée sur Flex.

   b. Saisissez le nom d'utilisateur et le mot de passe. Le nom d'utilisateur et le mot de passe sont sensibles à la casse.

   c. Cliquez sur **Login**

4. Ajoutez des licences au serveur DPA.

   Le serveur DPA est installé avec une licence temporaire de 90 jours.

   Si vous mettez à niveau et que vous n'ajoutez pas de capacité ou que vous ne passez pas à une nouvelle fonctionnalité de DPA18.1, aucune modification d'octroi de licences n'est nécessaire.

   La licence CLP est requise pour la nouvelle fonctionnalité DPA18.1 et accroît la capacité sur une instance DPA. Si vous effectuez une migration à partir de DPA 5.x vers DPA18.1, les licences existantes font l'objet d'une migration en même temps que la configuration et les données. Pour plus d'informations, reportez-vous à la section Coexistence de licences CLP et WLS dans DPA à la page 80.

   Si vous ajoutez des licences CLP, veillez à sélectionner des fichiers de licence dotés de l'extension .lic.

   Si vous ajoutez des licences WLS, sélectionnez des fichiers de licence dotés de l'extension .wls.

   Une fois le fichier de licence installé, vous êtes invité à fermer la console Web DPA pour pouvoir enregistrer le fichier de licence.

5. Reconnectez-vous à la console Web DPA.
6. (Recommandé) Si vous avez ajouté des licences CLP à l'étape 4, enregistrez le serveur d'applications DPA avec le ESRS-VE. Ce processus d'enregistrement permet au support clients d'assurer la maintenance de l'instance DPA.

Tenez compte des points suivants :

- Si vous mettez à niveau un ESRS précédemment enregistré, il est possible que ESRS indique qu'il est déjà enregistré avec l'erreur suivante : `[ERROR] This node is already registered with an EMC Secure Remote Support Service.`

  Ensuite, ESRS montre que IP de l'hôte n'est plus disponible avec les erreurs suivantes :

  `[ERROR] This node failed to delete with EMC Secure Remote Support Service.`

  `Offline: Validation error`

  Consultez l'article xxxxxx de l'EMC Knowledgebase, disponible sur http://www.support.emc.com, pour de plus amples informations. Il s'agit d'un problème d'environnement qui n'est pas lié à DPA.
- L'enregistrement d'ESRS après une nouvelle installation nécessite qu'un ESRS-VE soit déjà installé et accessible à partir du serveur d'applications DPA. Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE. Le *Guide de compatibilité de Data Protection Advisor* fournit les informations de module et de version du ESRS-VE pris en charge.
- Enregistrez un seul service d'application. L'enregistrement inclut à la fois le datastore DPA et les serveurs d'applications.
- Si vous travaillez dans un environnement de clusters, enregistrez le serveur d'applications maître auprès d'ESRS. Utilisez la commande `dpa app con` pour vérifier si votre serveur d'applications est un serveur maître ou esclave. Pour plus d'informations, reportez-vous à la section relative à CLI.
- Lorsque vous êtes invité à fournir un nom d'utilisateur et un mot de passe pour EMC Secure Remote Support, saisissez les informations d'identification du support en ligne EMC pour l'enregistrement. Par exemple :

```
dpa app support --register 10.11.110.111
Dell EMC Data Protection Advisor
Enter Data Protection Advisor Administrator username :
Enter Data Protection Advisor Administrator password :
Enter EMC Secure Remote Support username :
Enter EMC Secure Remote Support password :
```

- Notez les points suivants : Dans un environnement de clusters, n'utilisez pas le serveur d'applications enregistré auprès d'ESRS pour les rapports planifiés. Les problèmes éventuels de rapports planifiés ou de collecte de données sur le Listener sont propagés sur les serveurs d'applications dans le cluster.

a. Connectez-vous au serveur d'applications en utilisant l'option Connexion Bureau à distance de Windows ou PuTTY pour Linux.

b. Saisissez la commande `dpa app support --register ESRS_IP` pour enregistrer un serveur DPA.

Où *ESRS_IP* est l'adresse IP de la passerelle ESRS. Par exemple :

```
C:\Program Files\EMC\DPA\services\bin>dpa app support --
register 10.11.110.111
```

c. À l'invite, saisissez le nom d'utilisateur et le mot de passe EMC Secure Remote Support.

La sortie qui s'affiche indique que la demande d'enregistrement du serveur DPA avec l'adresse IP saisie est approuvée et que la commande a été exécutée avec succès.

7. (Recommandé) Si vous avez enregistré le serveur d'applications DPA avec l'ESRS-VE à l'étape 6, activez le Service de surveillance de l'intégrité sur le serveur d'applications DPA. Sur le serveur d'applications DPA, saisissez :
   a. **$ dpa health install**
   b. **$ dpa health start**
8. (Facultatif) Si vous souhaitez configurer des alertes relatives à la surveillance de la réplication, assurez-vous de créer des règles de capacité de restauration à la politique d'analyse et attribuez les règles à l'objet de votre choix. Accédez à **Policies** > **Analysis Policies**
9. (Facultatif) Si vous avez effectué une mise à niveau à partir d'une version 6.x précédente et que vous souhaitez afficher le tableau de bord de présentation de Data Domain et le tableau de bord des informations de Data Domain :
   a. Accédez à **Dashboard** > **+ icône** > **Open Existing Dashboard**.

      La fenêtre **Open Existing Dashboard** s'affiche.
   b. Sélectionnez **Data Domain**, puis cliquez sur OK.
10. (Facultatif) Si vous surveillez un Data Domain OS 5.7 et versions supérieures et que vous souhaitez vous assurer de la configuration de la collecte des données de Reporting sur la capacité physique :
    a. Attribuez manuellement la demande à des cases de Data Domain OS 5.7.
    b. Exécutez la demande afin que les statistiques soient collectées sur le Data Domain et que le planning soit créé. Puis, lorsque vous êtes prêt à exécuter le premier rapport, les données sont renvoyées.

Chiffrement du serveur d'applications DPA

Pour chiffrer les informations qui transitent entre le serveur d'applications et la console Web DPA, vous devez installer un certificat sur le serveur d'applications.

Chiffrement du serveur d'applications DPA

Les informations qui transitent entre le serveur d'applications DPA et la console Web DPA sont chiffrées à l'aide du certificat auto-signé inclus avec le serveur d'applications DPA. Aucune action n'est nécessaire. Ce certificat est généré au cours de l'installation, tout comme le mot de passe du magasin de clés.

Avant de commencer :

- Assurez-vous que vous avez demandé et obtenu un certificat approuvé et une clé privée pour le serveur d'applications, auprès d'une autorité de certification.

- Assurez-vous que vous avez fusionné le certificat fiable et la clé privée au sein d'un fichier de magasin de clés. Pour plus d'informations, consultez la documentation de votre autorité de certification.
- Si vous mettez en œuvre le clustering des serveurs d'applications, assurez-vous d'avoir bien effectué la configuration du cluster avant d'activer le chiffrement sur le datastore et les serveurs d'applications.

Procédure

1. Utilisez la commande `dpa app impcert -kf` pour importer le certificat auto-signé.

   `dpa app impcert -kf "C:\work\new.keystore" -al newkey -pw password`

   Voici le mot de passe du nouveau fichier de magasin de clés créé. Ce mot de passe se trouve à l'emplacement suivant : `C:\work\new.keystore`.

2. Redémarrez le service d'application DPA. Pour plus d'informations, exécutez la commande `dpa app --help`.
3. (Facultatif) Installez le certificat sur les navigateurs que vous utilisez pour accéder à DPA. Suivez les instructions de votre navigateur.

   Lors de la première connexion, en mode sécurisé, l'ouverture de DPA peut prendre quelques minutes.

Chiffrement de cluster de serveur d'applications

Pour chiffrer les clusters de serveur d'applications, vous devez disposer d'un certificat de domaine (caractère générique) du fournisseur de certificats fiables. Installez ce certificat sur tous les nœuds de cluster d'applications DPA.

Vous ne devez pas installer un certificat individuel pour chaque nœud d'application du cluster.

Configuration du logiciel antivirus avec DPA

Définissez la configuration antivirus suivante. Consultez la documentation de votre logiciel antivirus spécifique pour plus d'informations sur la façon de configurer le logiciel afin qu'il n'existe aucune surveillance en temps réel de ces processus ou des fichiers qu'ils lisent.

Il n'est pas nécessaire que tous les systèmes de fichiers DPA soient surveillés par un logiciel antivirus, et l'analyse de certains systèmes de fichiers et processus peut entraîner une dégradation des performances globales en raison de l'impact de l'activité accrue d'E/S de disque.

Procédure

1. Excluez les fichiers et les processus suivants de la surveillance de l'antivirus.

   Si vous configurez le logiciel antivirus sous Linux, les noms de fichier suivants n'auront pas d'extension `.exe`.

   - Serveur d'applications DPA :
     - `<install_dir>services\executive\wrapper.exe`
     - `<install_dir>\agent\bin\dpaagent.exe`
     - `<install_dir>\services\_jre\bin\java.exe`

- Serveur de datastore DPA :
  - `<install_dir>\services\datastore\engine\bin\postgres.exe`
  - `<install_dir>\agent\bin\dpaagent.exe`

2. Excluez les répertoires spécifiques suivants de la surveillance de votre logiciel antivirus.
   - Serveur d'applications DPA :
     - `<install_dir>\services\standalone\**`
     - `<install_dir>\services\tmp\**`
     - `<install_dir>\services\shared\**`
   - Espace de fichier sur le serveur de datastore DPA :

     Remarque

     Si vous avez sélectionné la présentation avancée du système de fichiers lors de l'installation du datastore, les autres répertoires peuvent être utilisés au lieu des valeurs par défaut suivantes.

     - `<install_dir>\services\datastore\data\**`
     - `<install_dir>\services\datastore\data\pg_log\**`

Mises à niveau

Vous pouvez effectuer une mise à niveau des versions précédentes de DPA vers DPA18.1 et les versions mineures. Les*Notes de mise à jour de Data Protection Advisor* fournissent des informations sur les mises à niveau prises en charge.

Notez que le programme d'installation de mise à niveau DPA18.1 n'offre pas la possibilité d'utiliser exclusivement la version 1.2 du protocole TLS. De plus, DPA conserve vos paramètres de version du protocole TLS existants après une mise à niveau. Vous ne pouvez changer la version du protocole TLS pour la version 1.2 qu'après la mise à niveau. La configuration de la version du protocole TLS en 1.2 postérieure à une installation ou à une mise à niveau fournit des informations.

Conditions préalables à la mise à niveau

Il existe un ensemble de bonnes pratiques recommandées avant d'exécuter une mise à niveau du serveur DPA.

- Sauvegardez le datastore DPA à l'aide de la commande `dpa ds export` . Pour plus d'informations, reportez-vous à la section Sauvegarde du datastore à la page 136. Le programme d'installation de DPA vous invite à procéder comme suit.
- Pour les mises à niveau des serveurs d'applications et du datastore, l'agent DPA sur ces serveurs est également mis à niveau dans le cadre de la mise à niveau du serveur. Vous devez effectuer une mise à niveau distincte pour les agents DPA autonomes uniquement.
- Pour garantir une communication sécurisée entre le serveur DPA et l'agent, définissez le mot de passe d'inscription de l'agent à l'aide de la commande de CLI

`dpa app agentpwd` sur l'hôte de serveur d'applications DPA. Vous devez également définir ce mot de passe sur tous les hôtes d'agents DPA. dpa application agentpwd fournit des informations à ce sujet. Puis, redémarrez le service d'application. Veillez à configurer ce mot de passe pour chaque agent. Cette règle a une exception : si vous exécutez simultanément des agents DPA antérieurs à la version 6.5, ainsi que la mise à niveau vers les agents 18.1 Pour plus d'informations, reportez-vous à la section Mise à niveau des agents DPA antérieurs à la version 6.5 parallèlement aux agents version 6.5 et au serveur DPA version 6.5 à la page 73.

- Exécutez dpa app ver et notez la build précédente de DPA 6.x installée sur votre système que la commande renvoie. Ce résultat est particulièrement important lors de la vérification de l'installation du package.
- Arrêtez le serveur d'applications DPA. La meilleure pratique consiste à exécuter une sauvegarde complète de l'hôte exécutant le serveur d'applications DPA.
- Arrêtez le datastore DPA. La meilleure pratique consiste à exécuter une sauvegarde complète de l'hôte exécutant le serveur de datastore DPA.
- Si votre infrastructure s'exécute sur une machine virtuelle, arrêtez l'application DPA et les serveurs de datastore et créez un snapshot des serveurs d'application et de datastore DPA afin de faciliter leur restauration en cas de problème de mise à niveau.
- Effacez le cache du navigateur.
- Assurez-vous que vous disposez de privilèges d'administration/root.
- En cas de mise à niveau sur UNIX/Linux, assurez-vous que la commande `unzip` pour InstallAnywhere est installée sur votre système.
- Lors de la mise à niveau ou de l'installation de correctifs dans des environnements en cluster, arrêtez le service d'application DPA sur tous les serveurs. Mettez d'abord à niveau le datastore, puis les serveurs d'applications. Vous devez arrêter le service d'application car le programme d'installation ne peut pas interrompre les services lorsque ceux-ci se trouvent sur des machines distinctes.
  Démarrez l'application DPA mise à niveau. Vérifiez que l'initialisation est terminée et que vous pouvez vous connecter à la console Web DPA avant de mettre à niveau les autres serveurs d'applications en cluster.
- Concernant la mise à niveau de la base de données :
  - Assurez-vous de disposer de 3 Go d'espace libre pour la mise à niveau de la base de données.
  - Assurez-vous d'exécuter une version LINUX avec une version glibc 2.12 au moins. Si votre version de LINUX exécute une version glibc antérieure à 2.12, utilisez la procédure fournie dans Mise à niveau de DPA avec une version de LINUX exécutant glibc antérieure à 2.12 à la page 73
- Si vous utilisez actuellement DPA pour le reporting RMAN via une licence de sauvegarde DPA existante, contactez votre responsable de compte pour la licence DPA for Enterprise Applications. La licence DPA for Enterprise Applications vous permet d'augmenter le nombre de serveurs RMAN inclus dans le reporting DPA lorsque vous effectuez une mise à niveau vers DPA 6.3 et les versions mineures. Saisissez la licence DDBEA dans DPA 6.3 et les versions mineures après l'installation.. Les notes de mise à jour *DPA 6.2 Release Notes* fournissent de plus amples informations sur la licence DDBEA.
- Si vous effectuez une mise à niveau depuis DPA 6.1, veillez à contrôler la période de rétention des demandes de collecte et à la modifier pour qu'elle corresponde

aux politiques de votre entreprise, et ce, avant d'effectuer une mise à niveau. En effet, les demandes de collecte de données contiennent une période de rétention par défaut différente dans DPA 6.1.

Mise à niveau de DPA

Utilisez cette procédure pour mettre à niveau DPA si aucun cluster ou réplication du datastore n'est configuré et si la version de LINUX que vous exécutez est une version glibc 2.12 au moins, le cas échéant.

Avant de commencer

Ajoutez la prise en charge pour les installations avec mise à niveau dans les cas où les tablespaces de base de données ont été configurés de façon à résider sur différents systèmes de fichiers.

- Assurez-vous que vous exécutez les étapes prérequises à la section Conditions préalables à la mise à niveau à la page 70.
- Assurez-vous que vous exécutez le programme d'installation en tant qu'administrateur/utilisateur root.

Si vous exécutez une version LINUX disposant d'une version glibc antérieure à 2.12, suivez la procédure fournie dans Mise à niveau de DPA avec une version de LINUX exécutant glibc antérieure à 2.12 à la page 73

Procédure

1. Si vous ne l'avez pas encore fait, arrêtez le service d'application.
2. Mettez à niveau le datastore. Suivez la procédure d'installation que vous indique le programme d'installation. Assurez-vous que le répertoire d'installation de DPA indiqué est correct.

   Vous devez installer le package de mise à jour de DPA dans le même répertoire d'installation que votre package DPA existant.
3. Mettez à niveau le serveur d'applications. Suivez la procédure d'installation que vous indique le programme d'installation. Assurez-vous que le répertoire d'installation de DPA indiqué dans le programme d'installation est correct.

   Vous devez installer le package de mise à jour de DPA dans le même répertoire d'installation que votre package DPA existant.
4. Redémarrez la console Web DPA.
5. Patientez jusqu'à ce que les fichiers soient déployés dans le dossier d'installation.

   Sous Windows : `C:\Program Files\EMC\DPA\<install_dir>services\applications`

   Sous Linux : `/opt/emc/dpa/services/applications`

   La page de la console Web DPA affiche l'état de la mise à niveau.
6. Exécutez les étapes fournies dans la section Procédure qui suit l'installation de DPA à la page 65.

Mise à niveau des agents DPA

Procédure

1. Arrêtez le service d'agent DPA.

2. Mettez l'agent à niveau à l'aide du programme d'installation de l'agent approprié à votre système d'exploitation. Suivez la procédure d'installation que vous indique le programme d'installation.

   Vous devez installer le package de mise à jour de l'agent dans le même répertoire d'installation que votre package DPA existant.

   Tenez compte du fait que lors de la mise à niveau, l'agent est arrêté et par conséquent, les demandes au cours de la mise à niveau peuvent échouer. Une fois la mise à niveau terminée, l'agent DPA continue de fonctionner normalement.

Mise à niveau des agents DPA antérieurs à la version 6.5 parallèlement aux agents version 6.5 et au serveur DPA version 6.5

Vous devrez peut-être exécuter des versions de l'agent DPA antérieures à 6.5, qui ne prennent pas en charge le mot de passe de l'agent. Dans ces situations, si vous définissez le mot de passe de gestion des licences de l'agent sur le serveur DPA, toutes les versions précédentes des agents DPA qui ne prennent pas en charge le mot de passe de l'agent ne parviennent pas à se connecter. Suivez la procédure ci-dessous pour éviter cette situation.

Vous devrez peut-être exécuter des versions de l'agent de DPA antérieures à la version 6.5 pour la collecte pour les systèmes qui ne sont plus pris en charge, ou vous aurez peut-être tellement d'agents autant que vous ne pouvez pas les mettre à niveau en une seule fois.

Procédure

1. Effectuez une mise à niveau du serveur DPA vers la version 6.5.

   Ne définissez pas le mot de passe d'inscription de l'agent. 3. Ne désinstallez pas l'ancienne version de l'agent, puis installez la version 6.5.

2. Mettez à niveau les agents DPA qui nécessitent une mise à niveau vers la version 6.5 en suivant le processus de mise à niveau normal.

   En cours de mise à niveau de l'agent DPA, il ne vous sera pas demandé de définir un mot de passe d'agent. Ce comportement diffère d'une nouvelle installation, qui demande de définir un mot de passe d'agent.

Mise à niveau de DPA avec une version de LINUX exécutant glibc antérieure à 2.12

Avant de commencer

- Assurez-vous que vous exécutez les étapes prérequises à la section Conditions préalables à la mise à niveau à la page 70.
- Assurez-vous que vous exécutez le programme d'installation en tant qu'administrateur/utilisateur root.

Procédure

1. arrêtez le service d'application.
2. Exportez le datastore. Pour plus d'informations, reportez-vous à la section Sauvegarde du datastore à la page 136.
3. Installez un nouveau datastore avec la dernière version de DPA et une version de LINUX exécutant glibc 2.12.

4. Importez le datastore existant sur le datastore nouvellement installé avec la dernière version de DPA et la version de LINUX prise en charge avec glibc version 2.12
5. Pointez le serveur d'applications DPA sur le datastore nouvellement installé et importé. Exécutez : `dpa app configure --master <datastore_ip>`
6. Mettez à niveau le datastore. Suivez la procédure décrite à la section Mise à niveau de DPA à la page 72.

Mise à niveau des clusters existants

Utilisez cette procédure pour mettre à niveau un cluster existant.

Avant de commencer

- Assurez-vous que vous exécutez toutes les étapes décrites à la section Conditions préalables à la mise à niveau à la page 70.
- Si vous utilisez des machines UNIX, assurez-vous que vous le faites en tant qu'utilisateur root.
- Arrêtez le répartiteur de charge sur les serveurs d'applications DPA et du datastore. La commande pour arrêter le répartiteur de charge dépend du système d'exploitation. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

Procédure

1. Arrêtez le service d'application sur les nœuds d'applications du cluster :
   a. Arrêtez le serveur d'applications esclave.
   b. Arrêtez le serveur d'applications maître.

   Exécutez :

   ```
   # dpa app stop
   ```
2. Mettez à niveau le serveur du datastore DPA :
   a. Démarrez le programme d'installation de DPA et suivez les invites.
   b. Assurez-vous que le datastore a été installé et a démarré correctement.

      Pour plus d'informations, reportez-vous à la section Procédure qui suit l'installation de DPA à la page 65.
3. Mettez à niveau le nœud d'application maître :
   a. Démarrez le programme d'installation de DPA et suivez les invites.
   b. Attendez que le service d'application démarre. Vérifiez que le fichier `server.log` comprend des sorties semblables à `DPA master started successfully`.
4. Mettez à jour les nœuds d'applications esclaves :
   a. Démarrez le programme d'installation de DPA et suivez les invites.
   b. Attendez que le service d'application démarre. Vérifiez que le fichier `server.log` comprend des sorties semblables à `DPA slave started successfully`.
5. Redémarrez l'application de répartiteur de charge sur les serveurs d'applications DPA et du datastore. La commande de démarrage du répartiteur de charge

dépend du système d'exploitation. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

Mise à niveau avec activation de la réplication du datastore pour DPA 6.3 et les versions plus récentes

Pour mettre à niveau avec la réplication du datastore activée, procédez comme suit :

Avant de commencer

- Assurez-vous que vous avez exécuté les étapes décrites à la section Conditions préalables à la mise à niveau à la page 70.
- Si vous utilisez des machines UNIX, assurez-vous que vous le faites en tant qu'utilisateur root.
- Assurez-vous que les processus de chaque étape sont terminés avant de démarrer le processus de l'étape suivante.

Procédure

1. Si vous ne l'avez pas encore fait, sur les serveurs d'applications, arrêtez le service d'application. Exécutez :

   ```
   # dpa app stop
   ```

2. Mettez à niveau le datastore esclave.

   Démarrez le programme d'installation de DPA et suivez les invites.

   Si vous implémentez la réplication en cascade, mettez à niveau le datastore de la fin de la chaîne en premier.

3. Mettez à jour le datastore maître.

   Démarrez le programme d'installation de DPA et suivez les invites.

4. Mettez à jour le ou les serveurs d'applications.

   Démarrez le programme d'installation de DPA et suivez les invites.

5. Assurez-vous que la réplication du datastore est en cours d'exécution. Exécutez :

   ```
   # dpa ds rep
   ```

   Le message STREAMING doit s'afficher.

Mise à niveau avec la réplication de datastore active pour les versions de DPA antérieures à la version 6.3

La mise à niveau avec réplication du datastore est automatisée et ne nécessite pas d'intervention de l'utilisateur, sauf lors de la mise à niveau du datastore esclave de réplication.

Avant de commencer

- Assurez-vous que vous avez exécuté les étapes décrites à la section Conditions préalables à la mise à niveau à la page 70.
- Si vous utilisez des machines UNIX, assurez-vous que vous le faites en tant qu'utilisateur root.
- Assurez-vous que les processus de chaque étape sont terminés avant de démarrer le processus de l'étape suivante.

Procédure

1. Arrêtez tous les services :
   a. Exécutez # dpa app stop sur le serveur d'applications.
   b. Exécutez # dpa ds stop sur le datastore maître.
   c. Exécutez # dpa ds stop sur le datastore esclave.
2. Mettez à jour le datastore maître :
   a. Démarrez le programme d'installation de DPA et suivez les invites.
   b. Assurez-vous que la réplication du datastore est en cours d'exécution. Exécutez : `# dpa ds rep`
3. Créez une copie du datastore maître. Type : `dpa ds rep -e <empty_dir>`
4. Désinstaller le datastore esclave existant.
5. Installez un nouveau serveur de datastore propre avec le même emplacement d'installation que le datastore maître et configurez le serveur de datastore nouvellement installé en tant que datastore esclave. Saisissez : `dpa.sh ds rep --role SLAVE <IP of master>`.

   Ne démarrez et n'arrêtez pas les services.
6. Initialisez le datastore esclave à partir de la copie du datastore maître. Saisissez : `dpa ds rep -i <master_copy>`
7. Démarrez le datastore esclave.
8. Mettez à niveau le serveur d'applications.

Mise à niveau avec la réplication de datastore et les clusters existants

Utilisez cette procédure pour mettre à niveau un système avec la réplication de datastore et les clusters existants.

Avant de commencer

- Assurez-vous que vous exécutez toutes les étapes décrites à la section Conditions préalables à la mise à niveau à la page 70.
- Si vous utilisez des machines UNIX, assurez-vous que vous le faites en tant qu'utilisateur root.
- Arrêtez le répartiteur de charge sur les serveurs d'applications DPA et du datastore. La commande pour arrêter le répartiteur de charge dépend du système d'exploitation. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

Procédure

1. Si vous ne l'avez pas encore fait, arrêtez le service d'application sur les nœuds d'application du cluster :
   a. Arrêtez le serveur d'applications esclave.
   b. Arrêtez le serveur d'applications maître.

   Exécutez :

   ```
   # dpa app stop
   ```
2. Exécutez les étapes fournies dans la section Mise à niveau avec activation de la réplication du datastore pour DPA 6.3 et les versions plus récentes à la page 75.

Si vous mettez à niveau avec une version DPA antérieure à 6.3, suivez les étapes indiquées dans « Mise à niveau avec la réplication de datastore active pour les versions de DPA antérieures à la version 6.3 »

3. Mettez à jour les nœuds d'applications esclaves :
   a. Démarrez le programme d'installation de DPA et suivez les invites.
   b. Attendez que le service d'application démarre. Vérifiez que le fichier `server.log` comprend des sorties semblables à `DPA slave started successfully`.
4. Redémarrez l'application de répartiteur de charge sur les serveurs d'applications DPA et du datastore. La commande de démarrage du répartiteur de charge dépend du système d'exploitation. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

CHAPITRE 3

Administration de DPA

Le présent chapitre contient les sections suivantes :

Gestion des licences

Cette section présente la gestion des licences dans DPA.

Licence d'évaluation fournie avec DPA

DPA est fourni avec une licence d'évaluation de 90 jours.

La licence d'évaluation est créée au moment de l'installation de DPA et est valable durant 90 jours maximum. Elle permet d'accéder à toutes les fonctions. Si vous importez une licence au cours de cette période d'évaluation de 90 jours, la licence d'évaluation est supprimée et votre accès aux fonctions de DPA dépend de la licence que vous avez importée.

Types de licences dans DPA

DPA utilise le type de licence *Common Licensing Platform* (*CLP*).

La licence CLP coexiste avec l'ancienne licence de type *Wysdm Licensing System* (*WLS*) auparavant utilisée avec DPA, avant la modification du nom du produit à DPA, et dans certains cas la remplace.

Coexistence de licences CLP et WLS dans DPA

La licence CLP est requise pour la fonctionnalité DPA.

Si vous n'ajoutez pas de capacité ou n'optez pas pour la nouvelle fonctionnalité DPA et ultérieure à 6.2, l'importation de licences CLP n'est pas nécessaire. Toutefois, si vous procédez à une mise à niveau vers la dernière version de DPA depuis une version antérieure à DPA 6.2, nous vous recommandons de contacter licensing@emc.com après la mise à niveau ou la migration afin d'obtenir de l'aide pour la transition des licences existantes vers les licences CLP, et ceci pour toutes vos licences WLS. Si vous migrez DPA de la version 5.x à la dernière version de DPA, les licences existantes font l'objet d'une migration en même temps que la configuration et les données. Seules les nouvelles fonctions de la dernière de version de DPA ou l'augmentation de la capacité actuelle de la licence nécessitent l'ajout de licences CLP.

Les licences CLP fonctionnent sur un modèle de remplacement. Lorsque vous importez une licence CLP, cette licence remplace toutes les licences existantes du même type. En outre, la fonctionnalité de la licence de base et de la licence d'entreprise est transférée sur chaque licence CLP. Lorsque vous commandez des licences CLP, vous devez connaître le nombre de licences existantes du même type, puis ajouter la nouvelle capacité requise et faire une commande pour la capacité totale. Pour obtenir des informations sur l'achat de licences pour votre installation DPA, contactez votre responsable de compte.

Un système migré ou mis à jour à partir d'une version précédente de DPA contient des licences WLS. WLS et CLP ne peuvent coexister que si la fonctionnalité pour laquelle ces deux licences sont prévues est différente.

Licences arrivées à expiration

Si une licence expire, un avertissement de violation de licence apparaît dans le titre des rapports exécutés à partir de l'ensemble des objets activés par la licence arrivée à expiration. En outre, il devient impossible d'ajouter de nouveaux objets à la console Web pour les composants de module activés par une licence arrivée à expiration.

Suppression de licence

Le retrait d'une licence entraîne l'affichage d'un avertissement de violation de licence lors de l'exécution de rapports sur les objets concernés par cette licence. Des nouveaux objets de ce type ne peuvent plus être ajoutés à la console Web jusqu'à ce qu'une licence de remplacement soit fournie.

Si vous utilisez des licences temporaires avec une date d'expiration, la boîte de dialogue License Expiration apparaît et vous avertit de l'arrivée à expiration de vos licences temporaires. Les licences permanentes ne sont pas affichées.

Ajout de nouvelles licences

Accédez à **Admin** > **System** et cliquez sur **Manage Licenses**.

Désactivation de la fenêtre contextuelle de licence temporaire automatique

Accédez à **User Properties** > **Show License Expiration** et décochez la case.

Utilisateurs et sécurité

Comptes utilisateur

Quatre utilisateurs par défaut sont fournis par défaut dans DPA : administrateur, propriétaire de l'application, ingénieur et utilisateur.

Le compte administrateur est le seul compte actif après l'installation de DPA. L'utilisateur définit le mot de passe du compte administrateur au cours du processus d'installation de DPA.

L'administrateur doit définir des mots de passe pour les autres comptes utilisateur par défaut avant que ces derniers puissent être utilisés pour l'accès à DPA. Si l'administrateur ne définit pas de mots de passe pour les autres comptes utilisateur, ils restent en état désactivé.

Gestion des utilisateurs

L'administrateur DPA peut gérer les comptes utilisateur dans la section **Manage Users**. Accédez à **Admin** > **Users & Security** > **Manage Users**. Dans cette section, l'administrateur peut créer, modifier, afficher et supprimer des comptes utilisateur.

Création d'un compte utilisateur

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage Users**.
2. Cliquez sur **Create User**.

   Vous pouvez également sélectionner un utilisateur existant et cliquer sur **Save As** pour créer une copie d'un utilisateur existant.

3. Dans l'onglet **Create User Properties**, mettez à jour les informations dans les différents onglets :

   a. Dans l'onglet **User Properties** , spécifiez le nom, le nom de connexion, le rôle, le type d'authentification et le mot de passe.

b. Si l'utilisateur doit être authentifié avec LDAP, sélectionnez le type d'authentification LDAP.

c. Dans les onglets **Report Preferences, Preferences and Appearance**, attribuez les préférences et les paramètres d'apparence. Remarque : le rôle que vous attribuez à l'utilisateur détermine les domaines de DPA auxquels il a accès.

d. Cliquez sur **OK** pour confirmer les paramètres.

4. Cliquez sur **Close**.

Modification et suppression de comptes utilisateur

L'administrateur DPA peut modifier ou supprimer tous les comptes utilisateur DPA à l'exception du compte administrateur par défaut.

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage users**.
2. Sélectionnez l'utilisateur à modifier ou à supprimer.
   - Cliquez sur **Edit** pour personnaliser les éléments souhaités, par exemple le nom, le rôle, le mot de passe et les préférences de rapport et de présentation de l'utilisateur.
   - Cliquez sur **Delete** et **Yes** pour le supprimer.
3. Cliquez sur **Close**.

Modifier les mots de passe de comptes utilisateur

L'administrateur DPA peut modifier les mots de passe de compte utilisateur dans **Manage Users**. Les utilisateurs non administrateurs peuvent modifier leur mot de passe dans **View User Properties** en cliquant sur l'icône en forme d'engrenage dans le coin supérieur droit de la console Web DPA.

Procédure

1. Accédez à **Admin** > **Users and Security** > **Manage Users**.
2. Sélectionnez le compte utilisateur dont vous souhaitez modifier le mot de passe, puis cliquez sur **Edit**.
3. Accédez à **Edit User Properties** et définissez **Authentication Type** sur **Password**.
4. Saisissez le nouveau mot de passe dans le champ **Password** et saisissez-le à nouveau dans le champ **Confirm Password**.

   Notez les points suivants concernant le mot de passe de DPA :

   - Les mots de passe vides ne sont pas pris en charge.
   - La longueur minimale est de 9 caractères.
   - Les critères suivants sont obligatoires :
     - Un minimum de 1 lettre majuscule et 1 lettre minuscule
     - Un minimum de 1 caractère numérique
     - Un minimum de 1 caractère spécial

5. Cliquez sur le bouton **OK**.

Paramètres de sécurité

Vous pouvez configurer les paramètres de sécurité utilisateur. Accédez à **Admin** > **Users & Security**

Tableau 16 Stratégie de mots de passe

Paramètre	Description
Nombre minimal de caractères	Le nombre minimal de caractères requis pour le mot de passe de la console web DPA. La valeur minimale est 9. Il n'y a pas de limite maximale de caractères. DPA prend uniquement en charge les caractères latins.
Must user uppercase characters	L'utilisation de lettres majuscules dans le mot de passe de la console web DPA est obligatoire. Option activée par défaut.
Must use lowercase characters	L'utilisation de lettres minuscules dans le mot de passe de la console web DPA est obligatoire. Option activée par défaut.
Must use special characters	L'utilisation de caractères spéciaux dans le mot de passe de la console web DPA est obligatoire. Option activée par défaut.
Must use numeric characters	L'utilisation de caractères numériques dans le mot de passe de la console web DPA est obligatoire. Option activée par défaut.

Tableau 17 Politique d'historique de mot de passe

Paramètre	Description
Password History	Permet de limiter l'historique du mot de passe.
Limit of password history	Le nombre de fois que DPA permet à l'utilisateur d'indiquer un mot de passe identique au précédent. La valeur par défaut est 1. La valeur maximale est 10. Option activée par défaut. Si le paramètre **Limit of password history** est laissée sur **1**, l'utilisateur ne peut pas changer son mot de passe pour l'actuel. Si le paramètre **Limit of password history** est fixé sur plus de 1, l'utilisateur ne peut pas changer son mot de passe pour l'actuel ou pour le précédent. DPA affiche un message indiquant que le mot de passe précédent était déjà configuré et que l'utilisateur doit indiquer un nouveau mot de passe.

Tableau 18 Limite de connexion

Paramètre	Description
Login limit	Active la limite du nombre de tentatives de connexion à la console web DPA.
Limit of login attempts	Le nombre de tentatives que DPA permet à l'utilisateur pour se connecter sur la console web DPA. La valeur par défaut est 5. La valeur est comprise entre 0 et 10.
Lockout timeout	La durée pendant laquelle DPA bloque temporairement l'utilisateur hors de la console web DPA après avoir dépassé la limite de temps de connexion spécifiée. La valeur par défaut est 3 minutes. La plage est de 1 à 60 minutes.

Tableau 19 Password Expiration

Paramètre	Description
Password Expiration	Permet l'expiration du mot de passe. La valeur par défaut est off.
Password expiration period (days)	La durée (en jours) pour laquelle le mot de passe DPA est valide. La valeur par défaut est 90. Le maximum est de 180.

Rôles et privilèges d'utilisateurs

Les rôles sont utilisés pour gérer les privilèges auxquels les utilisateurs ont droit. Pour obtenir leurs privilèges, les utilisateurs se voient tout d'abord attribuer le rôle qui convient.

Quatre rôles sont fournis par défaut au sein de DPA : administrateur, propriétaire de l'application, ingénieur et utilisateur. Les rôles d'utilisateur par défaut sont définis et ne peuvent pas être modifiés.

Le tableau suivant décrit les privilèges de rôle par défaut.

Tableau 20 Rôles Utilisateur

Rôles Utilisateur	Privilèges
Administrator	Peut effectuer toutes les fonctions de configuration et de reporting.
Application owner	Peut effectuer toutes les fonctions de reporting et modifier les paramètres des informations d'identification.
Engineer	Peut effectuer toutes les fonctions de reporting et la plupart des fonctions de configuration. Les ingénieurs ne peuvent ni créer ni modifier d'utilisateur ou de rôle d'utilisateur. Ils ne

Tableau 20 Rôles Utilisateur (suite)

Rôles Utilisateur	Privilèges
	peuvent pas non plus modifier les paramètres du système.
User	Permet d'exécuter des fonctions de reporting.

Création d'un rôle d'utilisateur

L'administrateur DPA peut créer un nouveau rôle d'utilisateur personnalisé avec des paramètres et autorisations personnalisés.

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage Roles**.
2. Cliquez sur **Create Role**, ou sélectionnez un rôle existant et cliquez sur **Save As**.

   Choisissez **Save As** pour créer une copie.
3. Dans la fenêtre **User Role Properties** :
   a. Saisissez un nom et une description pour le nouveau rôle dans les champs **Name** et **Description**.
   b. Définissez les privilèges, les groupes accessibles, les tableaux de bord et les menus.
   c. Cliquez sur **OK** pour confirmer les paramètres.
4. Cliquez sur **Close**.

Modification et suppression de rôles d'utilisateurs

L'administrateur DPA peut modifier ou supprimer uniquement les rôles d'utilisateurs personnalisés. Les rôles par défaut ne peuvent pas être modifiés ou supprimés. Il n'est pas possible de supprimer un rôle tant que d'autre rôles n'ont pas été attribués aux utilisateurs de ce rôle.

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage Roles**.
2. Sélectionnez le rôle d'utilisateur personnalisé à modifier ou supprimer :
   - Cliquez sur **Edit** pour personnaliser les privilèges, les groupes accessibles, les tableaux de bord et les menus.
   - Cliquez sur **Delete** et **Yes** pour supprimer le rôle d'utilisateur.

Affichage des utilisateurs au sein des rôles d'utilisateurs

Accédez à **Admin** > **Users & Security** > **Manage Roles**. L'administrateur DPA peut passer en revue les utilisateurs associés à un rôle d'utilisateur dans l'onglet **Manage Roles**, en sélectionnant le nom d'un rôle utilisateur spécifique. La liste des rôles par défaut (administrateur, propriétaire de l'application, ingénieur, utilisateur) s'affiche, ainsi que tous les nouveaux rôles ajoutés depuis l'installation.

Limitation de l'affichage des utilisateurs à certains groupes spécifiques

Vous pouvez configurer un utilisateur DPA afin qu'il ne voie que des groupes ou des éléments de configuration de sauvegarde spécifiques lors de l'exécution de rapports.

Avant de commencer

Les groupes doivent déjà exister.

Par défaut, les utilisateurs peuvent afficher l'intégralité de l'inventaire d'objets DPA. Toutefois, vous pouvez limiter ce que certains utilisateurs voient dans l'inventaire d'objets DPA. Par exemple, les fournisseurs de services peuvent configurer des groupes dans leur inventaire d'objets DPA, qui correspondent à leurs clients. Les fournisseurs de services peuvent souhaiter une configuration telle que les clients voient et exécutent des rapports uniquement sur un inventaire d'objets spécifique configuré dans leur groupe client lorsqu'ils se connectent à DPA.

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage Roles**.
2. Créez le rôle personnalisé dont vous avez besoin ou sélectionnez le rôle d'utilisateur personnalisé que vous souhaitez modifier, puis cliquez sur **Edit**.
3. Sélectionnez l'onglet **Accessible Groups**.

   La liste des groupes disponibles s'affiche.
4. Sélectionnez le groupe qui sera accessible par le rôle et cliquez sur **>** ou **>>** pour déplacer tous les groupes.
5. Cliquez sur **OK** pour confirmer les paramètres.
6. Cliquez sur **Close**.

Restreindre les groupes d'utilisateurs

Vous pouvez restreindre les groupes d'utilisateurs de manière à ce que certains groupes d'utilisateurs ou rôles puissent définir des valeurs pour des attributs personnalisés sans avoir la possibilité de mettre à jour les attributs de système, de créer ou de modifier des groupes.

Avant de commencer

- Veillez à identifier le serveur DPA en tant qu'administrateur.

Procédure

1. Créez le rôle Read Inventory :
   a. Accédez à **Admin** > **Users & Security** > **Manage Roles** et cliquez sur **Create Role**.

      La boîte de dialogue **User Role Properties** s'affiche.

   b. Renseignez les champs en conséquence :

      Dans le champ **Name**, saisissez le nom que vous souhaitez donner à votre rôle. Par exemple, cliquez sur **Read Inventory**.

      Dans le champ **Description**, saisissez une description si vous le souhaitez.

   c. Dans l'onglet **Privileges**, sous **Inventory**, sélectionnez **View existing objects and group management**.

   d. Dans **Accessible Group**, sélectionnez les groupes que vous souhaitez afficher, cliquez sur **Move selected groups** puis cliquez sur **Close**.

2. Créez l'utilisateur pour Read Inventory :
   a. Accédez à **Admin** > **Users & Security** > **Manage Users** et cliquez sur **Create Role**.

      La boîte de dialogue **Create User Properties** s'affiche.

   b. Renseignez les champs en conséquence :

      Dans le champ **Name**, saisissez le nom que vous souhaitez donner à votre utilisateur. Par exemple, **Read**.

      Dans le champ **Logon**, indiquez l'identifiant que l'utilisateur doit saisir. Par exemple, `Read`.

      Dans le champ **Role**, sélectionnez celui que vous avez créé à l'étape 1 pour le rôle Read Inventory.

      Dans le champ **Authentication**, sélectionnez le type d'authentification souhaitée dans la liste déroulante. Si vous sélectionnez Password, indiquez et confirmez un mot de passe.

   c. Cliquez sur **OK**.
3. Créez le rôle Assign Attribute et Read Inventory :
   a. Accédez à **Admin** > **Users & Security** > **Manage Roles** et cliquez sur **Create Role**.

      La boîte de dialogue **User Role Properties** s'affiche.

   b. Renseignez les champs en conséquence :

      Dans le champ **Name**, saisissez le nom que vous souhaitez donner à votre rôle. Par exemple, **Assign Attribute et Read Inventory**.

      Dans le champ **Description**, saisissez une description si vous le souhaitez.

   c. Dans l'onglet **Privileges**, sous **Inventory**, sélectionnez **Assign/unassign attributes**.

      Le privilège **View existing objects and group management** est sélectionné automatiquement.

   d. Dans l'onglet **Accessible Group**, sélectionnez les groupes que vous souhaitez afficher, cliquez sur **Move selected groups** puis cliquez sur **Close**.
4. Créez l'utilisateur pour Assign Attribute et Read Inventory :
   a. Accédez à **Admin** > **Users & Security** > **Manage Users** et cliquez sur **Create Role**.

      La boîte de dialogue **Create User Properties** s'affiche.

   b. Renseignez les champs en conséquence :

      Dans le champ **Name**, saisissez le nom que vous souhaitez donner à votre utilisateur. Par exemple, **Assign**.

      Dans le champ **Logon**, indiquez l'identifiant que l'utilisateur doit taper. Par exemple, `Assign`.

      Dans le champ **Role**, sélectionnez celui que vous avez créé à l'étape 3 pour les rôles Assign Attribute et Read Inventory.

Dans le champ **Authentication**, sélectionnez le type d'authentification souhaitée dans la liste déroulante. Si vous sélectionnez Password, indiquez et confirmez un mot de passe.

c. Cliquez sur **OK**.

À effectuer

Authentification externe, intégration avec LDAP et liaison

DPA prend en charge la configuration d'une méthode d'authentification externe via l'annuaire LDAP. DPA prend en charge Microsoft Active Directory et OpenLDAP comme serveurs LDAP

Les mots de passe de compte utilisateur ne sont stockés dans le Datastore DPA que lorsque la méthode d'authentification interne est configurée. Dans la méthode d'authentification externe, les mots de passe sont stockés sur le serveur LDAP. Pour activer l'authentification LDAP, sélectionnez **Admin** > **Users & Security** > **Manage External Authentication**.

DPA prend en charge deux méthodes de liaison LDAP : liaison anonyme et liaison simple. Pour configurer une liaison anonyme, assurez-vous que la case **anonymous bind** est cochée dans l'onglet **Manage External Authentication**. Pour une liaison simple, assurez-vous que la case **anonymous bind** n'est pas cochée. En outre, assurez-vous que le nom d'utilisateur et le mot de passe d'un utilisateur avec accès de base en lecture est défini.

Configuration de l'authentification LDAP

Les champs suivants sont utilisés pour la configuration de l'authentification LDAP dans DPA.

Tableau 21 Configuration de l'authentification LDAP dans DPA

Champ	Description
Server	Nom d'hôte du serveur LDAP. Le nom d'hôte doit pouvoir être résolu à partir du serveur DPA.
Use SSL	Sélectionnez cette option pour vous connecter au serveur LDAP à l'aide d'une connexion SSL.
Port	Port sur lequel écoute le serveur LDAP pour les demandes : • port 389 pour les connexions non-SSL • port 636 pour les connexions SSL. Lorsque vous utilisez Microsoft Active Directory configuré en tant que serveur de Catalogue Global, spécifiez les éléments suivants dans la boîte de dialogue Manage External Authentication : • port 3268 pour les connexions non-SSL • port 3269 pour les connexions SSL.
LDAP Version	Version de LDAP utilisée sur le serveur.

Tableau 21 Configuration de l'authentification LDAP dans DPA (suite)

Champ	Description
	DPA prend en charge les versions 2 et 3.
Base Name	Emplacement de tous les utilisateurs potentiels. Cet emplacement est utilisé comme point de départ pour toutes les requêtes auprès de l'annuaire. La valeur saisie doit être le nom unique de la base de l'annuaire, par exemple, DC = eng, DC = entreprise, DC = com.
Identification Attribute	L'attribut LDAP ou Active Directory utilisé pour rechercher un compte utilisateur, par exemple, sAMAccountName (Active Directory) ou uid (OpenLDAP).
Anonymous Bind	DPA prend en charge deux liaisons LDAP distinctes : • Anonyme Bind : cochez la case pour vous connecter au serveur LDAP avec une liaison anonyme. • Simple Bind : ne cochez pas la case pour utiliser la liaison simple. Cela active les champs nom d'utilisateur et mot de passe.
Username	Le nom unique de liaison de l'utilisateur sur le serveur LDAP autorisé à rechercher dans l'annuaire LDAP au sein de la base de recherche définie.
Password	Mot de passe d'utilisateur.
Validate	Cliquez pour tester l'authentification des utilisateurs avec le serveur LDAP. Un message s'affiche, que la connexion au serveur LDAP ait réussi ou non.

Création d'un compte utilisateur avec authentification LDAP

En tant qu'administrateur DPA, après avoir configuré et testé la liaison LDAP, vous pouvez créer ou modifier les comptes utilisateur qui doivent être authentifiés par le serveur LDAP.

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage External Authentication**
2. Définissez la valeur **LDAP** dans le champ **Authentication type**.
3. Fournissez le nom unique de l'utilisateur (DN) ou la valeur d'attribut d'identification dans le champ **External Name**.

   Grâce à l'intégration d'Active Directory, la valeur d'attribut d'identification est généralement sAMAccountName. Avec OpenLDAP, il s'agit généralement de l'UID.

Provisionnement utilisateur automatisé

Le provisionnement utilisateur automatisé est disponible dans DPA lorsqu'il est intégré avec un serveur LDAP. L'activation de la fonction de connexion automatique permet à DPA de créer automatiquement un compte utilisateur lorsqu'un utilisateur se connecte à DPA.

Le rôle d'utilisateur attribué au nouvel utilisateur peut être configuré dans l'onglet **Auto Login**. L'administrateur peut configurer un rôle d'utilisateur par défaut ou un rôle en fonction de mappage de groupe LDAP.

Connexion automatique : rôle d'utilisateur par défaut

Lorsqu'un rôle d'utilisateur par défaut est défini dans l'onglet de connexion automatique, ce rôle est attribué à tous les nouveaux utilisateurs créés automatiquement par DPA. Vous pouvez afficher la liste complète des utilisateurs créés avec la fonction de connexion automatique dans l'onglet **Manage Users**. Ils auront la valeur *LDAPAUTO* dans le champ de type d'authentification.

Procédure

1. Configuration et test de l'intégration LDAP dans DPA.
2. Accédez à **Admin** > **Users & Security** > **Manage External Authentication** > **Auto-login Properties** > **Edit** et marquez **Enable Auto-login**.
3. Sélectionnez un rôle dans la liste déroulante Default User Role.
4. Cliquez sur **OK** pour confirmer les paramètres.
5. Cliquez sur **OK** dans l'onglet **Manage External Authentication** pour le fermer.

   Lorsque vous vous authentifiez à l'aide de la connexion automatique, DPA crée automatiquement un compte utilisateur pour vous au sein de DPA.

Connexion automatique : mappage de groupe LDAP

En tant qu'administrateur DPA, vous pouvez mapper les groupes LDAP spécifiques aux rôles d'utilisateur DPA dans les paramètres de connexion automatique.

Procédure

1. Configurez la connexion automatique avec un rôle d'utilisateur par défaut.
2. Cochez la case **Enable Group Mapping** pour activer le mappage de groupe :
   - Dans le champ **Group Base**, spécifiez le nom unique du groupe. Par exemple, `cn=users,dc=eng,dc=company,dc=com`
   - Dans le champ **Group Attribute**, spécifiez l'attribut LDAP utilisé pour la recherche de groupe. Il s'agit en général de *CN* ou *sAMAccountName* pour Active Directory ou de *uid* pour OpenLDAP.
   - Dans le champ **Group Member Attribute**, indiquez l'attribut qui spécifie les membres du groupe. Il s'agit en général de *member* pour Active Directory ou de *memberUid* pour OpenLDAP.
3. Cliquez sur **Add** pour ajouter une nouvelle ligne à la section **Group Mapping**.
4. Dans **LDAP Group Name**, définissez le nom du groupe à mapper au rôle d'utilisateur.
5. Dans **User Role**, choisissez l'un des rôles disponibles dans la liste déroulante.

6. Utilisez **Add**, **Remove**, **Up** et **Down** pour organiser le mappage du groupe.
7. Cliquez sur **OK** pour confirmer les paramètres
8. Cliquez sur **OK** dans l'onglet **Manage External Authentication** pour le fermer.

Mappage de groupes

La fonction de mappage de groupe permet à DPA de mapper les groupes LDAP spécifiés à des rôles DPA afin qu'il soit possible de vous attribuer différents rôles DPA en fonction des groupes LDAP dont vous êtes membre.

Si vous êtes membre de plusieurs groupes LDAP, vous disposez du rôle DPA qui est mappé avec le premier groupe dans la table de mappage. Assurez-vous que les groupes correspondant à un rôle DPA avec des autorisations supérieures sont en haut de la liste. Le rôle d'utilisateur par défaut est attribué aux utilisateurs qui ne sont pas membres d'un groupe dans la liste de mappage de groupe. Des boutons **Up** et **Down** permettent de déplacer les entrées du tableau vers la position souhaitée.

Configuration de l'intégration LDAP : paramètres de scénario

Dans les scénarios d'intégration LDAP ci-après, les paramètres suivants sont utilisés. Notez que ces paramètres sont uniquement des exemples.

Tableau 22 Ouvrir les paramètres du serveur LDAP

Description des paramètres	Paramètre
Nom du serveur	lab.emc.com
LDAP administrator	cn=admin dc=lab,dc=emc dc=com
Groupes	Administrators : cn=administrators,ou=groups,dc=lab,dc=emc,dc=com
	Users : cn=users,ou=groups,dc=lab,dc=emc,dc=com
	Support : cn=support,ou=groups,dc=lab,dc=emc,dc=com
Utilisateurs	Paul Abbey: uid=PAbbey,ou=people,dc=lab,dc=emc,dc=com (membre des utilisateurs)
	John Smith: uid=JSmith,ou=people,dc=lab,dc=emc,dc=com (membre du support)
	Tom Baley: uid=TBaley,ou=people,dc=lab,dc=emc,dc=com (membre du marketing)

Scénario : Configuration de l'intégration de LDAP avec une liaison simple

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage External Authentication**.
2. Vérifiez ou saisissez les valeurs suivantes dans les champs relatifs à l'utilisateur :

- **Use LDAP Authentication** : sélectionné
- **Server**: `lab.emc.com`
- **Use SSL** : sélectionné (facultatif)
- **Port** : `686`
- **LDAP Version** : `3`
- **Base Name** : `dc=lab,dc=emc,dc=com`
- **Identification Attribute** : `uid (sAMAccountName pour l'intégration Active Directory)`
- **Anonymous Bind** : non sélectionné
- **Username** : `cn=admin,dc=lab,dc=emc,dc=com`
- **Mot de passe** : `<admin_password>`

3. Cliquez sur **Validate** pour vérifier la liaison LDAP.

   Si la validation échoue, vérifiez la connectivité LDAP à partir du serveur d'applications DPA et les paramètres du serveur LDAP.

4. Cliquez sur **Test user** pour vérifier la liaison LDAP.

   Utilisez le nom d'utilisateur et le mot de passe suivants :

   Nom d'utilisateur : `PAbbey`

   Mot de passe : `<PAbbey_password>`

5. Cliquez sur **OK** pour vérifier l'authentification utilisateur LDAP.

   Si l'authentification échoue, vérifiez si le nom d'utilisateur et le mot de passe sont corrects sur le serveur LDAP.

6. Cliquez sur **OK** dans **Manage External Authentication** pour confirmer les paramètres et fermer.
7. Accédez à **Admin** > **Users & Security** > **Manage Users** et cliquez sur **Create User**.
8. Saisissez les valeurs suivantes dans l'onglet **User Properties** :
   - **Name** : `Paul Abbey`
   - **Logon** : `Pabbey`
   - **External Name** : `PAbbey`
   - Role : **User**
   - Authentication Type : **LDAP**
9. Cliquez sur **OK** et vérifiez que le compte est dans la liste des comptes utilisateur.
10. Cliquez sur **Close**.

Scénario : Configuration de provisionnement automatisé avec mappage de groupe

Procédure

1. Accédez à **Admin** > **Users & Security** > **Manage External Authentication**.
2. Vérifiez ou saisissez les valeurs suivantes dans les champs relatifs à l'utilisateur :
   - **Use LDAP Authentication** : sélectionné

- **Server**: `lab.emc.com`
- **Use SSL** : sélectionné (facultatif)
- **Port** : `686`
- **LDAP Version** : `3`
- **Base Name** : `dc=lab,dc=emc,dc=com`
- **Identification Attribute** : `uid (sAMAccountName pour l'intégration Active Directory)`
- **Anonymous Bind** : non sélectionné
- **Username** : `cn=admin,dc=lab,dc=emc,dc=com`
- **Mot de passe** : `<admin_password>`

3. Cliquez sur **Validate** pour vérifier la liaison LDAP.

   Si la validation échoue, vérifiez la connectivité LDAP à partir du serveur d'applications DPA et les paramètres du serveur LDAP.

4. Cliquez sur **Test user** pour vérifier la liaison LDAP.

   Utilisez le nom d'utilisateur et le mot de passe suivants :

   Nom d'utilisateur : `PAbbey`

   Mot de passe : `<PAbbey_password>`

5. Cliquez sur **Edit**.
6. Cochez **Enable Auto Login** et assurez-vous que le rôle d'utilisateur par défaut sélectionné est **User**.
7. Cochez **Enable Group Mapping** et vérifiez ou saisissez les valeurs suivantes :
   - **Group Base** : `ou=groups,dc=lab,dc=emc,dc=com`
   - **Group Attribute** : `cn`
   - **Group Member Attribute** : **memberUid (membre pour l'intégration avec Active Directory)**
8. Cliquez sur **Add**.

   LDAP Group Name:Support

   Role:Engineer

9. Cliquez sur **Close**.
10. Connectez-vous en tant que John Smith.

    Un nouveau compte utilisateur JSmith avec le rôle d'ingénieur doit avoir été créé.

11. Déconnectez-vous.
12. Connectez-vous en tant que Tom Baley.

    Un nouveau compte utilisateur TBaley avec le rôle d'utilisateur doit avoir été créé.

Paramètres système

Vous pouvez modifier les paramètres système par défaut pour les agents DPA, le serveur et le datastore.

Configuration des champs de résolution de sauvegarde et de restauration

DPA vous permet de créer jusqu'à cinq champs de résolution de restauration et de sauvegarde personnalisés qui vous permettent d'ajouter une résolution à une tâche qui a échoué et d'afficher la résolution à une date ultérieure afin de voir ce qui a provoqué l'échec.

Par exemple, vous pouvez créer un champ sous la forme d'une référence à un système d'émission de tickets externe qui comprend davantage d'informations de résolution pour les sauvegardes ayant échoué. Les administrateurs peuvent contrôler le format d'un champ personnalisé et rendre les champs obligatoires ou facultatifs.

Procédure

1. Sélectionnez **Admin** > **System** > **Manage Custom Resolutions**.

   La boîte de dialogue Manage Custom Resolutions s'affiche.
2. Sélectionnez une ligne disponible dans la liste et cliquez sur **Edit**.

   La boîte de dialogue **Resolution Custom Field** s'affiche.
3. Sélectionnez **Active** pour activer le champ personnalisé.
4. Saisissez un libellé pour le champ.

   Le libellé du champ est utilisé dans les boîtes de dialogue **Backup Resolution** et **Add Resolution**.
5. Sélectionnez le type de données du champ personnalisé dans le champ **Input Cast**.

   Les types valides sont les suivants :

   - Indicateur (True ou False)
   - Valeur de nombre entier
   - Valeur décimale
   - Texte
6. (Facultatif) Sélectionnez **Mandatory** pour imposer aux administrateurs de remplir un champ de type texte lors de la création ou de l'ajout de résolutions. Pour d'autres types de champ, la valeur par défaut est utilisée dans la résolution si l'utilisateur ne spécifie pas de valeur.
7. Cliquez sur le bouton **OK**.

À effectuer

Si vous le souhaitez, mettez en œuvre les résolutions de sauvegarde et de restauration dans les rapports d'analyse détaillée :

L'ajout/le visionnement d'actions de la résolution de sauvegarde peuvent être utilisés dans tous les rapports système utilisant le menu d'analyse détaillée de « Job Details Popup ».

1. Accédez à **Reports** > **Report Templates**> **Custom Report Templates**, sélectionnez le rapport que vous souhaitez ajouter à la résolution de sauvegarde, puis cliquez sur **Edit**.
2. Sélectionnez l'onglet **Preview**.
3. Cliquez sur **Drilldowns** pour afficher le menu des rapports d'analyse détaillée, puis sélectionnez **Same drilldown menu for all columns**.

4. Modifiez ou créez le menu contextuel avec les options de résolution :
   a. Sélectionnez **Action** et choisissez l'une des options de résolution de sauvegarde et de restauration :
      - Ajout de la résolution de sauvegarde
      - Ajout de la résolution de restauration
      - Afficher la résolution de sauvegarde
      - Afficher la résolution de restauration

      Les autres options comprennent l'affichage d'alertes sélectionnées, exclusion des modifications, détails des écarts, affichage des alertes associées et demande d'historique.
   b. Sélectionnez **Automatic**.
   c. Cliquez sur le bouton **OK**.

Affichage et modification des paramètres

Pour afficher ou modifier les paramètres système, sélectionnez **Admin** > System > Configure System Settings.

Paramètres système

Le système DPA comporte des paramètres pour les agents de collecte des données, le serveur, SharePoint, l'analyse de la réplication et la découverte sans agent. Le tableau suivant décrit chaque paramètre d'agent.

Tableau 23 Paramètres de l'agent de collecte des données

Paramètre	Description
Data Collection Agent Status	Permet la collecte des fichiers log. Option activée par défaut.
Data Collection Agent Version	La version de l'agent de collecte de données DPA qui est actuellement installée sur l'hôte.
Data Collection Agent Port	Port sur lequel l'agent de collecte de données écoute les demandes.
Concurrency	Nombre maximal de threads que l'agent de collecte de données utilise pour collecter des données. La valeur par défaut est cinq.
Log Level	Niveau de détail auquel l'agent de collecte des données écrit dans le fichier log. Par exemple, si le niveau Fatal est sélectionné, seules les erreurs critiques sont écrites dans le fichier log.
Log File	L'emplacement du fichier log sur l'hôte.
Max Log File Size (MB)	Taille maximale (en Mo) jusqu'à laquelle un fichier journal peut croître avant la création d'un nouveau fichier journal. Pour ne définir aucune limite pour la taille du fichier log, définissez cette valeur sur 0.
Max Number of Log Files	Nombre maximal de fichiers journaux conservés sur le système. Si un nouveau fichier est créé parce que la taille de fichier

Tableau 23 Paramètres de l'agent de collecte des données (suite)

Paramètre	Description
	maximale du fichier log en cours est dépassée, le plus ancien fichier log est supprimé.
Max Forward Queue Length	Nombre maximal de requêtes stockées localement par l'agent si le serveur est hors ligne.
Max Forward Queue Size (MB)	Taille maximale totale (en Mo) de toutes les requêtes stockées localement par l'agent de collecte de données DPA si le serveur est hors ligne. Vous pouvez spécifier un nombre illimité ou une taille sélectionnée.
Reload Data Collection Agent	Vous permet de recharger manuellement l'agent de collecte de données. Cette opération est effectuée automatiquement lorsque des modifications de configuration apportées à la console Web DPA affectent un agent de collecte de données.
Remove Data Collection Agent	Supprime l'agent de collecte de données sélectionné.
Make Agent Default	Fait de l'agent de collecte de données sélectionné l'hôte par défaut.

Tableau 24 Paramètres de serveur

Paramètre		Description
Global Data Collection Agent Settings	Binary Multiplier	Lorsque ce paramètre global est activé, tous les agents utilisent par défaut le multiplicateur binaire. Le multiplicateur binaire convertit toutes les données entrantes comme suit : 1024 Ko= 1 Mo. S'applique aux agents NetWorker uniquement lorsque les données entrantes émanant du serveur de sauvegarde sont converties sur le modèle 1 000 Ko = 1 Mo. Le multiplicateur binaire est ignoré lors de la surveillance d'autres applications.
	Timeout(s)	Paramètre d'expiration du délai que le serveur utilise lorsqu'il parle à l'agent. La valeur par défaut est 120 secondes.
Global Email Settings	Mail Server Hostname	Serveur de messagerie vers lequel les e-mails sont transférés lorsqu'ils sont envoyés à partir de DPA.
	Mail From Address	Adresse e-mail attribuée aux messages e-mail envoyés à partir de DPA.
	Mail Server Port	Numéro de port du serveur de messagerie.
Global Logging Settings	Global Logging Settings	Paramètres généraux de consignation pour le moteur d'analyse, la configuration, Listener, Publisher, l'analyse de la capacité de restauration, Reporter et l'API REST. Ces

Tableau 24 Paramètres de serveur (suite)

Paramètre		Description
		paramètres peuvent être INFO, DEBUG, DEBUG LOW, WARN, ERROR et FATAL.
Data Deletion	Data Deletion	Paramètre programmé pour supprimer les données collectées depuis votre environnement. La valeur par défaut est comprise entre 9h00 et 17h00 tous les jours.
Root Cause Analysis	Root Cause Analysis Settings	Option permettant d'activer le récapitulatif de l'analyse des causes premières.
		Option permettant d'activer la suppression de l'analyse des causes premières. Le paramètre de suppression par défaut supprime les données datant de plus de 200 jours. Cette période n'est pas configurable par l'utilisateur.
Generate Support Bundle	Generate Support Bundle	Option permettant de générer le fichier zip de support.
	Include all logs	Option pour inclure tous les fichiers log. Si elle est désactivée, DPA collecte uniquement les fichiers log les plus récents. Si elle est sélectionnée, DPA collecte tous les fichiers log historiques. Désélectionnée par défaut.
DB Export	Database Export Age Notification	L'option de définition d'une période de temps que la base de données DPA exporte est considérée comme à jour. La valeur par défaut est d'une semaine. Le minimum est de un jour. Une alerte est émise lorsque le délai expire et qu'il n'y a pas de nouvelle exportation de Datastore DPA durant cette période.

Tableau 25 Paramètres SharePoint

Paramètre		Description
Nom	Nom	Le nom défini par l'utilisateur du site SharePoint créé dans les paramètres du serveur SharePoint DPA.
Site	Site URL	L'URL de destination pour les publications de SharePoint. Le protocole HTTP utilise le port 80 par défaut et HTTPS le port 443. Vous pouvez également spécifier le port de manière explicite. Par exemple, pour définir http port 24438 site URL, saisissez : `http://sharepoint-2013:24438/sites/demo2/`.

Tableau 25 Paramètres SharePoint (suite)

Paramètre		Description
Utilisateur	Username	Le nom d'utilisateur associé au compte de SharePoint

Tableau 26 Paramètres d'analyse de la réplication

Paramètre		Description
Analyse de la réplication	Client-Server Time Difference	La valeur par défaut est de 10 minutes.
	Symmetrix and CLARiiON Log Level	Paramètres de connexion pour Symmetrix et CLARiiON. Ces paramètres peuvent être INFO et DEBUG.
	Support Symmetrix Masking Reports	Permet la prise en charge des rapports de masquage Symmetrix. Option activée par défaut.
	Support Application Discovery Impersonation	Permet la prise en charge d'Application Discovery Impersonation. Option activée par défaut.
Paramètres d'affichage	Display dirty Recovery Points	Permet d'afficher les points de restauration non synchronisés. Option activée par défaut.
	Aggregate Recovery Points	Permet d'agréger les points de restauration. Option activée par défaut.
	Nombre minimum de points de restauration à agréger	La valeur par défaut est 3. Le minimum est 1. Il n'existe pas de valeur maximale.

Découverte sans agent

Les paramètres de découverte sans agent sont décrits dans le tableau suivant.

Tableau 27 Paramètres de découverte sans agent

Paramètre	Description
Sudo Program Path	Chemin de programme sudo pour les paramètres de découverte sans agent. Le chemin par défaut est `/usr/local/bin/sudo`. La commande sudo peut également figurer dans `/sbin` ou `/usr/sbin`.
Agent Response Timeout	Temps pendant lequel DPA attend une réponse de l'agent avant que le délai n'expire.

Tableau 27 Paramètres de découverte sans agent (suite)

Paramètre	Description
Telnet/SSH Login Prompt Timeout	Temps pendant lequel DPA attend que la session Telnet/SSH soit créée avant que le délai n'expire.
Telnet/SSH Handshake Timeout	Temps pendant lequel DPA attend le protocole de transfert Telnet/SSH avant que le délai n'expire.
Delete files created on the client during agentless discovery	Détermine si les fichiers temporaires seront supprimés de l'objet analysé à la fin de la découverte. Par défaut, les fichiers sont supprimés.

Suppression des données du serveur

DPA met en œuvre un programme de suppression des données par défaut pour les données collectées et les données générées par le système. Les données collectées sont les données recueillies par les demandes configurées dans le cadre de la gestion des valeurs par défaut de la collecte des données. Les données générées par le système sont les données générées par les processus système, par exemple les messages de journal, les historiques de rapport et les alertes.

Les données dépassant la période de rétention peuvent faire l'objet d'une suppression. Ces données sont ensuite purgées en fonction du programme de suppression des données. Tous les éléments non traités restent dans la file d'attente jusqu'à l'heure de début planifiée suivante, heure à laquelle la suppression des données se poursuit.

Vous ne pouvez pas supprimer un programme actuellement utilisé pour la planification d'une tâche de suppression des données collectées. Un message d'erreur s'affiche si vous essayez de le faire.

Les données collectées et les données générées par le système, puis supprimées, font l'objet d'un suivi dans `server.log`. Par exemple :

```
Deleted 10 rows from table host_config
Deleted 10 rows from Request History
Deleted 10 rows from reportlogentry
Deleted 10 rows from dpa_request_statistics
Deleted 10 rows from reporterjob
```

Le programme de suppression des données par défaut a lieu tous les jours de 9h00 à 17h00.

Configuration du programme de suppression des données

Pour configurer et spécifier un nouveau programme, allez dans Schedule Properties.

Pour configurer la suppression des données, sélectionnez **Admin** > **System** > **Configure System Settings** > **Server** > **Data Deletion**. L'aide en ligne de DPA fournit des informations complémentaires à ce sujet.

Périodes de rétention par défaut

Le tableau suivant fournit des informations sur les périodes de rétention par défaut des données collectées.

Tableau 28 Périodes de rétention par défaut des données collectées

Informations système	Période de rétention par défaut
Données de configuration	365 jours
Données d'état	90 jours
Données de performances	30 jours
Données de tâche	toujours
Données d'occupation	365 jours

Les périodes de rétention par défaut des données collectées sont configurables par l'utilisateur dans **Admin** > **System** > **Manage Data Collection Defaults**.

Le tableau suivant fournit des informations sur les périodes de rétention par défaut des données générées par le système. Les périodes de rétention par défaut des données générées par le système ne sont pas configurables par l'utilisateur.

Tableau 29 Périodes de rétention par défaut des données générées par le système

Policy	Période de rétention par défaut
alertes (table analysisalert)	365 jours
historique de rapport (table reporterjob)	365 jours
entrées du journal d'erreur de l'agent (table reportlogentry)	14 jours
statistiques des demandes (table dpa_request_statistics)	28 jours

Paramètres d'analyse des causes premières

Vous pouvez définir le récapitulatif de l'analyse des causes premières afin de calculer régulièrement les causes premières potentielles, à partir des paramètres des systèmes. Vous pouvez également planifier le système afin d'effacer les données résultantes de l'analyse des causes premières. Le paramètre de suppression de l'analyse des causes premières supprime les données datant de plus de 200 jours. Cette période n'est pas configurable par l'utilisateur. Le récapitulatif et la suppression de l'analyse des causes premières sont activés par défaut.

Désactivation du récapitulatif de l'analyse des causes premières

Sélectionnez **Admin** > **System** > **Configure System Settings** > **Server** > **Root Cause Analysis Settings** > **Disable Root Cause Analysis**, puis cliquez sur **OK**.

Désactivation de la suppression de l'analyse des causes premières

Sélectionnez **Admin** > **System** > **Configure System Settings** > **Server** > **Root Cause Analysis Settings** > **Disable Root Cause Analysis Deletion**, puis cliquez sur **OK**.

Collecte des données de sauvegarde historiques à l'aide de la console Web DPA

Vous pouvez collecter les données de sauvegarde historiques sur Avamar, BackupExec, DB2, HP DataProtector, NetWorker, NetBackup, Oracle RMAN, SAP HANA et TSM.

Lorsque vous collectez les données de sauvegarde historiques à l'aide de la console Web DPA, tenez compte des points suivants :

- Vous ne pouvez pas collecter les données de sauvegarde historiques au niveau de l'hôte. Vous devez descendre d'un niveau dans l'arborescence de configuration, à l'objet d'application. Par exemple, pour collecter les données historiques à partir de NetWorker, vous devez choisir l'objet d'application Networker sous l'objet de niveau hôte.
- Vous pouvez uniquement collecter des sauvegardes historiques à partir de demandes JobMonitor.

Procédure

1. Dans la console Web, sélectionnez **Inventory** > **Group Management**.
2. Dans l'arborescence de configuration, sélectionnez l'objet d'application pour lequel vous souhaitez collecter des données de sauvegarde historiques.

   La fenêtre **Details** de l'objet d'application s'ouvre.
3. Dans la fenêtre des détails de l'hôte, sélectionnez l'onglet **Data Collection**.
4. Dans le champ **Data Collection**, sélectionnez JobMonitor request.
5. Cliquez avec le bouton droit de la souris sur **Run** et sélectionnez **Gather historical data**.
6. Dans la fenêtre **Gather historical data**, cliquez sur **OK**.

   Les mêmes options de données et d'informations d'identification sont disponibles que pour la demande elle-même.
7. Cliquez sur **Close** sur la boîte de dialogue qui s'affiche pour confirmer que DPA collecte les données de sauvegarde historiques.
8. Cliquez sur **History** pour afficher les tests collectés. Les lignes mises en surbrillance orange indiquent les résultats d'une collecte de sauvegardes historiques.

Generate Support Bundle

L'option Generate Support Bundle est un outil de support. L'option Generate Support Bundle génère et enregistre une archive zip avec les ressources fournies dans le système de fichiers, directement à partir de la console Web DPA.

Un ingénieur du support technique EMC peut vous demander de générer un bundle de support et de lui envoyer. Le fichier zip est enregistré en tant que logs suivants de l'agent local dans le dossier `support.zip` :

- dpaagent.log
- dpaagent.log.0
- dpaagent.log.1

L'emplacement par défaut est configurable par l'utilisateur.

Génération du bundle de support

Procédure

1. Sélectionnez **Admin** > **System** > **Configure System Settings** > **Server** > **Generate Support Bundle**, puis cliquez sur **OK**.
2. Lorsque vous y êtes invité, saisissez vos informations d'identification d'administrateur DPA.

Certificat numérique

DPA utilise un certificat numérique auto-signé pour l'identification et le chiffrement. La section Chiffrement du serveur d'applications DPA à la page 68 fournit des informations à ce sujet.

Périodes

Lorsque vous exécutez un rapport ou créez un rapport programmé, vous devez décider de la période pour laquelle le rapport s'exécute, par exemple immédiatement ou la dernière semaine. Plusieurs périodes de temps prédéfinies sont fournies par défaut et vous pouvez créer des périodes de temps personnalisées.

Création d'une période personnalisée pour les rapports

Pour créer une période personnalisée, sélectionnez **Admin** > **System** > **Manage Time Periods**.

Fuseaux horaires dans DPA

DPA collecte les données à partir de l'environnement et les stocke dans la base de données DPA au format UTC.

Si l'horodatage que la base de données DPA reçoit d'un serveur de sauvegarde, d'une application, d'un hôte ou d'un switch est dans un fuseau horaire local, comme EST, l'agent DPA le convertit en UTC avant de les envoyer au serveur DPA. Pour le reporting de ces données, plusieurs paramètres peuvent être définis. Pour plus d'informations, reportez-vous à la section Paramètres de fuseau horaire pour le reporting à la page 102.

Paramètres de fuseau horaire pour le reporting

Vous pouvez définir les paramètres suivants pour les fuseaux horaires afin de vous assurer que le fuseau horaire souhaité s'affiche dans vos rapports DPA.

Détails de l'objet découvert
Après avoir découvert un objet à l'aide du Discovery Wizard, vous pouvez sélectionner les propriétés et choisir de spécifier le fuseau horaire de l'emplacement de cet objet. Dans la fenêtre **Details** de l'objet découvert, sélectionnez **Time zone** dans la liste déroulante.

Préférences utilisateur
Vous pouvez choisir le fuseau horaire dans lequel vous souhaitez afficher les données dans **User Preferences** > **View User Properties** > **Preferences**. Dans la section Global Settings, sélectionnez le fuseau horaire dans la liste déroulante **Time zone**.

Propriétés de la fenêtre
Vous pouvez créer une période de temps tenant compte du fuseau horaire. Dans la fenêtre **Window Properties**, créez une nouvelle période de temps et assurez-vous que l'option **Adjust for time zone** est activée. Si vous sélectionnez **Adjust for time zone** et que l'objet est un client de sauvegarde, DPA vérifie le serveur de sauvegarde parent, si le client de sauvegarde ne dispose pas déjà d'un fuseau horaire défini explicitement, et crée un rapport compatible avec le fuseau horaire.

Format de tableau des rapports
Vous pouvez choisir de configurer un rapport de style tabulaire pour afficher l'objet de fuseau horaire sur lequel il a été exécuté avec l'horodatage, en spécifiant le champ à examiner pour rechercher le nom du serveur de sauvegarde. Dans l'éditeur de rapports, accédez à **Report Format** > **Table Format** > **Table Styles**. Sous la section des champs de Date, assurez-vous que l'option **Time Zone from Report Field** est sélectionnée.

Exemple : Configuration des fuseaux horaires pour le rapport de toutes les tâches

Cet exemple montre comment définir des fuseaux horaires sur un rapport All Jobs pour un serveur NetWorker qui se trouve dans le fuseau horaire Amérique/New York pour un administrateur de base de données qui se trouve dans le fuseau horaire Europe/Londres.

Avant que vous ne modifiiez des paramètres, la sortie du rapport et de l'affichage est au format UTC.

Procédure

1. Accédez à **User Preferences** > **View User Properties** > **Preferences** et sélectionnez **Europe/London** dans la liste déroulante **Time zone** de la section Global Settings. Cliquez ensuite sur **OK**.

   Lorsque vous exécutez le rapport de toutes les tâches sur le serveur NetWorker, DPA affiche le rapport au format UTC.
2. Mettez à jour le fuseau horaire du serveur NetWorker, qui se trouve à New York :
   a. Accédez à **Inventory** > **Object Library**, puis accédez à l'hôte NetWorker.
   b. Sélectionnez l'hôte NetWorker souhaité et, dans la fenêtre **Details**, sélectionnez **America/New York** dans la liste déroulante **Time Zone**.
   c. Cliquez sur **OK**.

   La sortie reste au format UTC, car le paramètre de fuseau horaire de l'utilisateur ou le paramètre de rapport n'ont pas encore été modifiés. Elle ne change pas pour le fuseau horaire Amérique/New York.
3. Création d'une période personnalisée compatible avec le fuseau horaire. Accédez à **Windows Properties** et créez un fuseau horaire personnalisé. Veillez à sélectionner l'option `Adjust for time zone`.

   Ainsi, la requête de rapport pour l'heure devient relative au fuseau horaire de l'objet. Par conséquent, le serveur NetWorker étant situé à New York, DPA exécute la requête pour la période personnalisée dans le fuseau horaire de New York.
4. Modifiez le format de tableau de rapport afin que les champs de date s'affichent dans le fuseau horaire de votre champ Server, au format de date souhaité pour le fuseau horaire :
   a. Dans l'éditeur de rapport, accédez à **Report Format** > **Table Format** > **Table Styles**.

b. Dans la section Date Fields, sélectionnez le format de date souhaité dans la liste déroulante **Date Format** et assurez-vous que l'option `Time Zone from Report Field` est sélectionnée.

c. Cliquez sur le bouton **OK**.

DPA actualise le rapport avec les horodatages du fuseau horaire du serveur NetWorker, dans ce cas, Amérique/New York.

Hiérarchisation automatique des rapports

Le nombre de rapports par défaut pouvant s'exécuter simultanément par serveur d'applications DPA est de 10. Vous pouvez configurer ces paramètres par défaut. Vous pouvez configurer les paramètres par défaut. Le nombre maximal de rapports pouvant s'exécuter simultanément par serveur d'applications DPA est de 50 et le nombre minimum, de 2.

DPA met automatiquement en file d'attente les rapports dont l'exécution simultanée est programmée ou les rapports exécutés simultanément, et récupère automatiquement les rapports lorsque les rapports précédemment programmés ont été exécutés. De plus, les rapports que vous lancez depuis la console Web priment sur les rapports automatisés programmés s'exécutant à partir du serveur, y compris les tests d'alerte planifiée.

Outre la priorité donnée à des rapports s'exécutant depuis la console Web, il existe également un espace simultané fixe d'au minimum 30 % réservé à ces rapports sur le serveur. Par exemple, si 10 accès simultanés sont autorisés, trois espaces d'exécution simultanée sur le serveur sont réservés aux rapports de la console Web. Par conséquent, trois rapports de console Web ou plus sur un maximum de 10 peuvent s'exécuter à un instant donné. Sept rapports programmés seulement peuvent être exécutés simultanément.

Configuration des paramètres de rapports simultanés

Procédure

1. Pour configurer les paramètres de rapports simultanés, sélectionnez **Admin** > **System** > **Configure Report Settings** > **Concurrency**.

À effectuer

Après avoir modifié le paramètre d'accès simultané dans la console Web DPA, veillez à redémarrer le service d'application DPA. S'il s'agit d'un environnement de clusters, redémarrez tous les serveurs d'applications DPA. Cela permet au service moteur de rapports de récupérer la nouvelle valeur d'accès simultanés.

Calendriers

Les calendriers servent à définir quand il convient d'exécuter un rapport programmé ou de générer un bloc de vues du tableau de bord, ou à préciser la fenêtre de sauvegarde spécifiée dans la règle de protection. Plusieurs calendriers prédéfinis sont fournis par défaut et vous pouvez aussi créer des calendriers personnalisés.

Un calendrier comprend des composants qui définissent quand celui-ci produit certains résultats ou exécute certains rapports. L'éditeur de calendrier permet de créer des calendriers de deux façons :

- L'éditeur de base vous permet de créer des calendriers sur une base hebdomadaire uniquement et de modifier le jour et l'heure du calendrier.
- L'éditeur avancé vous permet de créer des calendriers plus complexes en modifiant manuellement les paramètres de calendrier.

Vous pouvez modifier les calendriers créés dans l'éditeur de base à l'aide de l'éditeur avancé. Toutefois, les calendriers créés et enregistrés dans l'éditeur avancé ne peuvent pas être modifiés dans l'éditeur de base.

Création de plannings

Pour créer un planning, sélectionnez **Admin** > **System** > **Manage Schedules**.

Gestion des paramètres par défaut de collecte des données

Une demande DPA contient des données sur la manière de collecter des données à partir d'un objet, et sur le moment où cette opération doit être effectuée. Les valeurs par défaut de la collecte des données sont utilisées comme modèle par le Discovery Wizard pour attribuer des demandes aux objets. Vous pouvez définir les paramètres par défaut globaux dans **Admin > System > Manage Data Collection Defaults**.

Chaque demande est associée à une fréquence de collecte de données et à un ensemble d'options par défaut. Vous pouvez modifier les valeurs par défaut de la collecte de données globale qui seront utilisées par le Discovery Wizard pour certains objets. L'aide en ligne DPA fournit des informations sur la modification de demandes.

Vous pouvez rassembler certains types de données avec DPA sans déployer un agent sur le périphérique surveillé. Pour ce faire, un agent situé sur un autre ordinateur (tel que le serveur DPA) collecte les données à distance. Lors de la collecte de données à distance, l'hôte de l'agent est appelé serveur proxy. L'agent utilise un protocole pour recueillir des données sur l'ordinateur distant et les transmettre au serveur DPA. Le protocole utilisé dépend du type de données collectées.

Pour certains types de périphériques, tels que des switches IP et Fibre Channel, les données doivent toujours être collectées à distance, car il est impossible d'installer un agent directement sur un switch.

Pour configurer la collecte de données à distance dans DPA, configurez les détails lors de l'attribution des demandes. Si le Discovery Wizard a créé les objets, cette configuration est déjà créée. Toutefois, si les détails sur le proxy ou les données d'identification ont changé, modifiez-les en conséquence. Les périodes de rétention des demandes sont définies pour chaque demande dans la boîte de dialogue Edit Request. Le tableau 15 fournit des informations sur les périodes de rétention par défaut des politiques de collecte de données.

Options de demande de collecte de données par module

Les options de demande de collecte de données par module sont décrites dans le tableau suivant.

Tableau 30 Options de demande de collecte de données par module

Module	Nom de l'option	Valeur	Description
ARCserve	dateformat	%d/%m/%Y %T qui correspond aux jour/mois/ année et à l'heure.	Format de date à utiliser. L'option `dateformat` est l'une des options disponibles pour les demandes suivantes : • Surveillance des tâches • État du volume

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			La remarque 1. fournit plus d'informations sur les formats d'heure.
Avamar	capacityfactor	1,075	Facteur décimal de capacité Avamar. L'option `capacityfactor` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	dbname	mcdb	Nom de la base de données. L'option `dbname` est l'une des options disponibles pour les demandes suivantes : • Configuration • Surveillance des tâches • Demandes d'état
	dbport	5555	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes : • Configuration • Surveillance des tâches • Demandes d'état
	amount of seconds in the job collection	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution de surveillance des tâches. La valeur par défaut est 86400, ce qui correspond à 1 jour, exprimé en secondes. La valeur est configurable.
Backup Exec	dbserver	Aucune valeur par défaut	Serveur/instance de base de données. L'option `dbserver` est l'une des options disponibles pour les demandes suivantes : • Configuration • Surveillance des tâches • État • État du volume

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
CLARiiON VNX	Connector	Aucune valeur par défaut	Indique le connecteur pour la demande d'importation d'informations clariion
	EventLog History Polling	21	Ancienneté des données (en jours) au-delà de laquelle elles ne sont plus incluses dans la recherche, pour une demande d'importation d'informations clariion
Celerra	port	Aucune valeur par défaut	Numéro des ports HTTPS/HTTP (nombres entiers). L'option `port` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
	secure	True	Indique que les demandes sont envoyées via HTTPS au lieu de HTTP. L'option `secure` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	timeout	1 800	Délai d'expiration de la demande HTTP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
CommVault Simpana	appversion	0	Version de CommVault Simpana à utiliser. L'option `appversion` est l'une des options disponibles pour les demandes suivantes : • Configuration • Capacité client • Surveillance des tâches • État • État du volume

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	dbserver	Aucune valeur par défaut	Nom du serveur DB. L'option `dbserver` est l'une des options disponibles pour les demandes suivantes : • Configuration • Capacité client • Surveillance des tâches • État • État du volume
	setBackupJobsWithErrsToSuccess	False	Si ce paramètre est défini sur *True*, DPA rapporte les sauvegardes commvault qui se terminent avec l'état *Completed w/one or more errors* en tant que travaux réussis. L'option `setBackupJobsWithErrsToSuccess` est présente dans la demande de surveillance des tâches.
Data Domain	timeout	10	Valeur du délai d'expiration SSH en secondes. L'option `timeout` pour SSH est l'une des options disponibles pour les demandes suivantes : • Analyse • Configuration SSH • Performance SSH • État SSH • SSH PCR
	timeout	10	Valeur du délai d'expiration SNMP en secondes. L'option `timeout` pour SNMP est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
Data Protector	timeout	900	Valeur du délai d'expiration en secondes pour l'exécution de commandes dans le cadre d'une demande de configuration

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	timeout	300	Valeur du délai d'expiration en secondes pour l'exécution de commandes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • la base de données interne • Surveillance des tâches • Service Status • État • État du volume
	ignorefailedclones	False	Indique que les informations sur les objets sources pour les tâches de clonage qui ont échoué ne sont pas collectées, pour la demande de surveillance des tâches.
	nojobmedia	False	Indique que les informations sur les médias associées à chaque tâche ne sont pas collectées, pour la demande de surveillance des tâches.
	occupancy	False	Indique que la collecte des statistiques de capacité est activée, pour la demande de surveillance des tâches.
	timeformat	Aucune valeur par défaut	Format d'heure omnidb pour la demande de surveillance des tâches. La remarque 2. fournit plus d'informations sur les formats d'heure.
DB2	amount of seconds in the job collection	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution de surveillance des tâches. La valeur par défaut est 86400, ce qui correspond à 1 jour, exprimé en secondes. La valeur est configurable.
	Port de la base de données	50 000	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes : • Surveillance des tâches

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
EDL	timeout	10	Valeur du délai d'expiration SNMP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
Fibre Channel Switch	timeout	10	Valeur du délai d'expiration SNMP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
Host System Monitoring	disk	True	Indique que les informations sur le disque hôte sont consignées, pour la demande de configuration et de réplication.
	ESXRequestParameters.ESX_CREDENTIALS	Aucune valeur par défaut	Informations d'identification associées au serveur ESX pour la demande de configuration et de réplication
	ESXRequestParameters.ESX_SERVER	Aucune valeur par défaut	Nom du serveur ESXServer à utiliser pour la demande de configuration et de réplication
	fchba	True	Inclut des informations sur les adaptateurs HBA FC. L'option `fchba` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État
	fs	True	Inclut des informations sur le système de fichiers de l'hôte. L'option `fs` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	host	True	Inclut des informations sur l'hôte de base. L'option `host` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • État
	logical	False	Inclut les interfaces réseau logiques. L'option `logical` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État
	memory	True	Inclut des informations sur la mémoire de l'hôte. L'option `memory` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État
	netint	True	Inclut des informations sur l'interface réseau de l'hôte. L'option `netint` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État
	remote	False	Inclut des systèmes de fichiers montés à distance. L'option `remote` est l'une des options disponibles pour les demandes suivantes : • Configuration et réplication • Performance • État
	REPLICATION_MONITORING_OPTION	False	Active la surveillance de la réplication pour la demande de configuration et de réplication.
	srm	True	Utilise des bibliothèques srm pour des informations disk/fs pour la

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			demande de configuration et de réplication.
	Time Offset (secondes)	0	Décalage de temps en secondes, pour la demande de configuration et de réplication
	disk	True	Inclut des informations sur le disque hôte. L'option `disk` est l'une des options disponibles pour les demandes suivantes : • Performance • État
	fullpath	False	Inclut le chemin complet du nom de processus pour la demande d'état.
	process	True	Inclut des informations sur les processus s'exécutant sur l'hôte pour la demande d'état.
	specific	Aucune valeur par défaut	Surveillez le processus nommé uniquement pour la demande d'état ; Windows uniquement.
Illuminator clarapi Engine Discovery	TIME_OFFSET_OPTION	0	Décalage de temps en secondes, pour la demande de découverte du moteur Illuminator clarapi
HP Disk Array	port	5989	Port du fournisseur CIM pour les baies de disques HP EVA. L'option `port` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
HP Virtual Library System	port	5989	Port vers les baies de disques HP VLS. L'option `port` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	SSLflag	True	La balise SSL est activée pour les baies de disques HP VLS. L'option `SSLflag` est l'une des options disponibles pour les demandes suivantes : • Configuration

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• État
	timeout	600	Délai d'expiration en secondes pour les baies de disques HP VLS. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
Illuminator symapi Engine Discovery	Symapi Version	Aucune valeur par défaut	Indique la version SYMAPI pour la demande de découverte du moteur Illuminator symapi.
	TIME_OFFSET_OPTION	0	Décalage de temps en secondes. L'option `TIME_OFFSET_OPTION` est l'une des options disponibles pour les demandes suivantes : • illuminator symapi engine discovery • Importation des informations symmetrix
	Autorisation de la gestion via SRDF	False	Permet la gestion via SRDF pour la demande de découverte du moteur Illuminator symapi.
	SYMAPI DB Path	Aucune valeur par défaut	Indique le chemin d'accès de la base de données SYMAPI pour la demande de découverte du moteur Illuminator symapi.
Switch IP	timeout	10	Délai d'expiration en secondes pour les demandes d'état, de performance et de configuration
Base de données SQL Server	dbparams	Aucune valeur par défaut	Spécification XML par paramètres de base de données/informations d'identification. L'option `dbparams` est l'une des options disponibles pour les demandes suivantes : • Configuration • Surveillance des tâches • État
	dbport	1433	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes :

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• Configuration • Surveillance des tâches • État
	HomeDir	Aucune valeur par défaut	Informations sur les répertoires d'accueil des applications pour la demande de découverte des applications mssql
	Tools Director	Aucune valeur par défaut	Informations sur les propriétés du répertoire d'outils pour la demande de découverte des applications mssql
	Virtual Computer Name	Aucune valeur par défaut	Informations sur les propriétés du nom de l'ordinateur virtuel pour la demande de découverte des applications mssql
NearStore	timeout	10	Valeur du délai d'expiration SNMP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
NetBackup	timeout	3600	Délai d'expiration de la commande en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Capacité client • Configuration • Surveillance des tâches • État du serveur de média • État • État du volume
	timeout	30	Délai d'expiration de la commande, en minutes. L'option `timeout` est présente dans les options de la demande d'état de tâche SLP.
	EMMserver	Aucune valeur par défaut	Nom d'hôte du serveur EMM (Enterprise Media Manager) ; uniquement requis s'il ne s'agit pas de l'hôte Master Server. L'option

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			`EMMserver` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	timeformat	Aucune valeur par défaut	Format de date/heure d'expiration de la licence pour la demande de configuration
	timeformat	Aucune valeur par défaut	Format d'heure bpdbjobs pour la demande de surveillance des tâches Les remarques 1. et 2. fournissent plus d'informations sur les formats d'heure.
	partialasfailed	False	Marque les tâches partiellement exécutées comme ayant échoué pour la demande de surveillance des tâches.
	Whether to include container jobs	False	Si ce paramètre est défini sur `True`, DPA collecte également la ligne de la tâche parent/conteneur, en plus des tâches enfant. Peut être défini pour la demande par défaut ou pour des objets individuels.
	command timeout	300	Délai d'expiration en secondes, utilisé pour l'exécution des commandes externes afin de collecter des données L'option `command timeout` est présente dans la demande d'état de tâche SLP.
	Intervalle maximal de données que regroupera chaque demande.	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution d'un état de tâche SLP. La valeur par défaut est 86400, ce qui correspond à 1 jour, exprimé en secondes. La valeur est configurable.
NetWorker	command timeout	3600	Délai d'expiration en secondes, utilisé pour l'exécution des commandes externes afin de collecter des données

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			L'option `command timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • État • État du client • Surveillance des tâches • Capacité • État du volume
	mminfo timeformat	Aucune valeur par défaut	Format dans lequel les horodatages dans la base de données des médias sont renvoyés (dans le format d'heure bpdbjob). Utilisé pour décoder l'heure de début/fin d'une tâche. Par défaut, cette option est désactivée et le module tente de calculer automatiquement cette valeur. L'option `mminfo timeformat` est présente dans la demande de surveillance des tâches.
	include jobs from media DB	True	Vous permet de désactiver la recherche de tâches réussies à partir de la base de données des médias de NetWorker. DPA effectue une recherche dans la base de données des médias en plus de la base de données des tâches NetWorker pour retrouver les tâches terminées. Si vous n'utilisez pas un ordonnanceur externe pour démarrer des sauvegardes, définissez ce paramètre sur `False` pour accélérer l'exécution de la demande de surveillance des tâches L'option `include jobs from media DB` est présente dans la demande de surveillance des tâches.
	max batch period of each request data poll	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution de surveillance des tâches. La valeur par défaut est 86400, ce qui correspond à 1 jour,

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			exprimé en secondes. La valeur est configurable.
NetWorker	individual ping timeout	10	Délai d'expiration en secondes, utilisé comme délai d'attente des réponses des clients de sauvegarde suite à la commande ping L'option `individual ping timeout` est présente dans la demande d'état du client.
	nsrexecd port	7937	Port d'écoute du processus client NetWorker. L'option `nsrexecd port` est présente dans la demande d'état du client.
	Number of concurrent pings	20	Nombre de clients sur lesquels une commande ping est exécutée simultanément. L'option `Number of concurrent pings` est présente dans la demande d'état du client.
	List of critical clients to ping	Aucune valeur par défaut	Nom du fichier qui contient la liste des clients stratégiques séparés par des virgules, sur lesquels une commande ping doit être exécutée (plutôt que sur tous les clients). L'option `List of critical clients to ping` est présente dans la demande d'état du client.
	Chemin et nom du fichier utilisé pour stocker les données d'occupation temporaires avant le traitement	Aucune valeur par défaut	Chemin et nom du fichier utilisé pour stocker les données d'occupation temporaires avant le traitement. La valeur doit être un chemin valide sur l'hôte de l'agent. Par exemple, sous Windows, utilisez `C:\temp` et, sous UNIX/Linux, utilisez `/tmp`. Vous devrez peut-être redémarrer l'agent après l'activation pour que l'option prenne effet. L'option `Path and name of file used to store temporary occupancy data before processing` est présente dans la demande d'occupation.

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	Forces short client names	true, false	Indique s'il faut revenir à la version abrégée du nom du client ou pas. L'option `Forces short client names` est l'une des options disponibles pour les demandes suivantes : • Configuration • État • État du client • Surveillance des tâches • Capacité client
	time format used to determine bootstrap time	False	Spécifie le format horaire utilisé pour décoder les horodatages renvoyés dans les résultats à partir de NetWorker. Par défaut, cette option n'est pas activée et le module utilise la meilleure supposition pour décoder le format horaire. L'option `time format used to determine bootstrap time` est présente dans la demande d'état.
	time format used to determine volume access time	False	Format horaire à utiliser lors du décodage des horodatages concernant l'heure du dernier accès à un volume. Par défaut, cette option n'est pas définie et le module tente de calculer un format horaire automatiquement. L'option `time format used to determine volume access time` est présente dans la demande de volume.
	time format used to determine volume retention period	False	Format horaire à utiliser lors du décodage des horodatages concernant la rétention des médias pour un volume. Par défaut, cette option n'est pas définie et le module tente de calculer un format horaire automatiquement. L'option `time format used to determine volume retention`

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			`period` est présente dans la demande de volume.
	Whether to include failed jobs which are retried	False	L'agent DPA ne collecte que l'état final d'une procédure de sauvegarde. Si l'option de la tâche est définie sur `False` et que le délai est important avant son exécution, la nouvelle tentative échoue et ceci retarde le reporting de l'échec de la tâche. Si la nouvelle tentative réussit, la base de données DPA comporte une entrée pour la tâche, et cette entrée indique que la tâche est réussie. Si l'option de la tâche est définie sur `True`, l'agent DPA collecte toutes les tentatives qui ont échoué et l'état final de la tâche, et les envoie à la base de données DPA. Par exemple, si la tâche fait l'objet d'une seule nouvelle tentative et qu'elle réussit, la base de données DPA enregistre 2 entrées pour la tâche (1 échec et 1 succès). Si les deux tentatives échouent, la base de données DPA enregistre 2 entrées pour la tâche dans la base de données DPA, les deux en tant qu'échecs. Vous pouvez utiliser le rapport All Jobs - No Restarts pour filtrer les tentatives infructueuses et afficher seulement l'état final de la tâche.
Oracle	dbparams	Aucune valeur par défaut	Spécification XML par paramètres de schéma/informations d'identification. L'option `dbparams` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	dbport	1521	Port de la base de données (nombre entier). L'option `dbport` est l'une des options disponibles pour les demandes suivantes : • Configuration

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• État
	HomeDir	Aucune valeur par défaut	Informations sur les répertoires d'accueil des applications pour la demande de découverte des applications Oracle
	ArchivesPattern	Aucune valeur par défaut	Informations sur le schéma d'archive des applications pour la demande de découverte des applications Oracle
	LogPattern	Aucune valeur par défaut	Informations sur le schéma de log des applications pour la demande de découverte des applications Oracle
	LogsDir	Aucune valeur par défaut	Informations sur le répertoire de log des applications pour la demande de découverte des applications Oracle
PostgresSQL Database	dbparams	Aucune valeur par défaut	Spécification XML par paramètres de schéma/informations d'identification. L'option `dbparams` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	dbport	5432	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	initialdb	postgres	Base de données d'origine pour se connecter à ce port. L'option `initialdb` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
PureDisk	dbport	10085	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes : • Capacité client • Configuration

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• Surveillance des tâches
	dbserver	Aucune valeur par défaut	Hôte du serveur de base de données. L'option `dbserver` est l'une des options disponibles pour les demandes suivantes : • Capacité client • Configuration • Surveillance des tâches
RecoverPoint	scanforrecover	False	Analyse pour la capacité de restauration pour la demande de configuration
	Time Offset (in seconds)	0	Décalage de temps en secondes, pour la demande de configuration
	timeout	300	Valeur du délai d'expiration SSH en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance cs • Performance
	filename	long_term_stats.tar.gz	Nom de fichier de statistiques pour la demande de performance cs
	workdir	../tmp	Répertoire de travail pour la demande de performance cs
RecoverPoint for VMs	Time Offset (in seconds)	0	Décalage de temps en secondes, pour la demande de configuration
	timeout	300	Valeur du délai d'expiration de l'API REST en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance CS • Performance • État
RMAN	dbport	1521	Port d'écoute Oracle TNS. L'option `dbport` est l'une des options disponibles pour les demandes suivantes :

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• Fichier de contrôle de la surveillance des tâches • Catalogue de restauration de la surveillance des tâches
	amount of seconds in the job collection	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution de surveillance des tâches. La valeur par défaut est 86400, ce qui correspond à 1 jour, exprimé en secondes. La valeur est configurable.
	Schéma RMAN	Aucune valeur par défaut	
SAP HANA	Port de la base de données	30115	Port de la base de données pour la demande de surveillance des tâches
	amount of seconds in the job collection	86400	Modifie le temps d'exécution maximal de la demande de collecte de données sur les tâches en une seule exécution de surveillance des tâches. La valeur par défaut est 86400, ce qui correspond à 1 jour, exprimé en secondes. La valeur est configurable.
Symmetrix	Connector	Aucune valeur par défaut	Indique le connecteur pour la demande d'importation d'informations symmetrix
	Gather HBA Information	True	Collecte d'informations sur les adaptateurs HBA pour la demande d'importation d'informations symmetrix
	Time Offset (in seconds)	0	Décalage de temps en secondes, pour la demande de configuration
	Symaudit History Polling	21	Ancienneté des données (en jours) au-delà de laquelle elles ne sont plus incluses dans la recherche, pour une demande Symaudit
Tape Library	timeout	10	Délai d'expiration SNMP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • État

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
TSM	timeout	Aucune valeur par défaut	Délai d'expiration interne pour les commandes envoyées au serveur TSM en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Capacité client • Surveillance des tâches • Surveillance des processus • État du volume
	timeout	3600	Délai d'expiration interne pour les commandes envoyées au serveur TSM en secondes, pour la demande de configuration
	timeout	900	Délai d'expiration interne pour les commandes envoyées au serveur TSM en secondes, pour la demande d'état
	tsmhost	Aucune valeur par défaut	Nom d'hôte du serveur TSM. L'option `tsmhost` est l'une des options disponibles pour les demandes suivantes : • Capacité client • Configuration • Surveillance des tâches • Surveillance des processus • État • État du volume
	tsmport	1500	Port du serveur TSM. L'option `tsmhost` est l'une des options disponibles pour les demandes suivantes : • Capacité client • configuration • Surveillance des tâches • Surveillance des processus • état • État du volume

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	disableprivatevolumes	False	Désactive le reporting des volumes privés. L'option `disableprivatevolumes` est l'une des options disponibles pour les demandes suivantes : • Configuration • État du volume
	backupsets	True	Indique si les jeux de sauvegardes doivent être collectés pour la demande de surveillance des tâches.
	filterbynoderegtime	True	Filtre les tâches manquées avant l'enregistrement des nœuds pour la demande de surveillance des tâches
	Whether to gather failed jbos from the activity log	False	Si cette option est activée et définie sur `True`, les messages du log d'activité TSM qui indiquent un échec de sauvegarde sont également signalés comme étant en échec dans DPA. L'option `Whether to gather failed jbos from the activity log` est présente dans la demande de surveillance des tâches.
	processingtype	Aucune valeur par défaut	Source des tâches de traitement pour la demande de surveillance des tâches. Elle peut être SUMMARY ou ACTLOG.
	OPTION_LIB_MANAGER_CRED	OptionDefinition.Type.Credential	Informations d'identification du gestionnaire de bibliothèques pour la demande d'état du volume
	ignorewarnings	Aucune valeur par défaut	Les codes d'avertissement à traiter comme ayant réussi (chaîne séparée par des virgules).
VMware	port	443	Port du serveur VMware. L'option `port` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
	timeout	3600	Délai d'expiration interne pour les commandes envoyées à l'hôte VMware en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
	usessl	True	Utilise SSL via HTTP. L'option `usessl` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
	vmwarehost	Aucune valeur par défaut	Nom d'hôte du serveur VMware. L'option `vmwarehost` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
VMware vSphere Data Protection (VDP)	capacityfactor	1,075	Facteur décimal de capacité. L'option `capacityfactor` est l'une des options disponibles pour les demandes suivantes : • Configuration • État
	dbname	mcdb	Nom de la base de données. L'option `dbname` est l'une des options disponibles pour les demandes suivantes : • Configuration • Surveillance des tâches • Demandes d'état
	dbport	5555	Port de la base de données. L'option `dbport` est l'une des options disponibles pour les demandes suivantes :

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
			• Configuration • Surveillance des tâches • Demandes d'état
VPLEX	port	443	Port HTTPS/HTTP pour la demande de configuration
Webserver	page	Aucune valeur par défaut	Page Web à obtenir pour la demande de réponse
	port	80	Port du serveur Web. L'option `port` est l'une des options disponibles pour les demandes suivantes : • Configuration • Réponse
Xsigo	timeout	10	Valeur du délai d'expiration SNMP en secondes. L'option `timeout` est l'une des options disponibles pour les demandes suivantes : • Configuration • Performance • État
Remarque Les formats d'heure suivants sont pris en charge :	1.	• %c - Spécifique aux paramètres régionaux • %x %X - Spécifique aux paramètres régionaux : autre format • %m/%d/%y %I:%M:%S %p - Format de date américain codé en dur 12 heures • %m/%d/%Y %I:%M:%S %p • %d/%m/%y %I:%M:%S	Les éléments des formats de date et d'heure se comprennent comme suit : • %c : date et heure au format défini par le paramètre régional actuel • %x : date au format défini par le paramètre régional actuel • %X : heure au format défini par le paramètre régional actuel • %m : mois sous forme de nombre entier (1 à 12) • %d : jour du mois sous forme de nombre entier (00 à 31) • %y, %Y : année sans le siècle, sous forme de nombre entier (0 à 99) • %I : heure au format 12 heures (1 à 12) • %M : minutes sous forme de nombre entier (0 à 59)

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
		%p - Format de date européen codé en dur 12 heures • %d/%m/%Y %I:%M:%S %p • %m/%d/%y %r • %m/%d/%Y %r - Spécifique aux paramètres régionaux • %d/%m/%y %r • %d/%m/%Y %r • %d/%m/%y %T • %d/%m/%Y %T • %m/%d/%y %T • %m/%d/%Y %T • %x - Spécifique aux paramètres régionaux • %m/%d/%Y • %m/%d/%y • %d/%m/%y • %d/%m/%Y • %d.%m.%Y %T	• %S : secondes sous forme de nombre entier (0 à 59) • %p : équivalent AM/PM du paramètre régional • %r : heure au format am/pm 12hr • %T : heure, alias pour heures:minutes:secondes.
	2.	• %c • %x %X	

Tableau 30 Options de demande de collecte de données par module (suite)

Module	Nom de l'option	Valeur	Description
		• %x, %X	

Gérer les sites

Vous pouvez définir l'attribut `Site` dans la boîte de dialogue des propriétés de l'objet, comme `Credentials` et `Schedule`. Vous pouvez assigner l'attribut `Site` à tous les objets de niveau supérieur et aux composants.DPA ne prend pas en charge l'assignation de l'attribut `Site` à des groupes d'objets. Les objets sont consultables par l'attribut `Site`.

Aller à **Admin** > **System** > **Manage Sites** pour ajouter, modifier et supprimer des sites.

Création, modification et suppression de sites

Procédure

1. Aller à **Admin** > **System** > **Manage Sites**

   La fenêtre **Manage Sites** s'affiche.
2. Si vous souhaitez :
   - Créer un site :
     a. Cliquez sur **Create Site**.
     La boîte de dialogue **Create Site** apparaît.
     b. dans le champ **Site Name**, tapez un nom pour votre site.
     c. Dans le champ **Location**, saisissez trois caractères ou plus correspondants à l'emplacement géographique le plus proche de votre site, puis sélectionnez le lieu lui correspondant le mieux.
     d. Cliquez sur **Select Location** puis **OK**.
   - Modifier un site :
     a. Sélectionnez le site que vous souhaitez modifier dans la liste de sites. La boîte de dialogue **Edit Site** apparaît.
     b. Modifiez le champ souhaité et cliquez sur **OK**.
   - Supprimer un site :
     a. Sélectionnez le site que vous souhaitez supprimer dans la liste de sites. La boîte de dialogue **Delete Site** apparaît.
     b. Confirmer ou annuler la suppression du site, selon le cas.

Administration du service d'application

Exécution de l'application DPA Linux en tant qu'utilisateur non-root

Par défaut, l'application DPA s'exécute sous l'utilisateur root avec Linux. Effectuez cette procédure sur le serveur d'applications DPA afin de configurer l'application DPA pour une exécution en tant qu'utilisateur non-root.

Procédure

1. arrêtez le service d'application DPA. Saisissez : **`dpa app stop`**
2. Créez un utilisateur de système d'exploitation à utiliser pour l'exécution de l'application DPA.

   Sinon, sélectionnez le nom d'utilisateur du système d'exploitation `apollosuperuser` à utiliser pour l'exécution de l'application DPA à partir du groupe `dpaservices`.

   L'utilisateur `apollosuperuser` est créé lors de l'Installation de DPA.
3. Transférez la propriété du répertoire d'installation des services DPA à l'utilisateur du système d'exploitation qui exécutera l'application DPA. Saisissez : **`chown --dereference -LR <user_to_run_dpa>:<group_of_user> <dpa_install_dir>/services`**
4. Modifiez le fichier `<dpa_install_dir>/services/executive/applnsvc.sh`. Modifiez la ligne **`RUN_AS_USER=`** to **`RUN_AS_USER=<user_to_run_dpa>`**.
5. Démarrez le service d'applications DPA. Saisissez : **`dpa app start`**
6. (Facultatif) Si vous avez configuré des scripts tiers, comme un script de prétraitement pour les rapports planifiés, un script de post-traitement dans les paramètres de publication ou des scripts pour les politiques d'analyse, modifiez les scripts pour l'utilisateur du système d'exploitation vers `<user_to_run_dpa>`, comme indiqué dans l'étape 4.

   L'application DPA peut recevoir un refus d'autorisation pour l'exécution de scripts sous un nouvel utilisateur de système d'exploitation, s'ils s'exécutaient précédemment sous l'utilisateur root.

Configuration de la version du protocole TLS en 1.2 postérieure à une installation ou à une mise à niveau

Vous ne pouvez définir la version du protocole TLS comme 1.2 qu'après l'installation ou la mise à niveau de DPA à l'aide de la commande `dpa application tlslevel`.

Procédure

1. Arrêtez le serveur d'applications DPA. Type :

   dpa app stop
2. Exécutez la commande `dpa application tlslevel` pour définir le protocole TLS comme version 1.2 uniquement. Type : **`dpa app tls 1.2`**
3. Démarrez le serveur d'applications DPA. Type :

   dpa app start

Personnalisation des informations de service

Cette section fournit des informations sur les types de personnalisation du service DPA pouvant uniquement être mis en œuvre par un administrateur. Vous devez disposer d'un accès physique à l'hôte sur lequel DPA s'exécute.

Le document *Guide produit de Data Protection Advisor* fournit des informations sur la personnalisation des viewlets, des tableaux de bord et des rapports. Les utilisateurs peuvent effectuer ces personnalisations.

Modèles de VTL

Lorsque le processus Publisher crée des rapports lors de la publication au format HTML, il utilise les modèles de la VTL situés dans le répertoire `vtltemplates` sur le serveur DPA pour déterminer la mise en page et le style par défaut du rapport. Par défaut, le serveur DPA utilise les fichiers de modèle suivants : `reportcard.vtl`, `chart.vtl` et `table.vtl`. Vous pouvez néanmoins utiliser un autre fichier de modèle. Vous pouvez créer des fichiers de modèle pour modifier l'apparence des rapports publiés par le processus du serveur DPA.

Les types de modèle disponibles sont les suivants :

- Default utilise la VTL par défaut pour le mode d'affichage.
- pivot permet de générer des tableaux croisés dynamiques.
- pivot.css permet de générer des tableaux croisés dynamiques à l'aide de CSS.
- pivot.controlpanel.css permet de générer des tableaux croisés dynamiques dans les panneaux de configuration à l'aide de CSS.

Le tableau suivant présente les modèles de VTL.

Tableau 31 Modèles de VTL

Modèle de VTL	Description	Type de modèle
chart.vtl	Utilisé par les modes d'affichage graphiques qui produisent une image pour la sortie HTML, par exemple Aire, Colonne, Ligne, Secteur, Topologie.	Par défaut
chart.controlpanel.css.vtl	Identique à chart.vtl, mais utilise CSS.	s.o.
chart.css.vtl	Identique à chart.vtl, mais utilise CSS	css
email.attach.vtl	Utilisé lorsque le rapport est envoyé sous forme de pièce jointe à un e-mail.	s.o.
email.image.embed.vtl	Utilisé pour incorporer le rapport à l'e-mail.	s.o.
email.notification.vtl	Utilisé pour créer la notification qui peut être envoyée après la publication d'un rapport.	s.o.

Tableau 31 Modèles de VTL (suite)

Modèle de VTL	Description	Type de modèle
healthstatus.vtl	Utilisé pour l'état de santé.	Par défaut
healthstatus.controlpanel.css.vtl	Identique à healthstatus.vtl, mais utilise CSS. Ne contient pas non plus la date et la version dans la partie inférieure	s.o.
healthstatus.css.vtl	Identique à healthstatus.vtl, mais utilise CSS	css
reportcard.vtl	Utilisé pour les comptes rendus.	Par défaut
reportcard.controlpanel.css.vtl	Identique à reportcard.vtl, mais utilise CSS. Ne contient pas non plus la date et la version dans la partie inférieure	s.o.
reportcard.css.vtl	Identique à reportcard.vtl, mais utilise CSS	css
table.controlpanel.css.vtl	Identique à table.vtl, mais utilise CSS. Ne contient pas non plus la date et la version dans la partie inférieure	s.o.
table.vtl	Utilisé pour les tableaux.	Par défaut
table.css.vtl	Identique à table.vtl, mais utilise CSS	css
table.pivot.controlpanel.css.vtl	Identique à table.pivot.vtl, mais utilise CSS. Ne contient pas non plus la date et la version dans la partie inférieure	pivot.controlpanel.css
table.pivot.css.vtl	Identique à table.pivot.vtl, mais utilise CSS	pivot.css
table.pivot.vtl	Utilisé pour les tableaux croisés dynamiques.	tableau croisé dynamique
timeline.vtl	Utilisé pour les graphiques de chronologie. Le langage HTML est incorporé à la VTL.	Par défaut
timeline.controlpanel.css.vtl	Identique à timeline.vtl, mais utilise CSS. Ne contient pas non plus la date et la version dans la partie inférieure	s.o.
timeline.css.vtl	Identique à timeline.vtl, mais utilise CSS	css

Exemple : 1re partie : ajout d'un message et des informations sur l'entreprise au modèle de VTL

Si vous êtes chargé d'envoyer aux clients des rapports quotidiens ou hebdomadaires au format HTML à l'aide de rapports planifiés, vous pouvez ajouter du texte personnalisé (un message ou les coordonnées de l'entreprise) au rapport planifié en créant un modèle de VTL personnalisé. Le texte personnalisé s'affiche pour tous les rapports HTML utilisant ce modèle.

Procédure

1. Dans le répertoire `styles` ou `vtltemplates` du serveur DPA, copiez le modèle du tableau, `table.vtl`, et renommez-le. Par exemple, si vous créez un modèle de VTL pour les rapports tabulaires d'EMC, utilisez la dénomination standard `table.<companyName.vtl` , puis renommez le modèle par `table.emc.vtl`
2. Ouvrez la VTL dans un éditeur de texte.
3. En utilisant des balises HTML, ajoutez du texte similaire à celui ci-dessous dans le corps du message.

```
<body bgcolor="$background"><font face="Arial, Verdana,
                Helvetica, Sans-serif" color="$foreground">

<body>
Dear customer,
<p>
Your daily system status report is below.
<p>
Thank you,<br>
EMC Corporation
<p>
US Phone:1-800-555-5555<br>
Email:support@EMC.com<br>
Website: www.EMC.com
<p>
<table>
...
</table>
</body>
```

4. Enregistrez la VTL.

Exemple : 2e partie : utilisation d'un modèle de VTL personnalisé dans un rapport planifié

À présent que vous disposez d'un modèle de VTL personnalisé, sélectionnez cette VTL dans l'Assistant Scheduled Report.

Procédure

1. Dans la console Web de DPA, créez un rapport planifié ou mettez-en un à jour.
2. Dans **Publish Settings**, sélectionnez le format de rapport Web Page (.html) et remplissez les champs restants.
3. Dans **Advanced**, sélectionnez le modèle EMC et cliquez sur **OK**. Le modèle nommé Default correspond au modèle table.vtl non modifié.
4. Cliquez sur l'icône de test pour envoyer le rapport planifié au processus Publisher. Si vous effectuez la publication dans un fichier, passez au répertoire par défaut pour afficher le rapport, puis apportez les mises à jour nécessaires au

modèle de VTL. Le répertoire par défaut du rapport est :<install-dir\services\shared\report-results\scheduled.

5. Si aucune autre mise à jour n'est requise pour le modèle de VTL, enregistrez-le puis fermez l'éditeur de rapport planifié.

Importation et exportation de modèles personnalisés

Vous pouvez importer et exporter des modèles de rapport et de tableau de bord personnalisés depuis les versions DPA 5.5.1 et ultérieures vers DPA à partir d'un fichier WDS via la section Custom Templates. L'importation et l'exportation depuis/vers XML ne sont pas prises en charge. Par ailleurs, il est impossible d'importer ou d'exporter des modèles système. Les rapports importés doivent être pris en charge sur DPA.

Vous pouvez importer et exporter des modèles de rapport et de tableau de bord personnalisés pour répondre aux besoins suivants :

- Importer des rapports personnalisés depuis DPA 5.x.
- Importer des rapports personnalisés créés par EMC Professional Services.
- Exporter des rapports personnalisés afin de les sauvegarder.
- Exporter un rapport personnalisé qui ne fonctionne pas afin de l'envoyer au Support Clients d'EMC pour dépannage.

Pour plus d'informations sur l'importation et l'exportation de modèles de rapport personnalisés, consultez le système *Aide en ligne de Data Protection Advisor*.

Administration de clustering

Ajout d'un serveur d'applications à un cluster après le déploiement DPA

Suivez cette procédure pour modifier un serveur d'applications DPA installé en tant qu'un serveur autonome, l'état par défaut de l'installation, afin qu'il fasse partie d'un cluster après le déploiement et la mise en œuvre de DPA à l'aide de l'interface de ligne de commande DPA.

Avant de commencer

- Arrête les agents DPA.
- Si vous utilisez des machines UNIX, assurez-vous que vous le faites en tant qu'utilisateur root.

Les commandes utilisées dans cette procédure sont formatées pour UNIX.

Procédure

1. Si vous ne configurez pas le nœud comme esclave, passez à l'étape 2. Si le serveur d'applications autonome est un nœud esclave au sein du cluster, videz les files d'attente de messages :
   a. Arrêtez les agents de collecte des données.
   b. Vérifiez que le dossier `/opt/emc/dpa/services/standalone/data/messaginglargemessages` ne comporte aucun message. S'il ne comporte aucun message, passez à l'étape d.
   c. Si le dossier `/opt/emc/dpa/services/standalone/data/messaginglargemessages` n'est pas vide, exécutez l'appel REST suivant sur les deux nœuds d'application, maître et esclave :

      Opération HTTPS : `GET`

URL REST : https://<hostname>:9002/dpa-api/support/queues?name=DLQ

La sortie doit inclure une ligne semblable à la suivante : `<currentTotalMessageCount>21</currentTotalMessageCount>`

Dans cet exemple, >21< doit correspondre au nombre de fichiers dans le dossier `messaginglargemessages folder /opt/emc/dpa/services/standalone/data/messaginglargemessages`. Si le nombre de fichiers ne correspond pas, attendez que la file d'attente de la messagerie soit vide.

2. Définissez la taille du pool de connexions à la base de données dans tous les nœuds du datastore. Exécutez :

   # dpa ds tune --connections xxx <RAM>GB où *xxx* représente environ 250 pour chaque serveur d'applications. Par exemple, 500 pour un cluster à deux nœuds.

   Si le cluster est activé pour la réplication de datastore, exécutez cette commande pour tous les datastores esclaves.

3. Si vous n'exécutez pas UNIX, passez à l'étape 4. Si vous utilisez des machines UNIX, augmentez le nombre de descripteurs de fichier sur le serveur d'applications UNIX :

   a. Modifiez le fichier `edit /etc/sysctl.conf` pour ajouter la ligne **fs.file-max = 512000**

   b. À l'invite, exécutez la commande **# sysctl -p**.

   c. Modifiez le fichier `/etc/security/limits.conf` pour ajouter la ligne *** - nofile 65535**.

   d. À l'invite, exécutez la commande **# ulimit - n 65535**.

4. Arrêtez le serveur d'applications sur le premier nœud. Exécutez :

   # dpa app stop

5. Faites passer le serveur d'applications à un état permettant le clustering. Exécutez :

   dpa app promote --role MASTER --bind <MASTER_IP> --path <Chemin d'accès au partage de réseau>

   La commande `dpa app promote` utilise le port multidiffusion par défaut 239.1.2.10. Vous pouvez spécifier un autre port multidiffusion comme paramètre facultatif à cette commande. Assurez-vous que tous les nœuds de cluster utilisent la même adresse multidiffusion.

6. Démarrez le serveur d'applications. Exécutez :

   # dpa app start

7. Vérifiez dans `server.log` que ce nœud a démarré en tant que maître.

   Un cluster ne peut comporter qu'un seul nœud maître.

8. Installation des nœuds esclaves supplémentaires.

À effectuer

Appliquez la configuration suivante après la mise à niveau :

- Paramètres de configuration de rapport
  1. Connectez-vous à la console Web DPA.
  2. Accédez à **Admin** > **System**, puis à **Configure Report Settings** > **Concurrency** .
  3. Définissez le paramètre **Maximum Concurrent Reports per Application server** sur **6** pour le cluster.

Suppression d'un serveur d'applications d'un cluster

Vous pouvez supprimer un serveur d'applications d'un cluster à l'aide de l'interface de ligne de commande DPA, afin de le reconvertir en serveur autonome.

Procédure

1. Sur le serveur d'applications, saisissez `dpa application stop` pour arrêter le service d'application. Le service d'application doit être arrêté avant son retrait d'un cluster.
2. Sur le serveur d'applications, saisissez `dpa application demote` pour dégrader l'application d'un cluster en cours d'exécution.
3. Sur le serveur d'applications, saisissez `dpa application configure` pour vérifier que l'application est supprimée du cluster.

   Il s'affiche en tant que type `STANDALONE`.
4. Sur le serveur d'applications, saisissez `dpa application start` pour démarrer le service d'application et restaurer la fonctionnalité du serveur d'applications.

   Commande dpa CLI à la page 142 offre davantage d'informations sur les commandes CLI de clustering DPA.

Considérations relatives aux clusters lors de la modification des mots de passe

Si le mot de passe de l'utilisateur du domaine est modifié, vous devez désinstaller et réinstaller le nœud d'application DPA.

- Exécutez les commandes suivantes :

```
dpa app uninstall
dpa app install  --user (DOMAIN\username) --password (password)
```

où :

- (*DOMAIN**username* d'utilisateur) correspond au compte utilisateur à utiliser pour l'exécution du service d'application. Les droits Ouvrir une session en tant que service de Windows doivent également être activés.
- <password> correspond au mot de passe de l'utilisateur spécifié.

Administration du service de datastore

Notez les limitations suivantes associées à la réplication de datastore :

- Dans les environnements à fort taux d'utilisation, il est recommandé d'arrêter les serveurs d'applications pour exporter la réplication de datastore, afin que l'exportation puisse être finalisée et importée sur le datastore esclave, avant de la resynchroniser avec le datastore maître.

- DPA prend en charge les exportations de réplication du datastore depuis le datastore maître uniquement. DPA ne prend pas en charge les exportations de réplication du datastore exécutées à partir du datastore esclave.

Sauvegarde du datastore

Il est recommandé de sauvegarder le datastore DPA régulièrement, et en particulier avant d'apporter toute modification majeure au DPA comme la mise à niveau vers une version plus récente ou la migration vers un nouveau matériel. L'exportation des contenus du datastore fait partie d'une sauvegarde complète de l'instance DPA.

L'exportation et l'importation d'un datastore DPA ne sont prises en charge que sur la même version de datastore DPA.

Exportation du datastore DPA

Avec cette commande d'exportation, une copie complète et cohérente du datastore est exportée dans le système de fichiers local, à un emplacement qui peut éventuellement être spécifié.

Le dossier/sous-répertoire par défaut de l'exportation est : datastore-<*version*> <*date and time*>.

Par exemple, `datastore-6_3_0_90597-2017-10-01-1135`.

Saisissez la commande suivante depuis une invite de ligne de commande. **`dpa datastore export [options]`**

Par défaut, le dossier de datastore exporté est sauvegardé dans le même répertoire que celui dans lequel la commande d'exportation a été exécutée.

Pour sauvegarder le dossier de datastore exporté dans un répertoire spécifique, indiquez l'emplacement à la fin de la ligne de commande. Par exemple, la ligne de commande suivante exporte le dossier vers `C:\` car il s'agit de l'emplacement spécifié : **`C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:\`**

Exportation du datastore DPA dans un pipe

Avec ce format d'exportation, une copie complète et cohérente du datastore est diffusée dans un canal nommé à partir d'un emplacement d'où Avamar peut lire le contenu.

Saisissez la commande suivante depuis une invite de ligne de commande. **`dpa datastore export --pipeline`**

Par exemple, **`dpa datastore export --pipeline /mydir/mypipe`**

DPA prend en charge la sauvegarde jusqu'à Avamar à l'aide de la commande `ds export` et la transfère directement vers Avamar. Pour plus d'informations sur le transfert d'une sauvegarde vers Avamar à l'aide de « canaux nommés », consultez la documentation Avamar.

Après l'exportation du datastore

La commande `dpa ds export` produit un dossier qui contient tous les fichiers d'exportation du datastore DPA. Apprenez-en davantage sur les actions recommandées pour ce dossier.

Vous devez sauvegarder le dossier qui contient tous les fichiers d'exportation du datastore DPA avec Avamar, NetWorker ou toute autre application de sauvegarde.

Si vous utilisez Avamar, vous devez d'abord restaurer le contenu, puis ensuite procéder à l'importation sur DPA.

Si vous utilisez NetWorker, envisagez de placer ces dossiers d'exportation du datastore dans un système de fichiers distinct et utilisez la méthode de sauvegarde en mode bloc de NetWorker pour sauvegarder ce dossier efficacement.

Importation du datastore DPA

L'option de ligne de commande `dpa datastore import` sert à importer le contenu d'un fichier de datastore dans le datastore DPA.

Procédure

1. arrêtez le service d'application DPA.
2. Importez le datastore.
3. Démarrez le serveur d'applications DPA.
4. Depuis une invite de ligne de commande, saisissez la commande suivante :

   `dpa app stop dpa datastore import [options] <filename> dpa app start` where *<filename>* désigne le fichier de datastore exporté précédemment. La commande `import` remplace le contenu existant du datastore par celui du fichier d'exportation du datastore.

À effectuer

Pour obtenir la liste complète des commandes de CLI DPA, saisissez **`dpa --help`** depuis une invite de ligne de commande. Pour plus d'informations, reportez-vous à la section Opérations de ligne de commande DPA à la page 142.

Administration de la réplication de datastore

Configuration de la réplication du datastore après déploiement

Suivez cette procédure pour configurer la réplication du datastore sur un système qui est déjà installé et opérationnel. Notez que les commandes de l'interface de ligne de commande fournies dans cette section sont formatées pour Linux RHEL.

Procédure

1. Confirmez que le serveur de datastore est installé en tant qu'esclave. Si tel n'est pas le cas, configurez le serveur de datastore en tant que datastore esclave. Exécutez la commande **`dpa.sh ds rep --role SLAVE <IP of master>`** pour configurer le serveur de datastore en tant qu'esclave.
2. Suivez la procédure décrite à la section Intégration du datastore esclave après qu'il a été mis hors ligne à la page 140.

Configuration de la réplication en cascade du datastore

Vous pouvez configurer une réplication en cascade du datastore après l'installation, uniquement avec l'interface de ligne de commande DPA. Avec la réplication en cascade du datastore, le datastore maître est répliqué vers une chaîne de datastores esclaves, l'un d'entre eux pouvant être distant. Notez que les commandes de l'interface de ligne de commande fournies dans cette section sont formatées pour Linux RHEL.

Avant de commencer

- Arrêtez tous les serveurs d'applications. Type : **`dpa.sh app stop`**
- Arrêtez tous les serveurs de datastore. Type : **`dpa.sh ds stop`**

- Le répertoire d'installation pour le datastore doit être identique sur chaque machine de datastore pour que la fonctionnalité d'importation/exportation fonctionne.

Procédure

1. Sur le datastore maître, exécutez les commandes suivantes :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role master
   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --addSlave <ip_of_replicating_slave> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

2. Sur le datastore esclave de réplication, exécutez les commandes suivantes :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role replicating_slave <ip_of_master> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --addSlave <ip_of_slave> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

3. Sur le datastore esclave, exécutez les commandes suivantes :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --role slave <ip_of_replicating_slave> <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

4. Synchronisez les datastores esclaves avec la dernière copie de datastore depuis le datastore maître :

   a. Pour chaque datastore, créez un répertoire vide sur le datastore maître dans lequel exporter le jeu de fichiers du datastore maître.

      Par exemple, `/tmp/export`.

   b. Sur le datastore maître, exécutez la commande suivante et assurez-vous que le datastore maître reste en cours d'exécution lorsque vous exécutez la commande

      dpa.sh ds rep --export /tmp/export

   c. Utilisez la plate-forme appropriée pour copier par commande les fichiers dans le répertoire vide, sur le datastore esclave.

   d. Sur le datastore esclave de réplication, exécutez les commandes suivantes :

      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

   e. Sur le datastore esclave, exécutez les commandes suivantes :

      <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/export <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

5. Vérifiez que la réplication fonctionne sur les datastores. Exécutez la commande :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep

   Le résultat de la réplication du datastore esclave ressemble à ce qui suit :

```
<DPA_HOME>/emc/dpa/services/logs # /binary/emc/dpa/
services/bin/dpa.sh ds rep

Data Protection Advisor
```

```
[INFO] Replication State : REPLICATING_SLAVE (for
10.11.111.110)
[INFO] Defined Slaves
                        : 10.11.111.111/12

[INFO]                                      SLAVE       BYTES
LAG      STATUS
[INFO]                             10.11.111.111
0      streaming

[INFO] SLAVE is behind the MASTER by 0 [HH:MM:SS]

Command completed successfully.
```

6. Démarrez les serveurs d'applications. Type : **dpa.sh app start**

À effectuer

Si le datastore maître échoue, vous pouvez transformer le datastore esclave de réplication ou le datastore esclave en un nouveau datastore maître pour que DPA puisse continuer à fonctionner. Pour plus d'informations, reportez-vous à la section Réalisation d'un basculement sur incident du serveur datastore à la page 139.

Réalisation d'un basculement sur incident du serveur datastore

Lorsque le datastore maître échoue, effectuez un basculement sur incident vers le datastore esclave.

Avant de commencer

Assurez-vous que le datastore esclave est en cours d'exécution.

Procédure

1. Sur le datastore esclave, saisissez :

   dpa.sh ds rep --failover

2. Arrêtez le serveur d'applications. Type :

   dpa.sh app stop

3. Reconfigurez le serveur d'applications pour qu'il pointe sur le nouveau datastore maître. Type :

   dpa.sh app con -m <hostname/IP of new MASTER>

4. Assurez-vous que le datastore est en cours d'exécution. Type :

   dpa.sh ds status
   Le résultat est `INSTALLED`, `STOPPED` ou `RUNNING`.

5. S'il n'est pas en cours d'exécution, démarrez-le. Type :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start

6. Démarrez le serveur d'applications. Type :

   dpa.sh app start

Reconfiguration des datastores

Utilisez cette procédure si vous avez basculé sur votre datastore esclave et que vous souhaitez reconfigurer l'ancien datastore maître en datastore esclave.

Procédure

1. Sur le nouveau datastore maître, utilisez la commande **addSlave** avec l'adresse IP du nouveau datastore maître. Type :

   ```
   dpa.sh ds rep --addSlave <ip_of_master>
   ```

2. Redémarrez le nouveau datastore maître. Type :

   ```
   dpa.sh ds restart
   ```

3. Exportez le nouveau datastore maître. Type :

   ```
   dpa.sh ds rep --export /export
   ```

4. Configurez le nouveau datastore esclave en tant que SLAVE. Type :

   ```
   dpa.sh ds rep --role SLAVE <ip of MASTER>
   ```

5. Arrêtez le datastore esclave. Type :

   ```
   dpa.sh ds stop
   ```

6. Importez le datastore maître sur le datastore esclave. Type :

   ```
   dpa.sh ds rep --import /import
   ```

7. Démarrez le serveur du datastore esclave. Type :

   ```
   dpa.sh ds start
   ```

Intégration du datastore esclave après qu'il a été mis hors ligne

Cette procédure n'est valable que si la réplication du datastore a été configurée au préalable et que le datastore esclave est hors service. Cette procédure s'applique également si vous introduisez la réplication du datastore dans un déploiement déjà opérationnel. Vous réintégrez ensuite un datastore esclave.

La réplication du datastore reprend automatiquement après de courtes périodes hors ligne, par exemple, après un redémarrage du serveur d'applications. Le datastore est configuré pour supporter environ 6 heures d'interruption de service avant qu'une réinitialisation ne soit nécessaire. Cette valeur reste toutefois approximative et un serveur soumis à une charge importante peut nécessiter une réinitialisation s'il a été arrêté sur une période plus courte. Nous vous recommandons d'effectuer des tests pour déterminer le seuil dans le cas de votre déploiement.

Cette procédure s'applique également à la resynchronisation d'un datastore esclave autonome après isolement. Il existe plusieurs exemples d'isolement, comme une panne réseau ou une rupture des communications entre les datastores maîtres et esclaves.

Procédure

1. Créez un répertoire vide sur le datastore maître dans lequel exporter les fichiers du datastore maître. Par exemple, `/tmp/export`
2. Exportez les fichiers du datastore maître depuis le datastore maître en cours d'exécution. Type :

   ```
   dpa.sh ds rep --export /tmp/export
   ```

3. Créez un répertoire vide sur le datastore esclave dans lequel copier les fichiers du datastore maître.
4. Utilisez la plate-forme appropriée pour copier par commande les fichiers dans le répertoire vide, sur le datastore esclave.
5. Importez le datastore esclave. Type :

<DPA_HOME>/emc/dpa/services/bin/dpa.sh ds rep --import /tmp/import
où <DPA_Home> est l'emplacement de l'installation DPA.

6. Démarrez le serveur du datastore esclave. Type :

   <DPA_HOME>/emc/dpa/services/bin/dpa.sh ds start où <DPA_Home> correspond à l'emplacement de l'installation DPA. L'état du datastore esclave à ce stade est STARTED.

7. Vérifiez que la réplication fonctionne correctement. Sur le datastore maître, saisissez :

   bin/dpa.sh ds rep
   Une sortie telle que celle présentée ci-dessous sur le datastore esclave s'affiche :EMC Data Protection Advisor [INFO] Replication State : SLAVE (for 10.11.111.112) Command completed successfully.

   Si l'esclave a été arrêté et redémarré, une sortie telle que celle présentée ci-dessous, indiquant le décalage d'octets et l'état du *rattrapage* sur le datastore maître s'affiche :

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                         : 10.11.111.111/12

[INFO]                                      SLAVE
BYTES LAG      STATUS
[INFO]                              10.11.111.111
11245376      catchup

Command completed successfully.
```

   Une fois le décalage rattrapé, une sortie telle que celle présentée ci-dessous, indiquant l'état *streaming* s'affiche :

```
EMC Data Protection Advisor

[INFO] Replication State : MASTER
[INFO] Defined Slaves
                         : 10.11.111.111/12

[INFO]                                      SLAVE
BYTES LAG      STATUS
[INFO]
10.11.111.111               0      streaming

Command completed successfully.
```

Arrêt de la réplication du datastore

Pour arrêter la réplication du datastore, arrêtez le datastore esclave. Sur le datastore esclave, saisissez **dpa.sh ds stop**.

Mot de passe de superutilisateur de la base de données DPA

Un seul compte superutilisateur de base de données DPA est fourni dans le datastore DPA : apollosuperuser. apollosuperuser est en fait l'utilisateur qui détient la base de données DPA et qui peut supplanter toutes les restrictions d'accès au sein de la base de données DPA.

Par défaut, la base de données DPA est accessible à l'aide de ce compte uniquement à partir de la machine locale. La commande CLI `dpa datastore superpassword` offre la possibilité de modifier le mot de passe apollosuperuser. La section commandes dpa datastore de la *Guide d'administration et d'installation de Data Protection Advisor* fournit des informations.

Opérations de ligne de commande DPA

Recherche de la source du fichier de configuration DPA pour les utilisateurs UNIX

Un ingénieur du support technique peut vous demander de vous procurer le fichier de configuration DPA avant d'exécuter tout fichier binaire d'agent (y compris une demande d'agent DPA en mode débogage et bkupjob) et toute opération de ligne de commande sous UNIX.

Procédure

1. Accédez au dossierDPA du répertoire d'installation `/etc`.
2. Exécutez la commande suivante :

Résultats

```
cd <DPA install dir>/agent/etc
. ./dpa.config
```

Le fichier de configuration DPA installe diverses variables d'environnement et divers chemins que l'agent DPA utilise. L'exécuter lorsque vous y êtes invité garantit que ces données sont correctement définies dans le shell dans lequel l'utilisateur travaille. Le non-respect de cette procédure lorsque celle-ci est demandée par un ingénieur du support technique peut entraîner l'échec de la commande CLI.

Commande dpa CLI

Dans une installation DPA par défaut, la commande dpa CLI se trouve dans le répertoire `<install_dir>/services/bin` sous UNIX et Linux, et dans `<install_dir>\services\bin` sous Windows.

Utilisez la syntaxe suivante :
Pour Windows :

```
dpa <service_part> <command> [options]
```

Pour Linux/UNIX :

```
dpa.sh <service_part> <command> [options]
```

où <service_part> correspond à une application, un datastore, un agent ou un service. Le composant de service inclut les services de datastore, d'agent et d'application.

```
dpa application <command> [options]
```

```
dpa datastore <command> [options]
```

```
dpa agent <command>
```

```
dpa service <command> [options]
```

La commande DPA server `start/stop/restart` s'applique à tous les services installés uniquement sur l'hôte actuel. Par exemple, si vous exécutez la commande **`dpa server stop`** sur le datastore DPA, les services qui s'exécutent sur le serveur d'applications DPA ne sont pas arrêtés.

Exemples d'abréviations de commandes et d'options

La commande dpa prend en charge les abréviations de commandes. Le tableau suivant répertorie certaines de ces abréviations. Reportez-vous à la commande dpa pour connaître les options disponibles pour cette commande.

Tableau 32 Abréviations des commandes et des options

Commande et option	Abréviation
--add	-a
--bind	-b
--cluster	-c
--delete	-d
--help	-h
--master	-m
--pipeline	-p
--platform	-p
tune	tun
dpa application	dpa app
dpa datastore	dpa ds
dpa service	dpa svc

commandes dpa agent

Utilisez les commandes dpa agent pour gérer le service agent DPA. Les commandes de l'agent dpa peuvent être appliquées uniquement à l'agent local.

```
dpa agent start
dpa agent stop
dpa agent status
dpa agent restart
dpa agent install
dpa agent uninstall

dpaagent --set-credentials
```

Après avoir démarré, arrêté ou redémarré un service, il peut s'écouler quelques minutes avant que le changement ne s'opère.

dpa agent start

Lance l'agent DPA. Le service d'agent doit être installé et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa agent start
```

dpa agent stop

Arrête l'agent DPA. Le service d'agent doit être installé et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa agent stop
```

dpa agent status

Affiche l'état du service d'agent. Par exemple, RUNNING, STOPPED.

```
dpa agent status
```

dpa agent restart

Redémarre le service Agent. En premier lieu, cette commande arrête le service d'agent, puis redémarre le service. Le service d'agent doit être en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa agent restart
```

dpa agent install

Installe le service d'agent. Les service d'agent fonctionne comme un service géré par le système à l'aide des commandes de service du système d'exploitation. La gestion du cycle de vie du service peut également s'effectuer via cet outil de ligne de commande.

Cette commande installe le service, mais ne le démarre pas automatiquement. Si le service d'agent est déjà installé, cette commande échoue.

```
dpa agent install
```

dpa agent uninstall

Désinstalle le service d'agent.

```
dpa agent uninstall
```

dpaagent --set-credentials

Définit le mot de passe d'inscription de l'agent DPA. Cette commande se trouve dans les emplacements de fichier suivants :

- Sous Unix et Linux : `<agent_install_dir>/agent/bin`
- Sous Windows : `<agent_install_dir>\agent\bin`

```
dpaagent --set-credentials
```

Notez les points suivants concernant le mot de passe de l'agent :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

C:\Program Files\EMC\DPA\agent\bin>dpaagent --set-credentials

```
DPA
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
agents use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

Commandes d'application dpa

Utilisez les commandes d'application dpa pour gérer le service d'application DPA.

```
dpa application  [options]
dpa application agentpwd [options]
dpa application adminpassword [options]
dpa application configure [options]

dpa application dspassword [options]
dpa application demote [options]

dpa application install [options]
dpa application importcertificate [options]
dpa application ping [options]
dpa application promote [options] [<Application Server_IP_Address>]
dpa application restart [options]
dpa application start [options]
dpa application status [options]
dpa application stop [options]
dpa application support [options] <ESRS_IP address>
dpa application tls [options]
dpa application tune <value>MB|GB [options]
dpa application uninstall [options]
dpa application version [options]
```

Après avoir démarré, arrêté ou redémarré un service, il peut s'écouler quelques minutes avant que le changement ne s'opère.

dpa application adminpassword

Réinitialise le mot de passe d'administrateur DPA. Vous devez exécuter la commande alors que le service de datastore est en cours d'exécution.

```
dpa application adminpassword [options]
dpa app pwd [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Notez les points suivants concernant le mot de passe d'administrateur :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

C:\Program Files\EMC\DPA\services\bin>dpa app adminpassword

```
DPA
Enter new administrator password.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new admin password :
[INFO] Your new password has been set.
[INFO] You must restart all DPA application nodes for this new
password to be used.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application agentpwd

Configure le mot de passe de gestion des licences de l'agent DPA du côté de l'application.

```
dpa application agentpassword [options]
dpa app agentpwd [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Notez les points suivants concernant le mot de passe de l'agent :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

C:\Program Files\EMC\DPA\services\bin>dpa app agentpwd

```
DPA
Enter new password for the agent connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the agent connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
```

```
agents use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application configure

Configure le service d'application et indique le datastore et le cluster avec lesquels il communique. Le service d'application doit être interrompu pour que cette commande puisse s'exécuter.

```
dpa application configure [options]
dpa app con [options]
```

Options de commandes

--master (-m) <IP_address> — Identifie le datastore avec lequel communiquer.

--bind (-b) <IP_address> — Définit l'adresse de liaison pour le service d'application.

--httprotocol (-hp) <http status> — Active ou désactive le protocole HTTP. Les valeurs possibles sont TRUE pour activer le protocole HTTP et FALSE pour désactiver le protocole HTTP.

Si vous exécutez la commande sans aucune option, le résultat affiche des informations sur la manière dont le serveur d'applications est actuellement configuré. Le Mode de fonctionnement dans la sortie identifie si l'application se trouve dans un cluster ou si elle est autonome.

Exemples

Résultat pour le serveur de cluster autonome :

```
C:\Program Files\EMC\DPA\services\bin>dpa app con
DPA
[INFO] Bind Address      : 0.0.0.0
[INFO] Datastore Service : 127.0.0.1
[INFO] Operation Mode    : STANDALONE
```

Résultat pour le datastore maître :

```
DPA
[INFO] Bind Address      : 0.0.0.0
[INFO] Datastore Service : 127.0.0.1
[INFO] Operation Mode    : CLUSTER
[INFO] Cluster Role      : MASTER
[INFO] Cluster Address   : 10.64.213.61
[INFO] Multicast Address : 239.1.2.61
```

dpa application demote

Rétrograde le service d'application à partir d'un environnement de clusters. Le service d'application fonctionnera en tant qu'instance d'objet autonome. Le service d'application doit être installé et arrêté pour que cette commande puisse s'exécuter.

```
dpa application demote [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
dpa application demote
dpa app demote
```

dpa application dspassword

Configure le mot de passe de datastore DPA.

```
dpa application dspassword [options]
dpa app dspwd [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Notez les points suivants concernant le mot de passe du datastore :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

C:\Program Files\EMC\DPA\services\bin>dpa app dspassword

```
DPA
Enter new password for the datastore connection.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection :
[INFO] Your new password has been applied to the configuration.
[INFO] For this new password to be used you must ensure that all
datastore nodes use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa application install

Installe le service d'application. Le service d'application fonctionnera comme un service géré par le système à l'aide des commandes de service du système d'exploitation. La gestion du cycle de vie du service peut également s'effectuer via cet outil de ligne de commande. Cette commande installe le service, mais ne le démarre pas automatiquement. Si le service d'application est déjà installé, cette commande échoue.

```
dpa application install [options]
```

Options de commandes

--user (-U) (DOMAIN\username) Compte utilisateur doté d'un accès en lecture et en écriture au chemin partagé spécifié. L'utilisateur spécifié doit disposer des droits *Ouvrir une session en tant que service* de Windows activés.

--password (-pass) <password> Mot de passe de l'utilisateur spécifié (Windows uniquement). Si l'utilisateur a modifié le mot de passe, il doit désinstaller, puis réinstaller le service d'application.

--help (-h) Affiche l'écran d'aide

--version Affiche les informations sur la version de l'outil

--quiet Affiche uniquement les avertissements et les erreurs

dpa application importcertificate

Vous permet d'importer votre propre certificat dans l'application DPA afin de chiffrer les données au lieu d'utiliser le certificat fourni par DPA.

```
dpa application importcertificate [options]
dpa app impcert [options]
```

Options de commandes

--certificatefile (-cf) <certificatefile> — Définit le chemin d'accès au certificat (format X.509) à importer.

--keystorefile (-kf) <keystorefile> — Définit le chemin d'accès au magasin de clés contenant le certificat à importer.

--alias (-al) <alias> — Définit l'alias de certificat à utiliser lors de l'accès au magasin de clés spécifié.

--password (-pw) <password> — Définit le mot de passe à utiliser lors de l'accès au magasin de clés spécifié.

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
dpa app impcert -kf "C:\work\new.keystore" -al newkey -pw password
```

dpa application ping

Teste la connexion entre l'objet d'application à partir duquel l'envoi est effectué et le service de datastore maître défini.

```
dpa application ping [options]
dpa app pin [options]
```

Options des commandes

--help (-h) Affiche l'écran d'aide

--quiet Affiche uniquement les avertissements et les erreurs

dpa application promote

Promeut le service d'application vers un environnement de clusters. Le service d'application fonctionnera en tant qu'objet au sein d'un cluster d'objets. La gestion du cycle de vie du service peut également s'effectuer via cet outil de ligne de commande. Le service d'application doit être installé et arrêté pour que cette commande puisse s'exécuter.

```
dpa application promote [options]
```

Options de commandes

--bind (-b) <IP_address> — Définit l'adresse de liaison pour le service d'application

--user (-u) <username> — Pour UNIX : (nom d'utilisateur) correspond au compte utilisateur qui dispose d'un accès en lecture et en écriture au dossier partagé. S'il n'est pas défini, l'utilisateur root est utilisé. Pour Windows : (DOMAIN\Username) correspond au compte utilisateur qui dispose d'un accès en lecture et en écriture au dossier partagé. S'il n'est défini, l'utilisateur système local est utilisé. Ce compte utilisateur doit disposer des droits Ouvrir une session en tant que service de Windows activés.

--path (-p) <path> — Chemin partagé par les clusters

--multicast (-m) <multicast address> — Définit l'adresse multicast utilisée par les nœuds de l'application de cluster pour communiquer les uns avec les autres. Tous les nœuds de l'application du cluster doivent utiliser la même adresse multicast

--help (-h) — Affiche l'écran d'aide

--role (-r) <role> — Définit le rôle de l'application dans le cluster. Les valeurs possibles sont MASTER et SLAVE <MASTER_IP>

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
dpa app promote --bind 192.168.1.0 --role MASTER --user user1 --
path \\shared
```

dpa application restart

Redémarre le service d'application. En premier lieu, cette commande arrête le service d'application, puis le redémarre. Le service d'application doit être en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa application restart [options]
```

Options de commandes

--platform (-p) — Inclut les informations sur la version de la plate-forme

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa application start

Démarre le service d'application. Le service d'application doit être installé et arrêté pour que cette commande puisse s'exécuter.

```
dpa application start [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Retards observés lors du démarrage et de l'arrêt des services DPA

L'exécution de la console Web, au démarrage des services DPA, peut prendre un certain temps. Si les services DPA viennent d'être installés, un délai pouvant aller jusqu'à 10 minutes s'écoule lors de l'exécution de la console Web. De même, si les services DPA sont redémarrés, un délai d'environ 3 minutes peut s'écouler lors de l'exécution de la console Web.

Remarque

les services DPA doivent être en cours d'exécution pour que la console Web DPA puisse être démarrée.

dpa application status

Affiche l'état du service d'application. Par exemple, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa application status [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
# dpa application status
DPA
The status of the Application Service is RUNNING
```

dpa application stop

Arrête le service d'application. Le service d'application doit être installé et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa application stop [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa application support

Configure le serveur d'applications DPA avec la passerelle ESRS (EMC Secure Remote Support).

Si vous prévoyez d'utiliser ESRS-VE pour le dépannage à distance (recommandé), assurez-vous que l'environnement ESRS-VE est installé et configuré avant l'installation de DPA. La page d'accueil d'EMC Secure Remote Services (https://support.emc.com/downloads/37716_EMC-Secure-Remote-Services-Virtual-Edition) sur le site de support en ligne d'EMC fournit plus d'informations sur les installations ESRS-VE..

```
dpa application support [options]
```

```
dpa app support [options]
```

Options de commandes

--register (-r) <ESRS_IP address> — Enregistre l'application DPA avec la passerelle ESRS

--update (-u) <DPA_new_IP address> — Met à jour la passerelle ESRS avec la nouvelle adresse IP du serveur DPA

--deregister (-d) — Annule l'enregistrement du serveur d'applications DPA auprès de la passerelle ESRS

--ping (-p) <ESRS_IP address> — Exécute une commande ping afin d'obtenir des informations sur le nœud/serveur d'applications DPA

--help (-h) — Affiche l'écran d'aide

Exemple

```
C:\Program Files\EMC\DPA\services\bin>dpa app support --register
10.11.110.111
```

dpa application tlslevel

Définit la version du protocole TLS pour les services d'application de DPA. Cette commande installe le service, mais ne le démarre pas automatiquement. Si le service d'application est déjà installé, cette commande échoue.

```
dpa application tlslevel [options]
dpa app tls [options]
```

Options de commandes

1.2 : définit la version du protocole TLS pour les services d'application de DPA pour le protocole TLS version 1.2 uniquement

1.0 : définit la version du protocole TLS pour les services d'application de DPA pour les protocoles TLS version 1.0, 1.1 et 1.2

--help (-h) : affiche l'écran d'aide

--version : affiche les informations sur la version de l'outil

--quiet : affiche uniquement les avertissements et les erreurs

Exemple

```
dpa app tls 1.2
```

dpa application tune

Configure les paramètres réglables du service d'application pour les ressources mémoire disponibles de l'hôte.

```
dpa application --tune <size> MB|GB
dpa app tune <size> MB|GB
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa application uninstall

Désinstalle le service d'application.

```
dpa application uninstall [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa application version

Affiche les informations sur la version des différentes bibliothèques fonctionnelles qui constituent le service d'application. Les bibliothèques fonctionnelles incluent Apollo, Controller, DPA (DPA), RemoteX et UI.

```
dpa application version [options]
```

Options de commandes

--platform (-p) — Inclut les informations sur la version de la plate-forme

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
# dpa application version
[INFO] Version for     Apollo EAR is 1.0.0.3304
[INFO] Version for Controller RAR is 18.1.xxx
[INFO] Version for DPA EAR is 18.1.xxx
[INFO] Version for    Remotex EAR is 1.0.0.3304
[INFO] Version for         UI WAR is 18.1.x.local
```

Commandes dpa datastore

Utilisez les commandes dpa datastore pour gérer le service de datastore DPA.

```
dpa datastore [options]
dpa datastore configure [options]
dpa datastore dspassword [options]
dpa datastore export [options]
dpa datastore import [options] <import_filename>
dpa datastore install [options]

dpa datastore logtz <time zone>
dpa datastore recreate [options]
dpa datastore replicate [options]
dpa datastore restart [options]
dpa datastore start [options]
dpa datastore status [options]
dpa datastore stop [options]
dpa datastore superpassword [options]
dpa datastore support [options] <ESRS_IP address>
dpa datastore tune <size>MB|GB [options]
dpa datastore uninstall [options]

dpa datastore supportbundle [options] <directory of output file>
dpa datastore version
```

Après avoir démarré, arrêté ou redémarré un service, il peut s'écouler quelques minutes avant que le changement ne s'opère.

dpa datastore configure

Configure le service de datastore, y compris l'ajout ou la suppression d'un service d'application à la liste des connexions autorisées pour le service de datastore.

```
dpa datastore configure [options]
dpa ds configure [options]
```

Options de commandes

--bind <IP_address> — Définit l'adresse de liaison pour le service de datastore. Le port par défaut est le 127.0.0.1.

NOTE

--bind ne peut pas être spécifié avec la commande --add ou --delete.

--add <IP_address> — Ajoute un nœud de service d'application en tant que client de datastore valide

--delete <IP_address> — Supprime un nœud de service d'application en tant que client de datastore valide

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
dpa datastore con --add 111.111.1.1
```

dpa datastore dspassword

Réinitialise le mot de passe du datastore DPA. Vous devez exécuter la commande alors que le service de datastore est en cours d'exécution.

```
dpa datastore dspassword [options]
dpa ds pwd [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Notez les points suivants concernant le mot de passe du datastore :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

```
C:\Program Files\EMC\DPA\services\bin>dpa ds dspassword
```

```
DPA
Enter new password for the datastore connection from the
application node.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the datastore connection from the
application node:
[INFO] Your new password has been applied to the datastore.
[INFO] For this new password to be used you must ensure that all
DPA application nodes use the same new password value.

Command completed succcessfully.

Completed in : 1min 25secs
```

dpa datastore export

Exporte le contenu du datastore vers le nom du fichier ou le pipeline spécifié. Le service de datastore doit être installé et en cours d'exécution pour que cette commande puisse s'exécuter. Tout nom de fichier existant présent est écrasé.

```
dpa datastore export [options]
```

```
dpa datastore export [options] <directory>
```

Options de commandes

--pipeline — Exportation dans un pipe

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
C:\Program Files\EMC\DPA\services\bin>dpa datastore export C:\
```

Le nom de fichier par défaut de la copie exportée est le suivant : datastore-<*version*><*date and time*>.

Par exemple, `datastore-6_2_0_90597-2014-10-01-1135`.

dpa datastore import

Importe le contenu du fichier d'exportation du datastore dans le datastore. Les fichiers d'importation doivent être disponibles sur le système de fichiers local. Vous êtes invité à arrêter tous les serveurs d'applications qui communiquent avec ce datastore avant

d'exécuter la commande. Le service de datastore doit être en cours d'exécution pour que la commande d'importation puisse s'exécuter.

```
dpa datastore import [options] <filename>
```

Où <filename> est un fichier de datastore précédemment exporté. La commande d'importation remplace le contenu existant du datastore par celui du fichier d'exportation du datastore.
Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

<import_filename> — Nom du fichier exporté à importer

Exemples

```
# dpa datastore import datastore-2013-02-20-1205
DPA
Datatstore imported from file : datastore-2013-02-20-1205
Imported to the datastore successfully
```

dpa datastore install

Installe le service de datastore. Le service de datastore fonctionne comme un service géré par le système à l'aide des commandes de service du système d'exploitation. La gestion du cycle de vie du service peut également s'effectuer via cet outil de ligne de commande. Cette commande installe le service, mais ne le démarre pas automatiquement. Si le service de datastore est déjà installé, cette commande échoue.

```
dpa datastore install [options]
```

Options de commandes

--help — Affiche l'écran d'aide --version — Affiche les informations sur la version de l'outil --quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore logtz

Configure le fuseau horaire des journaux de la base de données DPA

```
dpa datstore logtz <time zone>
```

```
dpa ds logstz <time zone>
```

Exemple

dpa datstore logtz 'Europe/Moscow' configure le fuseau horaire des journaux du Datastore de DPA comme étant Europe/Moscow

DPA datstore logtzDPA Datastore définit le fuseau horaire comme étant GMT

dpa datastore recreate

Recrée le datastore, en réinitialisant son contenu aux paramètres d'usine.

DESCRIPTION

dpa datastore recreate [options]

```
dpa ds rec [options]
```

Options de commandes

--force (-f) — Invite de remplacement indiquant que les données actuelles du datastore vont être remplacées

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

SYNTAXE

dpa datastore replicate

Configure la réplication du service de datastore sur une autre instance.

DESCRIPTION

```
dpa ds rep [options]
```

Options de commandes

--addSlave (-a) <hostname/IP of SLAVE> - Ajoute un datastore esclave à un datastore maître

--deleteSlave (-d) <hostname/IP of SLAVE> - Supprime un datastore esclave d'un datastore maître

--role (-r) MASTER - Redéfinit le rôle du datastore esclave par rapport au datastore maître

--role (-r) SLAVE <IP of MASTER> - Redéfinit le rôle du datastore maître par rapport au datastore esclave

--failover - Initie un basculement sur incident entre le datastore esclave et le datastore maître

--import (-i) <import> - Initialise un datastore SLAVE avec un réplica situé dans le répertoire spécifié

--export (-e) <export> - Produit un clone du datastore MASTER sur le répertoire spécifié

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

SYNTAXE

dpa datastore restart

Redémarre le service de datastore. En premier lieu, cette commande arrête le service de datastore, puis redémarre le service. Le service de datastore doit être en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa datastore restart [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore start

Démarre le service de datastore. Le service de datastore doit être installé et arrêté pour que cette commande puisse s'exécuter.

```
dpa datastore start [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore status

Affiche l'état du service de datastore. Par exemple, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa datastore status [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
# dpa datastore status
DPA
```

```
The status of the Datastore Service is RUNNING
```

dpa datastore stop

Arrête le service de datastore. Le service de datastore doit être installé et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa datastore stop [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore superpassword

Réinitialise le mot de passe de superutilisateur du datastore DPA. Le superutilisateur est l'utilisateur propriétaire de la base de données DPA. Vous devez exécuter la commande alors que le service de datastore est en cours d'exécution.

Si vous utilisez la réplication de datastore, vous devez exécuter cette commande sur tous les nœuds du datastore. Exécutez la commande sur le nœud maître d'abord, puis sur les nœuds esclaves de réplication.

```
dpa datastore superpassword [options]
dpa ds superpwd  [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--version — Affiche les informations sur la version de l'outil

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Notez les points suivants concernant le mot de passe du datastore :

- Les mots de passe vides ne sont pas pris en charge.
- La longueur minimale est de 9 caractères.
- Les critères suivants sont obligatoires :
  - Un minimum de 1 lettre majuscule et 1 lettre minuscule
  - Un minimum de 1 caractère numérique
  - Un minimum de 1 caractère spécial

Exemple

C:\Program Files\EMC\DPA\services\bin>dpa ds superpassword

```
DPA
Enter new password for the superuser owning the database.
The password must have:
 - at least 9 characters
 - at least 1 uppercase letter
 - at least 1 lowercase letter
 - at least 1 special character
 - at least 1 digit

Retype new password for the superuser owning the database:
[INFO] Your new password has been applied to the superuser owning
the database.

Command completed succcessfully.
```

dpa datastore supportbundle

Collecte des informations de support technique et stocke le fichier zip de bundle de support technique du DPA Datastore dans le répertoire spécifié.

```
dpa datastore supportbundle [options] <directory of output file>
dpa ds supbd [options] <directory of output file>
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore tune

Configure les paramètres réglables du service de datastore pour les ressources mémoire disponibles de l'hôte et les connexions à la base de données.

```
dpa datastore tune <size>MB|GB [options]
dpa ds tune <size>MB|GB [options]
```

Options de commandes

--connections (-c) <connections> — Nombre maximum de connexions de datastore simultanées autorisées

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa datastore uninstall

Désinstalle le service de datastore.

```
dpa datastore uninstall [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

DPA datastore version

Interroge le numéro de version et de patch de Datastore

```
dpa datstore version [options]
```

```
dpa ds version [options]
```

Options de commandes

--help (-h) — Affiche l'écran d'aide

Commandes de service dpa

Utilisez les commandes de service dpa pour gérer les services d'application DPA, de datastore DPA et d'agent DPA.

```
dpa service install [options]
dpa service restart [options]
dpa service start [options]
dpa service status [options]
dpa service stop [options]
dpa service uninstall [options]
```

dpa service install

Installe le service de datastore, puis le service d'application. Les services fonctionnent comme des services gérés par le système à l'aide des commandes de service du système d'exploitation. La gestion du cycle de vie des services peut également s'effectuer à l'aide de cet outil de ligne de commande. Cette commande installe les services, mais ne les démarre pas automatiquement. Si les services sont déjà installés, cette commande échoue.

```
dpa service install [options]
dpa svc install [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa service restart

Redémarre les services d'application et de datastore. Cette commande arrête le service d'application, arrête le service de datastore, puis démarre le service de datastore et le service d'application. Les services doivent être en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa service restart [options]
dpa svc restart [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa service start

Démarre le service de datastore, puis le service d'application. Les services doivent être installés et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa service start [options]
dpa svc start [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa service status

Affiche l'état des services de datastore et d'application. Par exemple, RUNNING (STARTING...), RUNNING, STOPPED

```
dpa service status [options]
dpa svc status [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Exemples

```
# dpa service status
DPA
The status of the Datastore Service is RUNNING
The status of the Application Service is RUNNING (STARTING ...)
```

dpa service stop

Arrête le service d'application, puis le service de datastore. Les services doivent être installés et en cours d'exécution pour que cette commande puisse s'exécuter.

```
dpa service stop [options]
dpa svc sop [options]
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

dpa service uninstall

Désinstalle le service d'application, puis le service de datastore.

```
dpa service uninstall [options] <certificate> <key>
dpa svc uninstall [options] <certificate> <key>
```

Options de commandes

--help — Affiche l'écran d'aide

--quiet — Supprime toute sortie à l'exception des messages d'erreur et des avertissements

Chargement des données des procédures de sauvegarde historiques

La méthode privilégiée pour collecter les données de sauvegarde historiques est l'utilisation de la console Web DPA.

Avant de commencer

Pour plus d'informations, reportez-vous à la section Collecte des données de sauvegarde historiques à l'aide de la console Web DPA à la page 101.
Quand un objet d'application de sauvegarde a été créé et que les demandes ont été attribuées, l'agent commence immédiatement la collecte des données sur les procédures de sauvegarde pour les stocker dans le datastore. Cependant, l'agent peut également recueillir des données sur les procédures de sauvegarde qui ont été exécutées avant la création de l'objet dans DPA.

Remarque

Pour consigner les données sur le serveur DPA, l'agent installé doit avoir précédemment démarré et s'être enregistré avec succès auprès du serveur DPA. Toutefois, il ne doit pas être en cours d'exécution afin de charger les données historiques.

Chaque module de sauvegarde possède un fichier exécutable équivalent dans le répertoire bin de l'agent installé, `<DPA_HOME>/emc/dpa/agent/bin` , où <DPA_Home> correspond à l'emplacement de l'installation DPA.

DESCRIPTION

L'exemple suivant recueille les données de procédures de sauvegarde exécutées sur un serveur NetWorker :

SYNTAXE

Exemple

```
<install_dir>/agent/bin/dpaagent_modnetworker -c -f jobmonitor -t
NetWorkerServer_IP -B "01/01/2012 00:00:00" -E "01/01/2012 00:00:00"
```

Le fait d'exécuter l'exécutable avec le paramètre -? affiche les options de ligne de commande valides. Il est peut-être nécessaire de spécifier explicitement sur la ligne de commande les options de module applicables à la demande (par exemple, timeformat) pour garantir un comportement cohérent avec une collecte de données « normale ». Plus précisément, dans le cas de la demande jobmonitor de DataProtector, l'option d'occupation doit être spécifiée explicitement pour que les données de l'historique fassent partie des calculs d'occupation. Pour plus d'informations sur cette option, reportez-vous à la section *Guide de référence pour la collecte des données de Data Protection Advisor*. La section « Job Monitor » quant à elle, fournit des informations complémentaires sur l'option d'occupation.

Pour charger les données de sauvegarde historiques, exécutez le fichier binaire de l'agent à partir de la ligne de commande en utilisant les paramètres suivants : Vous devez spécifiquement utiliser :

- -f <*nom de fonction*> : nom de la fonction de collecte des données à exécuter. Toujours jobmonitor. Obligatoire.
- -t <*hôte cible*> : adresse d'hôte du serveur d'application de sauvegarde. La valeur par défaut est localhost.
- -B <*heure de début*> : heure à partir de laquelle commencer à collecter les procédures de sauvegarde. Le format est jj/mm/aaaa hh:mm:ss.

- -E <*heure de fin*> : heure à laquelle la collecte de procédures de sauvegarde prend fin. Le format est jj/mm/aaaa hh:mm:ss.
  Les heures de début et de fin peuvent également être au format epoch d'Unix.

  Si l'<*heure de début*> est spécifiée et que l'<*heure de fin*> ne l'est pas, l'<*heure de fin*> est définie sur l'heure actuelle. Ceci inclut toutes les procédures de sauvegarde qui ont pris fin après l'<*heure de début*>.

  Si l'<*heure de fin*> est spécifiée et que l'<heure de début> ne l'est pas, l'<*heure de début*> est définie sur 0. Ceci inclut toutes les procédures de sauvegarde qui prennent fin après l'<*heure de fin*>.
- -i : nom de l'instance TSM (TSM uniquement).
- -l <log file name> : nom et chemin du fichier log à générer lors de l'exécution de la commande afin de charger les données historiques.
  L'emplacement par défaut du fichier log est celui à partir duquel la commande est exécutée.
- -U : nom d'utilisateur utilisé pour se connecter à l'application de sauvegarde (TSM et Avamar uniquement).
- -P : mot de passe utilisé pour se connecter à l'application de sauvegarde (TSM et Avamar uniquement).
- -c- Commit : indique au module qu'il doit envoyer les données au serveur DPA. Obligatoire.

L'exemple suivant recueille les données de procédures de sauvegarde exécutées sur un serveur Avamar :

Exemples

```
dpaagent_modavamar.exe -f jobmonitor -t De-dup-muc.corp.emc.com -U
viewuser -P viewuser1 -c -B "01/01/2012 00:00:00" -l /tmp/
mod_avamar.log
```

Rapports Job Summary

Les rapports Job Summary donnent un aperçu des totaux des procédures de sauvegarde et de maintenance (comme toutes les procédures, les procédures réussies, les procédures ayant échoué) qui ont eu lieu sur les serveurs de sauvegarde. Ces rapports utilisent la dernière version des données du datastore pour générer des résultats de récapitulatif précis.

DESCRIPTION

Pendant le chargement des données de procédures de sauvegarde historiques à l'aide des options de ligne de commande de l'agent, des rapports récapitulatifs peuvent afficher des totaux inexacts. Il est préférable d'attendre que toutes les données des tâches historiques aient été chargées avant d'exécuter des rapports récapitulatifs pour les périodes historiques chargées.

SYNTAXE

CHAPITRE 4

Découverte de l’environnement dans DPA

Le présent chapitre contient les sections suivantes :

Configuration de l'environnement pour la découverte

Présentation de la découverte

La figure ci-dessous illustre la relation entre l'objet d'application DPA et les agents DPA déployés pour surveiller votre infrastructure de protection des données.

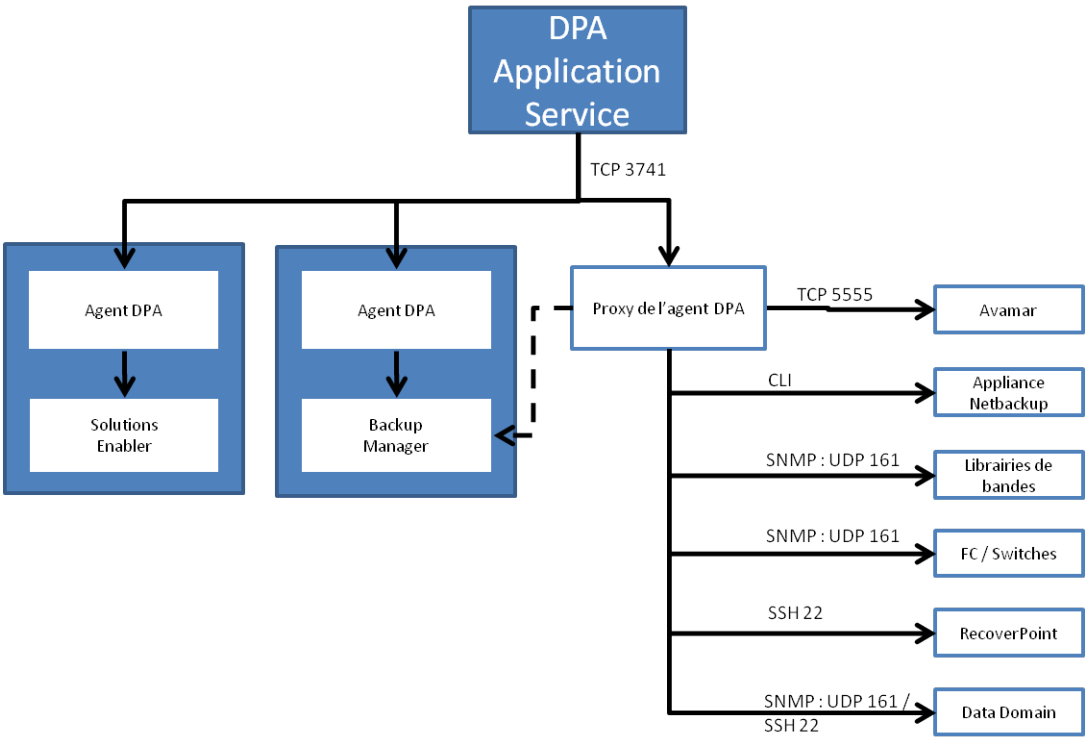
Certains types de périphériques doivent être surveillés avec un agent DPA déployé en tant que proxy. Un proxy est généralement utilisé lorsque l'objet surveillé est un élément de matériel et que l'accès pour installer l'agent n'est pas possible. La plupart des gestionnaires de sauvegarde peuvent être surveillés par un agent installé sur le même hôte que le gestionnaire de sauvegarde, ou à distance avec un agent proxy si le gestionnaire de sauvegarde a des ressources limitées.

DPA est insensible à la casse en ce qui concerne les noms de pool de sauvegarde. Par exemple, si vous définissez les pool

- test_name
- Test_name
- Test_Name

DPA crée un objet dans l'arborescence de configuration. Lorsque vous exécutez un rapport sur le périmètre et sélectionnez cet objet, vous ne pouvez voir qu'un seul ensemble de chiffres.

Figure 3 Relations entre les nœuds d'application DPA et les applications de surveillance d'agents DPA



Définition des objets à surveiller

Pour définir les objets à surveiller dans DPA, suivez les étapes du tableau suivant.

Tableau 33 Résumé de la configuration de la surveillance des données

Étape	Description :
Vérification des licences	Assurez-vous que les licences permettant de surveiller votre périphérique, votre hôte ou votre environnement ont été achetées et installées.
Installation de l'agent	Si vous êtes en train de surveiller l'objet depuis un hôte autre que le serveur DPA hôte, vous devez installer l'agent DPA. Reportez-vous à la section Installation de l'agent DPA à la page 57.
Installation de fichiers binaires tiers ou définition de l'objet à surveiller	Cette étape est nécessaire pour la collecte de données distante ou sans agent (proxy). Vous devrez peut-être installer les fichiers binaires sur l'hôte DPA ou sur l'hôte de l'agent distant pour vous connecter à l'objet surveillé. Il se peut également que vous ayez besoin de définir un compte ou une connexion sur l'objet surveillé. Les sections suivantes décrivent la configuration des conditions préalables pour tous les objets : • Configuration pour l'analyse de réplication à la page 204 • Configuration des baies de stockage pour l'analyse de la réplication à la page 206 • Surveillance des applications de sauvegarde à la page 173 • Surveillance de bases de données à la page 187 • Surveillance de RecoverPoint à la page 206 • Surveillance des systèmes d'exploitation à la page 201 • Surveillance de bibliothèques de bandes à la page 211 • Surveillance des switches et périphériques d'E/S à la page 213 • Surveillance des serveurs de fichiers à la page 206 • Surveillance du stockage de protection à la page 209

Tableau 33 Résumé de la configuration de la surveillance des données (suite)

Étape	Description :
	• Surveillance de StorageTek ACSLS Manager à la page 211 • Surveillance des serveurs de gestion des disques à la page 208 • Surveillance de l'environnement VMware à la page 214
Création ou modification des informations d'identification DPA	Les informations d'identification stockent les informations utilisées pour se connecter à l'objet surveillé. Il est peut-être nécessaire de modifier les informations d'identification par défaut ou d'en créer de nouvelles avec les détails du compte provenant de l'étape précédente.
Exécution du Discovery Wizard	Utilisez le Discovery Wizard pour définir les objets à surveiller. Sélectionnez **Inventory** > **System** > **Run Discovery Wizard**.
Modifiez les paramètres de collecte de données par défaut	Vérifiez les durées de rétention par défaut pour toutes les demandes et modifiez-les si nécessaire. Les demandes de collecte de données sont attribuées à l'objet créé par le Discovery Wizard. Si vous souhaitez modifier la collecte de données par défaut, sélectionnez **Admin** > **Systems** > **Manage Data Collection Defaults**.
Collecte des données de test	Après avoir laissé la demande s'exécuter pendant au moins 10 minutes, exécutez un rapport à partir de l'objet qui devrait inclure des données (par exemple, un récapitulatif de la procédure de sauvegarde ou un rapport de configuration).

Avant de démarrer le Discovery Wizard

Procédure

1. Vérifiez les licences installées. Dans la console Web DPA, accédez à **Admin** > **System** > **Manage Licenses**.

   Les options pouvant être configurées dans le Discovery Wizard dépendent des types des licences que vous avez installées avec DPA. Si la licence appropriée n'est pas installée, l'option permettant de créer ce périphérique ou cet hôte est désactivée dans l'assistant.

2. Si vous effectuez la découverte sur un hôte Linux, assurez-vous que la bibliothèque *libstdc++ .so.6* est installée sur l'hôte.
3. Assurez-vous de bien prendre en compte les informations sur la connexion, présentées dans le tableau suivant.

Tableau 34 Détails de connexion pour la configuration de la collecte des données via le Discovery Wizard

Élément	Valeur à noter pour la saisir dans l'assistant de découverte
Informations de configuration réseau pour le serveur ou l'agent DPA si l'agent est distant du serveur DPA	
Hostname	Value:
Adresse IP	Value:
Masque réseau	Value:
Adresse IP du serveur DNS principal	Value:
Adresse IP du serveur DNS secondaire	Value:
Adresse de passerelle	Value:
Fuseau horaire	Value:
Informations d'identification requises pour la découverte de disques virtuels via SSH	
Adresse IP du serveur VMware ESX	Value:
Informations d'identification root pour le serveur VMware ESX	Value:
Informations d'identification pour la découverte de serveurs et de baies	
Nom ou adresse IP du serveur	
Données d'identification SSH	Value:
Données d'identification RPC	Value:
Données d'identification WMI	Value:
Données d'identification Solutions Enabler Connexion obligatoire en tant root/avec informations d'identification d'administrateur	Value:
Données d'identification RPA	Value:
Données d'identification requises pour la surveillance de bases de données Oracle	
Nom d'utilisateur et mot de passe Oracle requis	Value:
Nom et port du service Oracle, plus spécifiquement l'identifiant SID Oracle et le port TNS	Value:
Oracle Monitor RMAN Un utilisateur Oracle ayant accès au catalogue pour le schéma RMAN, ainsi qu'un nom d'utilisateur et un mot de passe, sont requis.	Value:
Nom d'hôte Oracle	Value:
Schéma Oracle Monitor	Value:

Tableau 34 Détails de connexion pour la configuration de la collecte des données via le Discovery Wizard (suite)

Élément	Valeur à noter pour la saisir dans l'assistant de découverte
Si plusieurs schémas RMAN existent pour un identifiant SID Oracle, le nom d'utilisateur et le mot de passe de chaque propriétaire de schéma RMAN sont nécessaires.	
Données d'identification requises pour les bases de données SQL Server	
Création d'un compte utilisateur de base de données SQL	Value:
Instance de SQL Server	Value:
Nom de la base de données SQL	Value:
Données d'identification PostgreSQL	
Compte utilisateur PostgreSQL (doit être un superutilisateur)	Value:
Données d'identification pour les serveurs de sauvegarde, les bibliothèques de bandes et les périphériques d'E/S	
Compte utilisateur CommVault	Value:
Compte utilisateur Avamar À partir de la version 7.1, Avamar n'est plus fourni avec un mot de passe par défaut pour le compte viewuser, et le mot de passe du compte viewuser est défini par l'utilisateur lors de l'installation de Avamar. Si vous découvrez Avamar 7.1 ou une version supérieure, et que cette version n'a pas été mise à niveau à partir d'une version précédente, vous devez créer un nouveau jeu d'informations d'identification dans DPA. Accédez à **Admin** > **User** > **Set Credentials**.	Value:
Compte utilisateur HP Data Protector	
L'hôte TSM IBM, le nom d'instance TSM, le port TSM, ainsi que le nom d'utilisateur et le mot de passe TSM, sont requis pour chaque instance TSM.	Value:
Compte utilisateur Symantec Backup Exec	Value:
Compte utilisateur Symantec PureDisk	Value:
Chaîne de communauté SNMP pour Data Domain Nom d'utilisateur et mot de passe SSH pour Data Domain, de préférence un nom d'utilisateur et un mot de passe différents des informations d'identification par défaut de l'administrateur système Data Domain. Ces deux éléments sont nécessaires car les données sont collectées à l'aide des deux mécanismes.	Value:
Chaîne de communauté SNMP pour EDL	Value:
Chaîne SNMP pour switch Fibre Channel	Value:

Tableau 34 Détails de connexion pour la configuration de la collecte des données via le Discovery Wizard (suite)

Élément	Valeur à noter pour la saisir dans l'assistant de découverte
Chaîne de communauté SNMP pour les bibliothèques de bandes	Value:
Chaîne de communauté SNMP pour switch IP	Value:

Surveillance des applications de sauvegarde

Cette section explique comment surveiller des applications de sauvegarde.

Surveillance de CA BrightStor ARCserve

Les serveurs CA BrightStor ARCserve sont surveillés à partir d'un agent s'exécutant sur le serveur CA BrightStor ARCserve ou d'un agent exécuté sur tout autre ordinateur Windows dans l'environnement.

Avant de démarrer le Discovery Wizard pour la surveillance de CA BrightStor ARCserve

Avant de commencer

- Vous devez connaître le nom d'hôte pouvant être résolu et l'adresse IP du serveur ARCserve.
- Lors de l'exécution d'ARCserve 11.x, le nom d'hôte doit être le nom d'hôte court. Vous ne pouvez pas utiliser d'alias.

Procédure

1. Installez le gestionnaire ARCserve sur l'ordinateur sur lequel l'agent est en cours d'exécution.

   Les informations d'identification de l'agent doivent correspondre au compte ARCserve existant.

2. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour ARCserve, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Surveillance de CommVault Simpana

Surveillez les serveurs CommVault Simpana à partir d'un agent s'exécutant sur la base de données CommVault Simpana ou à partir d'un agent s'exécutant sur un autre ordinateur Windows de l'environnement.

Avant de démarrer le Discovery Wizard pour la surveillance de CommVault Simpana

Si le serveur SQL CommVault utilise l'authentification Windows, le service d'agent DPA doit s'exécuter avec un compte nommé. Le compte nommé choisi pour le service d'agent DPA doit disposer d'une autorisation d'accès en lecture à la base de données CommVault SQLServer.

De même, si l'authentification SQL est utilisée, vous devez définir les informations d'identification DPA des demandes CommVault, par exemple, nom d'utilisateur : cvadmin ; mot de passe : mot de passe de l'utilisateur cvadmin.

Vous devez connaître :

- Le nom d'hôte pouvant être résolu ou l'adresse IP du serveur CommVault.
- Le nom d'hôte de la base de données et le nom de l'instance si la base de données CommVault est distante par rapport au serveur.

Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour CommVault Simpana, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Surveillance d'Avamar

Surveillez les serveurs Avamar à l'aide d'un agent DPA installé sur un ordinateur distant dans l'environnement, y compris le serveur DPA. N'installez pas d'agent DPA sur l'objet de stockage ou le serveur Avamar.

Pour activer la surveillance de la grille Avamar de base par le déploiement DPA pris en charge, sur la version 7.2 ou ultérieure, veillez à sélectionner **Remote Data Collection Unit**.

Pour permettre l'affichage des données dans le rapport Clone Operations lorsque la grille source est sélectionnée comme portée du rapport, vous devez surveiller la grille source Avamar avec la demande Job Monitor à partir d'une configuration de réplication Avamar.

Avant de démarrer le Discovery Wizard pour la surveillance d'Avamar

Aucun logiciel supplémentaire n'est nécessaire pour surveiller un serveur Avamar à distance.

Avant de commencer

Avant de démarrer le Discovery Wizard, vous devez connaître le nom d'hôte pouvant être résolu ou l'adresse IP du serveur Avamar.

Procédure

1. Pour collecter des données à partir d'Avamar, DPA se connecte directement à la base de données Avamar. Il se connecte à la base de données mcdb sur le port par défaut pour Avamar, à savoir 5555. Si ces paramètres ont été modifiés, changez les options des demandes Configuration Avamar, Job Monitor Avamar et Status Avamar pour indiquer le nom de la base de données et le port utilisé. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
2. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour Avamar, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
3. Si vous découvrez Avamar 7.1 ou une version supérieure, et que cette version n'a pas été mise à niveau à partir d'une version précédente, vous devez créer un nouveau jeu d'informations d'identification dans DPA. Accédez à **Admin** > **User** > **Set Credentials**.

À partir de la version 7.1, Avamar n'est plus fourni avec un mot de passe par défaut pour le compte viewuser, et le mot de passe du compte viewuser est défini par l'utilisateur lors de l'installation de Avamar.

4. Créez de nouvelles informations d'identification dans le champ Default Avamar Credentials de la console Web DPA à partir de **Admin** > **System** > **Manage Credentials** car le nom d'utilisateur et le mot de passe sont réinitialisés lors de la mise à niveau.

   Quand DPA se connecte à la base de données, il utilise le compte viewuser pour ouvrir une session dans la base de données.

À propos de la collecte de données de tâches après la découverte d'Avamar

Découvrez-en plus sur la collecte de données de tâches d'Avamar après avoir découvert l'Avamar interne à DPA.

- Lorsqu'un nouveau serveur Avamar est découvert, DPA rassemble les données des tâches jusqu'à 14 jours antérieures.
- À chaque fois qu'une demande de surveillance de tâches est exécutée, DPA collecte une quantité de données de « période de lot » au maximum. Cette valeur est configurable et correspond par défaut à la quantité de données générées en une journée.
- Après avoir exécuté plusieurs demandes de surveillance de tâches, la période des tâches collectées arrive à l'heure actuelle et les nouvelles sauvegardes sont collectées.
- Le délai par défaut entre la fin de la dernière exécution de surveillance de tâche et l'exécution de la demande suivante est de 5 minutes. Cela peut être configuré, comme pour toutes les demandes.

Les Options de demande de collecte de données par module fournissent des informations supplémentaires.

Surveillance de NetWorker

Surveillez NetWorker à partir d'un agent s'exécutant sur le serveur de sauvegarde ou à distance, à l'aide d'un agent s'exécutant sur le serveur DPA ou sur un autre ordinateur distant de l'environnement.

Avant de démarrer le Discovery Wizard pour la surveillance de NetWorker

En cas de surveillance de NetWorker à distance, le package client NetWorker doit être installé sur l'hôte de l'agent. Le module NetWorker utilise des commandes telles que `jobquery` et `nsradmin` pour communiquer avec le serveur NetWorker et a besoin d'accéder aux fichiers binaires du package client NetWorker.

Avant de commencer

- Avant de démarrer le Discovery Wizard, vous devez connaître le nom d'hôte pouvant être résolu ou l'adresse IP du serveur NetWorker.
- Si vous surveillez NetWorker 9.0.0.4 et versions ultérieures, assurez-vous que vous disposez des credentials du serveur NetWorker. Vous devrez saisir les credentials du serveur NetWorker pour permettre à l'agent DPA d'émettre un `nsrauth` et d'exécuter nsradmin.

Procédure

1. Si vous surveillez NetWorker 9.0.0.4 et installez plus tard à distance Networker Client et NetWorker Extended Client. Le Client et le Client Extended de NetWorker 9 doivent être installés sur l'hôte de l'agent DPA. Si vous disposez

d'une version antérieure de NetWorker Client, vous devez la mettre à niveau. Si vous surveillez des versions plus anciennes de NetWorker, utilisez le Client et Extended Client NetWorker 9 pour surveiller ces autres versions si l'agent DPA est également utilisé pour surveiller un serveur NetWorker 9.

2. Si vous surveillez NetWorker 7.6 ou une version supérieure à distance, l'utilisateur DPA et l'hôte proxy doivent être ajoutés à la liste des utilisateurs du groupe d'utilisateurs des Administrateurs de NetWorker. Par exemple, si vous surveillez NetWorker à distance à partir de l'hôte DPA Agent Host et que l'agent est exécuté en tant qu'utilisateur Windows DPA Agent, vous devez ajouter la ligne suivante dans la liste de propriétés d'utilisateurs pour les Administrateurs :

   ```
   user=DPAAgent,host=DPAAgentHost
   ```

3. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour NetWorker, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console Web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

À propos de la collecte de données de tâches après la découverte de NetWorker

Découvrez-en plus sur la collecte de données de tâches NetWorker après avoir découvert le NetWorker interne à DPA.

- Lorsqu'un nouveau serveur NetWorker est découvert, DPA collecte les données des tâches jusqu'à 14 jours antérieures.
- Après avoir exécuté plusieurs demandes de surveillance des tâches, la période des tâches collectées arrive à l'heure actuelle et les nouvelles sauvegardes sont collectées.

Suite à cette opération, il faudra 7 heures pour que les demandes de surveillance des tâches commencent la collecte de données sur les tâches actuelles. En effet, chaque demande est planifiée par défaut pour s'exécuter toutes les 30 minutes et à chaque demande un maximum d'un jour de données est collecté. Options de demande de collecte de données par module fourni plus informations.

Surveillance de HP Data Protector

Un agent peut surveiller des serveurs HP Data Protector exécutés sur le gestionnaire de cellule Data Protector HP ou à distance à partir d'un autre ordinateur.

Avant de démarrer le Discovery Wizard pour la surveillance de HP Data Protector

En cas de surveillance à distance d'un gestionnaire de cellule, suivez les instructions de la section Surveillance du HP Data Protector à distance à la page 179.

Remarque

Vous ne pouvez pas attribuer la demande d'état lorsque vous surveillez le serveur HP Data Protector à distance car il dépend de la commande `omnisv`. La commande est disponible uniquement sur le serveur Data Protector.

Si vous surveillez un environnement Data Protector qui utilise l'option Manager of Managers, vous devez configurer DPA comme pour surveiller un serveur Data Protector distant.

Pour surveiller à distance HP Data Protector, vous devez installer le logiciel client HP Data Protector sur l'hôte de l'agent et configurer le client sur le gestionnaire de cellule Data Protector pour qu'il soit autorisé à exécuter des rapports. La section Surveillance du HP Data Protector à distance à la page 179 fournit des informations sur les tests de connexion depuis l'hôte de l'agent.

Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour HP Data Protector, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Collecte de données d'occupation

Par défaut, la collecte des données d'occupation n'est pas activée pour HP Data Protection. Pour l'activer, vous devez activer l'option d'occupation pour la demande Jobmonitor de Data Protector et attribuer la demande Client Occupancy de Data Protector au client Data Protector dans la boîte de dialogue **Edit Request**.

Vous pouvez utiliser la variable d'environnement *DP_OCCUPANCY_DB_PATH* pour que l'agent DPA contrôle où sont stockées les données d'occupation lors de l'exécution de la demande jobmonitor. Si vous n'utilisez pas la variable d'environnement *DP_OCCUPANCY_DB_PATH*, le système stocke les données d'occupation dans le répertoire temporaire.

Remarque

Collecter des informations d'occupation pour HP DataProtector peut avoir un impact important sur les performances du serveur Data Protector.

Modification de l'emplacement de la base de données d'occupation sous Linux
Procédure

1. Arrêtez l'agent DPA.
2. Utilisez la commande `cd` pour accéder au répertoire `/opt/emc/dpa/agent/etc`.
3. Modifiez le fichier `dpa.custom`. Ajoutez l'entrée suivante à la fin du fichier :

   ```
   COLLECTOR_DP_OCCUPANCY_DB_PATH=/your/absolute/path/
   export COLLECTOR_DP_OCCUPANCY_DB_PATH
   ```

   Assurez-vous de bien inclure la barre oblique inversée (\) dans le chemin d'accès.

4. Redémarrez l'agent DPA

Modification de l'emplacement de la base de données d'occupation sous Windows
Procédure

1. Arrêtez l'agent DPA.
2. Exécutez regedit.exe en tant qu'utilisateur administrateur.
3. Développez la clé de registre HKEY_LOCAL_MACHINE.
4. Développez la clé de registre SOFTWARE.
5. Si elle n'existe pas déjà, créez une clé de registre EMC.
6. Si elle n'existe pas déjà, créez une clé de registre DPA.

7. Si elle n'existe pas déjà, créez une clé de registre d'agent.
8. Créez une nouvelle valeur de registre de chaîne nommée DP_OCCUPANCY_DB_PATH et définissez la valeur sur le nom du chemin d'accès au répertoire souhaité.

   Par exemple : `C:\DPA\OccupancyData\` Assurez-vous de bien inclure la barre oblique (\) dans le chemin d'accès.
9. Redémarrez l'agent DPA.

Correctif omnirpt
HP a commercialisé un correctif pour Data Protector 6.1 qui doit être installé sur une installation de Data Protector 6.1 pour que DPA puisse le prendre en charge.

Le tableau suivant répertorie l'ID du correctif requis pour chaque plate-forme.

Tableau 35 ID de correctifs pour HP Data Protector 6.1

Plate-forme	ID de correctif
Windows	DPWIN_00417
HPUX PA-Risc	PHSS_39512
HPUX IA64	PHSS_39513
Linux	DPLNX_00077
Solaris	DPSOL_00371

Le correctif est disponible sur le site d'HP, à l'adresse www.hp.com. Saisissez l'ID de correctif dans le champ Search de la page d'accueil du site de HP. Vous êtes dirigé vers la page de téléchargement du correctif.

Configuration des données de tâche de restauration et des durées de conservation d'occupation mises à jour

Effectuez la procédure suivante pour obtenir les données de tâche de restauration et les durées de conservation d'occupation mises à jour de la fonction de surveillance des tâches.

Procédure

1. Dans l'interface utilisateur de HP Data Protector Manager, accédez à **Internal Database** > **Global Options**.
2. Ajoutez les options suivantes :

Option	Description
EnableRestoreReportStats	Active les données de restauration de session étendue
LogChangedProtection	Consigne la conservation modifiée d'occupation

   Assurez-vous que vous définissez la valeur des deux options sur **1** et sélectionnez**In Use** pour les deux.
3. Redémarrez les services HP Data Protector avec la commande `omnisv` pour que les modifications soient prises en compte.

Surveillance du HP Data Protector à distance

Vous devez installer le logiciel client sur l'ordinateur qui surveille le gestionnaire de cellule :

Procédure

1. Ouvrez l'interface d'administration du gestionnaire de Data Protector pour ajouter un client.
2. Lors de la sélection des composants logiciels à installer sur le client, veillez à ce que l'option **Interface utilisateur** soit sélectionnée.

   Le module Data Protector de DPA doit pouvoir accéder à des commandes telles que `omnirpt` et `omnicellinfo` pour collecter des données à partir du gestionnaire de cellule. Ces composants n'étant installés que si le composant d'interface utilisateur est installé, il est essentiel d'activer cette option.

3. Configurez le client pour l'autoriser à exécuter des rapports sur le gestionnaire de cellule. Commencez par déterminer l'utilisateur pour lequel le processus agent sera exécuté :
   - Dans les systèmes UNIX, l'agent est toujours exécuté en tant qu'utilisateur root.
   - Dans les systèmes Windows, l'agent est exécuté en tant qu'utilisateur du service agent DPA. Pour vérifier l'utilisateur de ce service dans un système Windows, ouvrez le Gestionnaire de contrôle des services Windows et affichez les détails du service Agent DPA.
4. Créez un utilisateur sur le gestionnaire de cellule qui correspond au nom d'utilisateur de l'agent. Saisissez le nom de l'hôte dans le champ de **définition de l'utilisateur**.
5. Ajoutez l'utilisateur à un groupe Data Protector disposant des autorisations de **Reporting et notification** et d'**Affichage des objets privés**.

   Cela implique généralement d'ajouter l'utilisateur au groupe Admin. Toutefois, pour empêcher qu'un utilisateur hérite d'autres privilèges d'administrateur, créez un groupe doté des autorisations Reporting et notification et Affichage des objets privés et ajoutez-y l'utilisateur.

6. Vérifiez que les privilèges d'authentification à distance sont correctement configurés en exécutant la commande suivante à partir de l'hôte de l'agent :

   ```
   omnirpt -tab -report list_sessions -timeframe 06/01/01 12:00
   06/01/30 12:00
   ```

   En cas de succès, cette commande renvoie une liste de toutes les sessions exécutées sur le serveur protecteur de données au cours de la période spécifiée. Si une erreur indiquant une autorisation insuffisante pour exécuter les rapports s'affiche, examinez les paramètres de configuration sur le serveur Data Protector.

Surveillance d'IBM Tivoli Storage Manager (TSM)

Surveillez un serveur TSM à partir d'un agent s'exécutant sur le serveur TSM ou à distance à partir d'un agent qui s'exécute sur un hôte différent (comme le serveur DPA). Si vous surveillez TSM à distance, suivez les instructions de la section

Surveillance de TSM à distance à la page 181 avant de configurer le serveur dans DPA.

Avant de démarrer le Discovery Wizard pour la surveillance de TSM

Les données d'identification TSM doivent utiliser le nom et le mot de passe d'un administrateur TSM. L'administrateur ne doit pas nécessairement disposer de privilèges d'accès illimités au système. Des privilèges d'analyste ou d'opérateur suffisent.

Procédure

1. Si le serveur surveillé est un client de librairie partagé, définissez l'agent avec les variables d'environnement DPA (UNIX) ou les paramètres de registre (Windows) suivants pour interroger le gestionnaire de librairies du serveur, afin de collecter certaines données :
   - AGENT_TSM_LIBMGRUSERNAME
   - AGENT_TSM_LIBMGRPASSWORD

   Par défaut, l'agent utilise les mêmes informations d'identification que celles utilisées pour interroger le client de bibliothèque pour interroger le gestionnaire de bibliothèques.
2. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour TSM, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.
3. Sélectionnez **Admin** > **System** > **Manage Credentials** pour modifier les informations d'identification TSM qui ont été créées une fois que vous avez utilisé le Discovery Wizard pour créer un objet TSM.

Greshem Clareti EDT

Dans les environnements Tivoli Storage Manager qui utilisent Gresham Clareti EDT pour le contrôle de périphériques, DPA communique avec EDT pour recueillir des informations de configuration du périphérique en lisant les informations provenant de deux fichiers, à savoir :

- `elm.conf`
- `rc.edt`

DPA lit dans le fichier `elm.conf` à l'emplacement suivant :

- Sous Windows, une variable d'environnement *EDT_DIR* est configurée par EDT. DPA recherche l'emplacement spécifié dans la variable d'environnement *EDT_DIR*.
- Sous Unix, DPA recherche d'abord `elm.conf` dans le fichier `/opt/GESedt-acsls/bin`. S'il ne le trouve pas, DPA cherche sur AIX à l'emplacement `/usr/lpp/dtelm/bin`. Dans d'autres versions d'UNIX/Linux, DPA cherche dans `/opt/OMIdtelm/bin`.

Si le fichier `elm.conf` ne figure pas dans ces répertoires, la variable de registre (Windows) ou la variable d'environnement (UNIX) `AGENT_TSM_ELMCONF_FILENAME` peut être définie sur l'emplacement de `elm.conf`, si nécessaire.

DPA lit dans le fichier `rc.edt` à l'emplacement suivant :

- Sous Windows, DPA recherche l'emplacement spécifié dans la variable d'environnement *EDT_DIR*.

- Sous UNIX, DPA recherche d'abord `rc.edt` dans `/opt/GESedt-acsls/SSI`. S'il ne le trouve pas, sous AIX DPA recherche dans `/usr/lpp/dtelm/bin`. Dans d'autres versions d'UNIX/Linux, DPA effectue la recherche dans `/opt/OMIdtelm/bin`.

Si le fichier `rc.edt` ne figure pas dans ces répertoires, la variable de registre (Windows) ou la variable d'environnement (UNIX) `AGENT_TSM_RCEDT_FILENAME` peut être définie sur l'emplacement de `rc.edt`, si nécessaire.

Remarque

Étant donné qu'un environnement TSM utilisant EDT a besoin de l'agent pour effectuer une lecture dans ces fichiers afin de collecter les données de configuration, l'agent doit être situé sur le même serveur que le serveur TSM.

Surveillance de TSM à distance

En cas de surveillance d'une instance TSM à distance, vous devez installer le logiciel client TSM sur l'hôte qui surveille l'instance TSM. Le module TSM utilise la commande `dsmadmc` incluse avec le logiciel client TSM pour se connecter à l'instance TSM et collecter ses données.

Dans une installation de client TSM par défaut sur un ordinateur Windows, les composants administratifs requis par DPA ne sont pas installés. Pour installer les composants administratifs :

Procédure

1. Cliquez sur **Custom** lorsque vous y êtes invité durant l'installation du client TSM.
2. Sélectionnez **Administrative Client Command Line Files**, puis cliquez sur **Next**.

   L'installation du client TSM continue.
3. Une fois l'installation du client TSM terminée, initialisez le client pour la première fois en démarrant l'interface utilisateur de TSM Backup-Archive à partir du menu **Start**. Utilisez l'assistant pour configurer le client.
4. Pour configurer le client, acceptez la valeur par défaut **Help me configure the TSM Backup Archive Client**, puis cliquez sur **Suivant**. Importez un fichier d'options existant ou créez-en un lorsque vous y êtes invité.
5. Acceptez la valeur par défaut **Create a new options file**. Vous devez créer un fichier d'options vierge nommé `dsm.opt` dans le répertoire `baclient`, sous le répertoire d'installation pour TSM (par défaut `C:\Program Files\Tivoli\TSM`).
6. Continuez à progresser dans l'exécution de l'assistant. Parcourez toutes les fenêtres de l'assistant jusqu'à créer un fichier d'options.

À propos de la collecte de données de tâches après la découverte de TSM

Découvrez-en plus sur la collecte de données de tâches TSM après avoir découvert le TSM interne à DPA.

- Lorsqu'un nouveau serveur TSM est découvert, DPA rassemble les données des tâches jusqu'à 14 jours antérieures.
- L'heure d'interrogation est actuellement fixée au jour suivant et les données seront collectées pour le lendemain lors de la prochaine demande de surveillance des tâches.

- Le temps d'interrogation actuel est avancé un jour à la fois à partir de 14 jours antérieurs. À chaque fois que la demande de surveillances des tâches s'exécute, les données du jour même sont collectées jusqu'à ce que deux semaines de données aient été collectées. La collecte de données reprend ensuite son fonctionnement normal.
- La valeur de temps d'interrogation par défaut est de 1 jour et est configurable par l'utilisateur dans la section d'options de demande de surveillances des tâches TSM.

Les Options de demande de collecte de données par module fournissent des informations supplémentaires.

Surveillance de Symantec Backup Exec

Surveillez les serveurs Symantec Backup Exec à partir d'un agent exécuté sur le serveur Backup Exec ou d'un agent exécuté sur un autre ordinateur Windows de l'environnement. Le service Agent DPA doit s'exécuter avec un compte nommé pouvant s'authentifier auprès du serveur BackupExec.

Surveillance de serveurs de sauvegarde dans un environnement Symantec Cluster Server et Microsoft Cluster Server

Cette section fournit des informations de configuration permettant de surveiller des serveurs de sauvegarde dans des environnements Symantec Cluster Server et Microsoft Cluster Server (MSCS).

Plates-formes prises en charge

- Symantec Cluster Server est pris en charge sous Linux et Solaris
- MSCS est pris en charge pour Windows

Le document *Guide de compatibilité de Data Protection Advisor* fournit des informations concernant les versions de plates-formes prises en charge.

Surveillance des applications de sauvegarde configurées comme partie d'un cluster

Vous pouvez surveiller vos applications de sauvegarde configurées comme faisant partie d'un cluster de plusieurs façons.

Pour surveiller une application de sauvegarde dans un environnement de cluster, procédez comme suit :

Procédure

1. Installez un agent distant sur un système en dehors du cluster. Assurez-vous que<:hs>:
   - l'agent peut accéder au serveur virtuel du cluster via les ports requis.
   - l'agent dispose de tous les fichiers binaires d'application de sauvegarde requis.
2. Découvrez le serveur virtuel du cluster à l'aide du DPA Discovery Wizard.
3. Collectez les données à l'aide de l'agent distant.

Résultats

Dans cette configuration, si le serveur bascule, le nom du cluster se résout systématiquement et fournit les données de sauvegarde.

Procédure alternative pour la surveillance des applications de sauvegarde configurées comme partie d'un cluster
Pour surveiller une application de sauvegarde dans un environnement de clusters ainsi que les ressources de l'hôte local

Procédure

1. Installez un agent local sur chaque hôte du cluster pour la surveillance de l'hôte uniquement.
2. Sélectionnez un des agents sur les serveurs physiques pour surveiller le serveur virtuel.

Avant de démarrer le Discovery Wizard pour la surveillance de Symantec Backup Exec

Pour surveiller un serveur de sauvegarde Symantec Backup Exec à distance, l'agent doit être exécuté en tant que compte utilisateur nommé plutôt que comme compte de système local. Lors de l'installation de l'agent, vous êtes invité à spécifier si l'agent est exécuté à l'aide du compte Système local ou en tant qu'utilisateur nommé.

Les données d'identification de Backup Exec doivent utiliser le nom d'utilisateur et le mot de passe d'un compte administrateur Windows sur le serveur Backup Exec.

Sélectionnez **Admin** > **System** > **Manage Credentials** pour modifier les informations d'identification de Backup Exec qui ont été créées après l'utilisation du Discovery Wizard pour créer un objet Backup Exec.

Surveillance de Backup Exec à distance

Pour vérifier que l'agent est en cours d'exécution, démarrez le Gestionnaire de contrôle des services Windows (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**). Cliquez avec le bouton droit de la souris sur le service de l'agent DPA et sélectionnez Properties :

Procédure

1. Sélectionnez l'onglet **Log On** du panneau Service Properties.
2. Sélectionnez **This account**.
3. Saisissez le nom d'utilisateur et le mot de passe du compte d'administrateur local exécuter le service.
4. Modifiez les détails du compte de service, puis cliquez sur **OK**.
5. Redémarrez le service pour activer les modifications.

Surveillance de Symantec NetBackup

Configurez un serveur Symantec NetBackup à surveiller à partir d'un agent exécuté sur le serveur maître Netbackup Master Server ou à partir d'un agent exécuté sur un autre hôte, tel que le serveur DPA.

Lors de la surveillance de Symantec NetBackup à partir d'un agent proxy, il est possible qu'un agent proxy surveille des serveurs maîtres NetBackup se trouvant dans le même domaine que NetBackup Media Manager (EMM). Cela signifie qu'un agent est requis pour chaque domaine EMM.

Avant de démarrer le Discovery Wizard pour la surveillance de Symantec NetBackup

Les données relatives à l'état du serveur de média ne peuvent uniquement être collectées si un agent est installé sur le serveur de média lui-même. Elles ne peuvent pas être collectées par l'intermédiaire d'un proxy.

Vous devez spécifier l'option `timeformat` dans la demande jobmonitor pour recueillir des informations sur les fichiers ouverts, les erreurs et le montage. Par exemple, "%m/%d/%Y %T"
Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour NetBackup, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Configuration d'une authentification NetBackup pour une collecte de données à distance

Pour collecter des données à distance, vous devez configurer les éléments suivants :

- L'installation de la console d'administration à distance NetBackup, un composant du logiciel serveur NetBackup, est requise sur l'hôte de l'agent.
- L'hôte de l'agent doit pouvoir résoudre NetBackup Master Server.
- NetBackup Master Server doit pouvoir résoudre l'hôte de l'agent.

Les sections suivantes indiquent comment résoudre l'hôte de l'agent à partir du serveur maître NetBackup sous Unix et Windows.

Configuration d'une authentification NetBackup pour une collecte de données à distance sur UNIX

Si le NetBackup Master Server s'exécute sur un ordinateur UNIX, vous devez ajouter le nom de l'hôte sur lequel l'agent est en cours d'exécution, au fichier `bp.conf` sur le serveur maître NetBackup.

Pour ajouter l'hôte :

Procédure

1. Ouvrez le fichier `/usr/openv/netbackup/bp.conf` pour le modifier et ajoutez la ligne suivante :

   SERVER = *Agent*host
   où *Agenthost* est le nom d'hôte de l'agent. Le nom d'hôte de l'agent doit pouvoir être résolu par le Master Server.

2. Redémarrez NetBackup sur le Master Server pour valider les modifications.

Configuration d'une authentification NetBackup pour une collecte de données à distance sur Windows

Si le Master Server NetBackup est exécuté sur un ordinateur sous Windows, ajoutez le nom de l'hôte de l'agent via la console d'administration NetBackup :

Procédure

1. Sur le serveur NetBackup, démarrez **NetBackup Administration Console** et ouvrez la boîte de dialogue **Master Server Properties** :
   - Sélectionnez **Netbackup Management** > **Host Properties** > **Master Servers**.
2. Double-cliquez sur **Host** dans le volet de droite.
3. Dans le champ **Master Servers Properties, Servers** entrez le nom de l'hôte de l'agent à la liste des serveurs supplémentaires autorisés à accéder au Master Server.
4. Cliquez sur **OK**.

5. Redémarrez les services NetBackup. Vous pouvez également redémarrer la machine pour activer les modifications.

Surveillance de Symantec PureDisk

Configurez un serveur Symantec PureDisk à surveiller à partir d'un agent exécuté sur le serveur PureDisk ou à partir d'un agent exécuté sur un autre hôte. Symantec PureDisk peut uniquement être surveillé sur SUSE Linux 10. L'utilisateur root ne peut pas être utilisé pour recueillir des données sur PureDisk.

Avant de démarrer le Discovery Wizard pour la surveillance de Symantec PureDisk

Les serveurs PureDisk mettent en œuvre un pare-feu qui peut empêcher DPA de collecter des données à partir de PureDisk ou de communiquer avec un agent installé sur le serveur PureDisk. Pour vous assurer de la réussite de la collecte de données et des communications, lisez les sections suivantes. Elles traitent de la façon de configurer le serveur PureDisk avant de configurer le serveur dans DPA.

Le processus de configuration dépend de la version du PureDisk surveillé.

Configuration manuelle du pare-feu (versions de PureDisk antérieures à la version 6.5)

Procédure

1. Connectez-vous au serveur PureDisk en tant qu'utilisateur root.
2. Désactivez le pare-feu de PureDisk en exécutant la commande suivante :

   `/etc/init.d/pdiptables stop`

3. Modifiez le fichier `/etc/puredisk/iptables-rules` en insérant l'une des lignes suivantes juste après cette ligne dans le fichier :

   ```
   -A INPUT -p icmp -j ACCEPT
   ```

   Remarque

   Il est important d'insérer la ligne au bon endroit du fichier. Dans le cas contraire, la ligne pourrait ne pas être active.

   - Si vous surveillez PureDisk à l'aide d'un agent installé sur le serveur PureDisk, ajoutez la ligne suivante :

     `-A INPUT -p tcp -m tcp --dport 3741 -j ACCEPT`

   - Si vous surveillez PureDisk à l'aide d'un agent installé sur un hôte différent, ajoutez la ligne suivante :

     `-A INPUT -p tcp -m tcp --dport 10085 -j ACCEPT`

4. Réactivez le pare-feu de PureDisk en exécutant la commande suivante :

   `/etc/init.d/pdiptables start`

Mise à jour des règles de table IP (PureDisk version 6.5)

La configuration manuelle du pare-feu ne fonctionnera pas pour PureDisk version 6.5. Pour mettre à jour la table IP de PureDisk :

Procédure

1. Ouvrez le fichier suivant dans un éditeur de texte :

   ```
   /etc/puredisk/custom_iptables_rules
   ```

2. Si l'agent DPA est installé sur le serveur PureDisk, ajoutez la ligne suivante au fichier de règles (trois colonnes séparées par une tabulation) :

   ```
   tcp     {controller_host_ip}     3741
   ```

   Vous autorisez ainsi les connexions depuis l'hôte du contrôleur vers l'agent DPA sur le port 3741 du serveur Puredisk.

3. Si l'agent DPA est installé sur un hôte distant, ajoutez la ligne suivante au fichier de règles (trois colonnes séparées par une tabulation) :

Résultats

```
tcp     {agent_host_ip}     10085
```

Vous autorisez ainsi les connexions depuis l'hôte de l'agent vers la base de données Postgres sur le port 10085 du serveur Puredisk.

Vous pouvez spécifier un seul hôte ou l'intégralité d'un sous-réseau (en incluant un / masque), comme dans l'exemple suivant :

```
tcp    10.64.205.0/24                  10085
```

Pour plus d'informations sur la configuration de ce fichier, consultez le fichier /etc/puredisk/custom_iptables_rules.

Surveillance de VMware vSphere Data Protection

Surveillez les serveurs VMware vSphere Data Protection (VDP/A) à l'aide d'un agent DPA installé sur un ordinateur distant dans l'environnement, y compris le serveur DPA.

N'installez pas d'agent DPA sur le serveur VMware vSphere Data Protection.

Avant de démarrer Discovery Wizard pour la surveillance de VDP/A

Aucun logiciel supplémentaire n'est nécessaire pour surveiller un serveur VMware vSphere Data Protection à distance.

Avant de commencer

Assurez-vous que vous disposez du nom d'hôte pouvant être résolu ou de l'adresse IP du serveur VMware vSphere Data Protection.

Pour recueillir des données sur un serveur VMware vSphere Data Protection, DPA se connecte directement à la base de données VDP/A. Cette connexion à la base de données est effectuée sur le port par défaut, à savoir 5555. Le port n'est pas configurable.

Pour la surveillance de VDP 5.5, 5.8 et 6.0

Procédure

1. Modifiez le fichier `postgressql.conf`. Supprimez le commentaire de ligne de la commande suivante et modifiez `localhost` en `localhost, Agent_IP_Address`

```
vi /data01/avamar/var/mc/server_data/postgres/data/
postgresql.conf
listen_addresses='localhost,Agent_IP_Address'
```

2. Modifiez le fichier `pg_hba.conf`. Ajoutez la deuxième ligne :

```
vi /data01/avamar/var/mc/server_data/postgres/data/pg_hba.conf
host all all Agent_IP_Address/0 trust
```

3. Modifiez firewall.base, `vi /etc/firewall.base`.
   a. Activez l'accès à distance au service de base de données Postgres.
   b. Ajoutez les lignes suivantes à la fin du fichier `firewall.base` :

```
iptables -I INPUT 1 -p tcp --dport 5555 -j ACCEPT
iptables -I INPUT 1 -p tcp --dport 5558 -j ACCEPT
```

4. Redémarrez l'appliance VDP.

Surveillance des applications d'entreprise de sauvegarde Data Domain

DPA prend en charge les applications de sauvegarde d'entreprise Data Domain (DDBEA) pour les bases de données de sauvegarde, sans utiliser d'autre application de sauvegarde. Par exemple, la sauvegarde d'Oracle RMAN s'effectue sans utiliser NetWorker. Pour plus d'informations sur les bases de données prises en charge, consultez le guide de compatibilité EMC Data Protection Advisor Software Compatibility Guide.

Si vous surveillez l'application d'entreprise pour la sauvegarde d'Oracle RMAN, suivez la procédure fournie dans la section Surveillance d'Oracle et d'Oracle RMAN à la page 191.

Si vous surveillez l'application d'entreprise pour la sauvegarde de Microsoft SQL Server, suivez la procédure fournie dans la section Surveillance de Microsoft SQL Server à la page 190.

Si vous surveillez l'application d'entreprise pour la sauvegarde de PostgreSQL, suivez la procédure fournie dans la section Surveillance de PostgreSQL à la page 198.

Si vous surveillez l'application d'entreprise pour la sauvegarde de SAP HANA, suivez la procédure fournie dans la section Surveillance SAP HANA à la page 199.

Surveillance de bases de données

Cette section explique comment surveiller des bases de données.

Surveillance de DB2

Une base de données DB2 peut être surveillée à partir d'un agent exécuté sur le même hôte que le serveur DB2 ou à partir d'un agent exécuté sur un autre hôte, tel que le serveur DPA. L'Agent DPA doit être exécuté sous Windows ou Linux.

Avant de démarrer le Discovery Wizard pour la surveillance de DB2

Pour que l'agent DPA collecte les données de la base de données DB2, vous devez copier le fichier client DB2 .jar dans le répertoire des plug-in DPA.

Procédure

1. Créez un dossier appelé *plugins* dans `<DPA_install_dir>\agent\`.
2. Copiez le fichier jar DB2 client *db2jcc4.jar* dans le dossier *plugins* dans `..\EMC\dpa\agent\`.

   Si vous utilisez un autre emplacement ou chemin d'accès, ajoutez la balise suivante : `<PLUGINSDIR>path </PLUGINSDIR> in dpaagent_config.xml` situé sous `<DPA_install_dir>\agent\etc`

   où *path* désigne le chemin d'accès au répertoire créé lors de l'étape 1.

   Par exemple `<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>`
3. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour DB2, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Autorisations

Assurez-vous que vous disposez des autorisations adéquates pour collecter des données sur DB2.

Assurez-vous que vous disposez des autorisations Select operations :

- affichage `sysibmadm.db_history`.
- tables `<user_name>.UTILSTOP_DPABACKUP` et `sysibm.syscolumns`. Cela est requis pour DB2 11.1.1.1 et les versions ultérieures.

Configuration de DB2 pour l'affichage de la taille du champ dans le rapport Backup All Jobs

Vous devez créer le DB2 EVENT MONITOR DPABACKUP sur la base de données DB2 pour que l'agent DPA envoie des données vers le serveur DPA avec la valeur de taille de sauvegarde DB2.

Avant de commencer

- DPA prend en charge le calcul de la taille de la sauvegarde uniquement pour DB2 11.1.1 et versions ultérieures.
- L'event monitor doit être créé par l'utilisateur dont informations d'identification sont attribuées à la demande Jobmonitor de DB2.

Effectuer cette procédure sur la base de données DB2. Pour plus d'informations sur la manière d'effectuer ces étapes sur DB2, consultez la documentation du fournisseur.

Procédure

1. Créer un événement : `CREATE EVENT MONITOR DPABACKUP FOR CHANGE HISTORY WHERE EVENT IN (BACKUP) WRITE TO TABLE autostart`
2. Démarrer Event Monitor.
3. Définir Event Monitor sur `DPABACKUP state 1`.
4. Vérifier que l'événement a bien été créé. Exécuter la base de données de sauvegarde en ligne. Saisir : `backup database sample online`

   Le nouvel enregistrement doit être présent dans le tableau.
5. Sélectionner *__from UTILSTOP_DPABACKUP__.

À propos de la collecte de données de tâches après la découverte

Découvrez-en plus sur la collecte de données de tâches après avoir découvert certaines applications internes à DPA.

Les informations contenues dans cette section s'appliquent aux applications suivantes :

- NetWorker
- Avamar
- TSM
- HP Data Protector
- Commvault Simpana
- NetBackup
- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

En ce qui concerne les applications ci-dessus, notez les points suivants :

- Lorsqu'un nouveau serveur est découvert, DPA rassemble les données des tâches jusqu'à 14 jours antérieures si vous activez cette fonction.
- L'heure d'interrogation est actuellement fixée au jour suivant et les données seront collectées pour le lendemain lors de la prochaine demande de surveillance des tâches.
- Le temps d'interrogation actuel est avancé un jour à la fois à partir de 14 jours antérieurs. À chaque fois que la demande de surveillances des tâches s'exécute, les données du jour même sont collectées jusqu'à ce que deux semaines de données aient été collectées. La collecte de données reprend ensuite son fonctionnement normal.
- La valeur de temps d'interrogation par défaut est de 1 jour et est configurable par l'utilisateur dans la section d'options de demande de surveillances des tâches.
- Lors de la configuration de la collecte de données, la **fréquence** doit toujours être une valeur inférieure à **la période maximale des données recueillies par chaque demande**. Dans le cas contraire, la demande ne rattrape pas l'heure actuelle et elle prend davantage de retard à chaque exécution et ne collecte pas les données restantes.

Les Options de demande de collecte de données par module fournissent des informations supplémentaires.

Surveillance de Microsoft SQL Server

Surveillez les serveurs Microsoft SQL Servers à partir d'un agent s'exécutant sur la base de données SQL Server ou à partir d'un agent s'exécutant sur un autre ordinateur Windows de l'environnement. Le service Agent DPA doit s'exécuter avec un compte nommé pouvant s'authentifier auprès des serveurs Microsoft SQL Server.

Assurez-vous que vous spécifiez les règles de trafic entrant du pare-feu de façon à autoriser les connexions entrantes au service SQL Server Browser SQLBrowser.exe. Il utilise le port 1434 UDP.

Avant de démarrer le Discovery Wizard pour la surveillance de Microsoft SQL Server

Pour se connecter à SQL Server avec l'authentification Windows, l'agent DPA doit être exécuté en tant que compte utilisateur nommé avec accès MS-SQL plutôt qu'en tant que compte de système local. Vérifiez que le service est exécuté avec le bon compte utilisateur avant de poursuivre la configuration de la base de données.

Pour surveiller les installations de SQL Server en cluster, configurez DPA pour le surveiller en tant que cible distante, même si l'agent DPA est installé localement sur un nœud physique du cluster. Le nom de la cible doit être défini sur le nom de l'alias du cluster.
Assurez-vous que l'agent DPA dispose d'un accès en lecture à la fois pour le rôle de maître DPA et pour les bases de données MSDB pendant le test de découverte DPA, même si vous ne sélectionnez pas la surveillance de base de données.

Prérequis de l'agent pour la surveillance de Microsoft SQL Server

L'agent doit être en mesure de se connecter à la base de données « principale » SQL Server afin de collecter les données requises. L'agent peut soit :

- utiliser l'authentification SQL Server à l'aide des informations d'identification de la demande (si cet élément est configuré) ;
- utiliser l'authentification SQL Server à l'aide des informations d'identification sur une base de données « principale » explicite qui est répertoriée dans la liste des bases de données à surveiller (si cet élément est configuré) ;
- si ces éléments ne sont pas configurés, l'agent utilise l'authentification Windows à l'aide de l'ID de connexion du processus de l'agent.

Si aucun de ces éléments ne permet d'établir une connexion à la base de données « principale », la demande ne collectera aucune donnée.

Prérequis de compte utilisateur pour la surveillance de Microsoft SQL Server

Pour collecter des données, le compte utilisateur utilisé pour se connecter à la base de données SQL Server doit disposer de privilèges spécifiques. Tout utilisateur de SQL Server avec accès dbo dispose par défaut des privilèges appropriés.

Si vous ne voulez pas vous connecter avec un utilisateur disposant d'un accès dbo, configurez un utilisateur de la façon suivante :

- Mappez l'utilisateur sur la base de données avec le rôle public.
- Octroyez explicitement des privilèges VIEW SERVER STATE et VIEW DEFINITION (SQL Server 2005 uniquement).

Le privilège VIEW SERVER STATE est accordé au niveau du serveur. Le privilège VIEW DEFINITION peut être accordé au niveau du serveur (sous le nom VIEW ANY DEFINITION) ou au niveau de la base de données, du schéma ou de l'objet individuel.

- Accordez explicitement l'autorisation d'exécution du système `stored procedure xp_readerrorlog`.

SQL Server 2005 et 2008

Pour octroyer des privilèges au niveau de tout le serveur à la connexion SQL Server utilisée par l'agent, y compris des privilèges VIEW DEFINITION pour toutes les tables de base de données, connectez-vous à SQL Server en tant qu'administrateur et exécutez ce qui suit :

```
GRANT VIEW SERVER STATE TO <login\domain> GRANT VIEW ANY DEFINITION TO <login\domain>
```

Toutefois, pour accorder des privilèges VIEW DEFINITION limités aux bases de données spécifiques que vous souhaitez surveiller, connectez-vous à SQL Server en tant qu'administrateur et exécutez ce qui suit :

```
GRANT VIEW SERVER STATE TO [login\domain] GRANT VIEW DEFINITION ON DATABASE :: <dbname> TO <username>
```

Pour accorder l'autorisation d'exécution de la procédure stockée du système xp_readerrorlog, exécutez :

```
USE Master GO GRANT EXECUTE ON OBJECT::sys.xp_readerrorlog TO ddDBO GO
```

Surveillance de Microsoft SQL Server pour l'analyse de la réplication

Le serveur DPA doit se connecter en tant qu'utilisateur de base de données doté de privilèges de connexion sur toutes les bases de données et d'une autorisation d'écriture sur la base de données TEMPDB. Pour l'authentification Windows, l'utilisateur doit pouvoir se connecter à toutes les bases de données SQL Server et disposer du privilège en écriture pour la base de données TEMPDB.

Surveillance d'Oracle et d'Oracle RMAN

DPA peut collecter des données depuis deux parties d'Oracle : soit directement depuis la base de données Oracle, où il collecte des metrics relatifs à l'instance de base de données ; soit depuis Oracle RMAN. Dans les deux cas, il vous faut installer le logiciel client Oracle.

DPA ne fournit pas de bibliothèques de client Oracle (OCI) avec l'agent DPA. Vous pouvez télécharger le logiciel client Oracle Instant depuis oracle.com pour la plate-forme/l'OS pour lequel vous souhaitez l'installer. Assurez-vous que la version de l'architecture correspond bien à votre système d'exploitation ainsi qu'à vos versions d'Oracle. Pour collecter des données depuis une base de données Oracle 12c par exemple, utilisez la version du client Oracle 12c Instant. Si vous collectez depuis des versions d'Oracle mixtes, utilisez la dernière version pour le client instantané dans votre environnement. Pour que l'agent DPA collecte les données d'une base de données Oracle ou de Oracle RMAN, les bibliothèques suivantes sont nécessaires :

- `libociei.so`
- `libocci.so`
- `libclntsh.so`
  Il vous faut créer un lien symbolique pour la bibliothèque `libclntsh.so` dans le répertoire de versions actuel d'Oracle. Pour plus d'informations, reportez-vous à la

section Création d'un lien symbolique pour le répertoire de versions actuel d'Oracle sous UNIX à la page 192.

Vous devez la copier manuellement dans `AGENT_ORACLE_CLIENT_PATH` afin d'utiliser l'agent DPA.

Sous Windows, il s'agit du répertoire `OCI.DLL` et sous Unix, il s'agit de `libclntsh.so`.

Remarque

La bibliothèque doit être destinée à la même plate-forme que l'agent DPA. Par exemple, si un agent DPA pour Windows 64 bits est installé, vous devez alors utiliser la bibliothèque Oracle pour Windows 64 bits.

Le client Oracle Database Instant est téléchargeable depuis le site http://www.oracle.com/technetwork/database/features/instant-client/index.html

Lors de l'installation de l'agent DPA, vous êtes invité à préciser si vous voulez utiliser l'agent pour surveiller Oracle et, le cas échéant, à indiquer l'emplacement des bibliothèques du client Oracle. Sous Windows, cette action permet de définir un paramètre de registre et sous UNIX, elle permet de modifier une variable d'environnement dans le fichier `dpa.config`. Si vous modifiez l'emplacement des bibliothèques après la fin du processus d'installation, vous devez effectuer ces étapes manuellement.

Création d'un lien symbolique pour le répertoire de versions actuel d'Oracle sous UNIX

Il vous faut créer un lien symbolique pour la bibliothèque `libclntsh.so` dans le répertoire de versions actuel d'Oracle. Vous devez la copier manuellement dans `AGENT_ORACLE_CLIENT_PATH` afin d'utiliser l'agent DPA.

Procédure

1. Installez à l'aide de la commande `rpm`. Exécutez : **`rpm -i oracle.instantclient<version.build.architecture>.rpm`**.

   Par exemple : **`rpm -i oracle.instantclient12.1-basic-12.1.0.2.0-1.x86.rpm`**
   Les résultats de `/usr/lib/oracle/12.1/client64/lib` montrent la dernière version du client Oracle. Par exemple, `libclntsh.so.12.1`.
2. Créez le lien symbolique pour libclntsh.so et ajoutez des autorisations d'exécution sur les fichiers. Exécutez : **`ln -s libclntsh.so<version.build.architecture> libclntsh.so chmod 755 *`**

   Par exemple : **`ln -s libclntsh.so.21.1 libclntsh.so chmod 755 *`**
3. Vérifiez que le build actuel d'Oracle soit créé dans `/usr/lib/oracle` (http://docs.oracle.com/cd/B19306_01/server.102/b14357/ape.htm)

Windows

Procédure

1. Mettez à jour l'entrée du registre avec l'emplacement du logiciel client Oracle Instant :
   a. Rendez-vous à l'emplacement où le dossier contenant le logiciel client Oracle est situé.

b. Utilisez regedit pour modifier manuellement l'emplacement du logiciel client Oracle Instant.

Configuration manuelle de l'agent DPA afin de surveiller une base de données Oracle et Oracle RMAN

- Pour configurer manuellement l'agent DPA afin de surveiller Oracle RMAN : Sous Windows, définissez la clé de registre HKLM/Software/EMC/DPA/Agent sur le type de valeur REG_SZ comme suit :

  Nom de la valeur : *ORACLE_CLIENT_PATH*

  Données de la valeur : `<directory containing the Oracle client libraries - oci.dll>`

Remarque

La clé de registre est créée si vous avez sélectionné l'option Oracle database to be monitored pendant l'installation de l'agent DPA. Si la clé de registre n'a pas été créée, vous devez la créer manuellement.

- Sous UNIX, modifiez le fichier `dpa.config`

Le fichier `dpa.config` est disponible dans `<installdir>/agent/etc/dpa.config`. Recherchez la ligne AGENT_ORACLE_CLIENT_PATH= et définissez la variable dans le répertoire contenant les bibliothèques du client Oracle : `libclntsh.so`.

Redémarrez le service Agent si vous avez modifié le fichier `dpa.config` pour inclure le chemin du client Oracle.

Remarque

Nous vous recommandons de discuter des exigences en matière de licence RMAN avec votre responsable de compte EMC.

Avant de démarrer le Discovery Wizard pour la surveillance d'Oracle

Pour surveiller une base de données Oracle (données de protection des données), l'agent doit se connecter à la base de données sous un compte utilisateur Oracle.

Avant de commencer

DPA n'exige pas le mot de passe du système d'exploitation pour l'accès au serveur Oracle. DPA nécessite le nom d'utilisateur/mot de passe Oracle utilisé pour les requêtes de catalogue RMAN ou de catalogue système uniquement.

Pour que la collecte de données pour les bases de données Oracle s'exécute correctement, l'utilisateur en question doit pouvoir réaliser des sélections dans les tableaux et vues suivants :

- V_$INSTANCE
- V_$PROCESS
- V_$DATABASE
- V_$PARAMETER
- DBA_DATA_FILES
- V_$SYSTEM_PARAMETER
- V_$DATAFILE

- V_$SESS_IO
- V_$SESSION
- DBA_FREE_SPACE
- V_$SESSMETRIC (Oracle 10 uniquement)
- DBA_TABLESPACES
- DBA_TEMP_FILES
- DBA_EXTENTS
- USER_EXTENTS
- V$LOGFILE
- V$LOG
- AUDIT_ACTIONS
- V$CONTROLFILE

Tout utilisateur avec le rôle SYSDBA dispose par défaut de ces privilèges. Par conséquent, nous vous recommandons de définir un utilisateur ayant le rôle SYSDBA lors de la configuration de la base de données en vue de la surveillance. Pour ne pas avoir à utiliser un utilisateur avec le rôle SYSDBA pour vous connecter, vous pouvez créer un autre utilisateur et lui accorder explicitement des privilèges sur ces tables ou lui accorder un privilège « create session » suivi de SELECT_CATALOG_ROLE, comme dans l'exemple suivant :

Remarque

Les informations suivantes sont requises pour obtenir des données Oracle à partir d'un programme d'installation du cluster.

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$INSTANCE TO limited_user;
GRANT SELECT ON V_$PROCESS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$PARAMETER TO limited_user;
GRANT SELECT ON DBA_DATA_FILES TO limited_user;
GRANT SELECT ON V_$SYSTEM_PARAMETER TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$SESS_IO TO limited_user;
GRANT SELECT ON V_$SESSION TO limited_user;
GRANT SELECT ON DBA_FREE_SPACE TO limited_user;
GRANT SELECT ON DBA_TABLESPACES TO limited_user;
GRANT SELECT ON DBA_EXTENTS TO limited_user;
GRANT SELECT ON USER_EXTENTS TO limited_user;
GRANT SELECT ON DBA_TEMP_FILES TO limited_user;
GRANT SELECT ON V_$LOGFILE TO limited_user;
GRANT SELECT ON V_$LOG TO limited_user;
GRANT SELECT ON  AUDIT_ACTIONS TO limited_user;
GRANT SELECT ON V_$CONTROLFILE TO limited_user;
exit;
```

Ou

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

Pour vous connecter à la base de données du conteneur (CDB) avec une installation de base de données Oracle 12c RAC, vous pouvez utiliser un utilisateur commun qui a

le rôle SYSDBA lors de la configuration de la base de données pour la surveillance. Si vous ne souhaitez pas utiliser un utilisateur avec le rôle SYSDBA pour vous connecter, vous pouvez créer un autre utilisateur. Il doit être précédé par « c## » ou « C## » et posséder explicitement des privilèges sur ces tables ou un privilège « create session » suivi de SELECT_CATALOG_ROLE, comme dans l'exemple ci-dessus.

Pour vous connecter à une base de données enfichable (PDB), vous pouvez utiliser un utilisateur commun qui a le rôle SYSDBA lors de la configuration de la base de données pour la surveillance. Pour ne pas avoir à utiliser un utilisateur commun avec le rôle SYSDBA pour se connecter, vous pouvez créer un utilisateur local spécifique à la PDB et lui accorder explicitement des privilèges sur ces tables PDB ou accorder un privilège « create session » suivi de SELECT_CATALOG_ROLE pour la PDB.

Avant de démarrer le Discovery Wizard pour la surveillance de RMAN

Pour surveiller une base de données RMAN (données de protection des données), l'agent doit se connecter à la base de données sous un compte utilisateur Oracle.

Avant de commencer

Procurez-vous les paramètres de connexion d'informations suivants auprès de l'administrateur BD Oracle, depuis le catalogue RMAN ou depuis les requêtes du catalogue du système :

- Identifiant SID Oracle du catalogue RMAN
- Port TNS Oracle utilisé pour le catalogue RMAN
- Nom d'utilisateur/mot de passe Oracle RMAN avec les privilèges requis. Il s'agit des privilèges SELECT seuls ou des privilèges SELECT_CATALOG_ROLE. Dans le cas de multiples catalogues RMAN sur un serveur Oracle unique, vous devez disposer d'un nom d'utilisateur/mot de passe dans chaque schéma. La pratique recommandée consiste à utiliser la même combinaison nom d'utilisateur/mot de passe pour tous catalogues/schémas RMAN.
- Nom du propriétaire du schéma RMAN et, si plusieurs catalogues RMAN sont présents sur un serveur Oracle unique, le nom du propriétaire de chaque schéma RMAN

Pour que la collecte de données pour le catalogue de restauration de surveillances des tâches Oracle RMAN s'exécute correctement, l'utilisateur en question doit pouvoir réaliser des sélections dans les tables et vues suivantes :

- V_$RMAN_CONFIGURATION
- RC_BACKUP_SET
- V$PROXY_DATAFILE
- RC_RMAN_BACKUP_JOB_DETAILS
- RC_BACKUP_DATAFILE
- RC_BACKUP_PIECE
- RC_DATAFILE
- RC_DATABASE
- RC_BACKUP_CONTROLFILE
- RC_BACKUP_CONTROLFILE_DETAILS
- RC_BACKUP_DATAFILE_DETAILS
- RC_RMAN_STATUS
- RC_BACKUP_ARCHIVELOG_DETAILS

- RC_BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

Pour que la collecte de données pour le fichier de contrôle de surveillances des tâches Oracle s'exécute correctement, l'utilisateur en question doit pouvoir réaliser des sélections dans les tableaux et vues suivants :

- V_$RMAN_CONFIGURATION
- V_$RMAN_STATUS
- V_$BACKUP_DATAFILE
- V_$BACKUP_PIECE
- V$BACKUP_SET
- V$PROXY_DATAFILE
- V$RMAN_BACKUP_JOB_DETAILS
- V$DATABASE
- V$DATAFILE
- V$BACKUP_DATAFILE_DETAILS
- V$BACKUP_ARCHIVELOG_DETAILS
- V$BACKUP_REDOLOG
- RCVER
- PRODUCT_COMPONENT_VERSION

Tout utilisateur avec le rôle SYSDBA dispose par défaut de ces privilèges. Par conséquent, nous vous recommandons de définir un utilisateur ayant le rôle SYSDBA lors de la configuration de la base de données en vue de la surveillance. Pour ne pas avoir à utiliser un utilisateur avec le rôle SYSDBA pour vous connecter, vous pouvez créer un autre utilisateur et lui accorder explicitement des privilèges sur ces tables ou lui accorder un privilège « create session » suivi de SELECT_CATALOG_ROLE, comme dans l'exemple suivant :

Remarque

Les informations suivantes sont requises pour obtenir des données Oracle à partir d'un programme d'installation du cluster.

Pour le catalogue de restauration de surveillance des tâches Oracle RMAN :

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON RC_BACKUP_SET TO limited_user;
GRANT SELECT ON V$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON RC_RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_PIECE TO limited_user;
GRANT SELECT ON RC_DATAFILE TO limited_user;
GRANT SELECT ON RC_DATABASE TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE TO limited_user;
GRANT SELECT ON RC_BACKUP_CONTROLFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON RC_RMAN_STATUS TO limited_user;
GRANT SELECT ON RC_BACKUP_ARCHIVELOG_DETAILS TO limited_user;
```

```
GRANT SELECT ON RC_BACKUP_REDOLOG TO limited_user;
exit;
```

Ou

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

Par défaut, un utilisateur de catalogue virtuel ne dispose d'aucun accès au catalogue de restauration de base. Les privilèges suivants doivent être accordés pour lui permettre d'accéder aux métadonnées :

```
GRANT RECOVERY_CATALOG_OWNER to limited_user;
 GRANT CATALOG for DATABASE db to limited_user;
```

Pour le fichier de contrôle de surveillance des tâches :

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT ON V_$RMAN_CONFIGURATION TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_PIECE TO limited_user;
GRANT SELECT ON V_$RMAN_STATUS TO limited_user;
GRANT SELECT ON V_$BACKUP_SET TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
GRANT SELECT ON V_$DATABASE TO limited_user;
GRANT SELECT ON V_$BACKUP_DATAFILE_DETAILS TO limited_user;
GRANT SELECT ON V_$DATAFILE TO limited_user;
GRANT SELECT ON V_$BACKUP_ARCHIVELOG_DETAILS TO limited_user;
GRANT SELECT ON V_$BACKUP_REDOLOG TO limited_user;
GRANT SELECT ON V_$PROXY_DATAFILE TO limited_user;
GRANT SELECT ON V_$RMAN_BACKUP_JOB_DETAILS TO limited_user;
exit;
```

Ou

```
CREATE USER limited_user IDENTIFIED BY password;
GRANT CREATE SESSION TO limited_user;
GRANT SELECT_CATALOG_ROLE TO limited_user;
exit
```

Pour vous connecter à la base de données du conteneur (CDB) avec une installation de base de données Oracle 12c RAC, vous pouvez utiliser un utilisateur commun qui a le rôle SYSDBA lors de la configuration de la base de données pour la surveillance. Si vous ne souhaitez pas utiliser un utilisateur avec le rôle SYSDBA pour vous connecter, vous pouvez créer un autre utilisateur. Il doit être précédé par « c## » ou « C## » et posséder explicitement des privilèges sur ces tables ou un privilège « create session » suivi de SELECT_CATALOG_ROLE, comme dans l'exemple ci-dessus.

Pour vous connecter à une base de données enfichable (PDB), vous pouvez utiliser un utilisateur commun qui a le rôle SYSDBA lors de la configuration de la base de données pour la surveillance. Pour ne pas avoir à utiliser un utilisateur commun avec le rôle

SYSDBA pour se connecter, vous pouvez créer un utilisateur local spécifique à la PDB et lui accorder explicitement des privilèges sur ces tables PDB ou accorder un privilège « create session » suivi de SELECT_CATALOG_ROLE pour la PDB.

Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour Oracle RMAN, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Surveillance de PostgreSQL

Une base de données PostgreSQL peut être surveillée à partir d'un agent exécuté sur le même hôte que la base de données PostgreSQL ou à partir d'un agent exécuté sur un autre hôte, tel que le serveur DPA.

Avant de démarrer le Discovery Wizard pour la surveillance de PostgreSQL

Pour surveiller une base de données PostgreSQL, l'agent doit se connecter à la base de données avec un compte de superutilisateur PostgreSQL. Par défaut, un superutilisateur dispose des privilèges appropriés. Nous vous recommandons de spécifier un superutilisateur lors de la configuration de la base de données à surveiller.

Pour créer un superutilisateur, l'administrateur PostgreSQL doit être lui-même superutilisateur et créer un compte comme dans l'exemple suivant :

CREATE ROLE xxxxx WITH login superuser password yyyyyy ;

où *xxxxx* est le nouveau nom d'utilisateur et *yyyyyy* le mot de passe du nouvel utilisateur.

Les paramètres ci-après sont renseignés dans la table des paramètres du serveur de bases de données uniquement si vous vous connectez à la base de données en tant que superutilisateur :

- config_file
- data_directory
- dynamic_library_path
- external_pid_file
- hba_file
- ident_file
- krb_server_keyfile
- log_directory
- log_filename
- preload_libraries
- unix_socket_directory

Les éléments suivants sont également indisponibles pour les comptes autres que ceux de superutilisateur :

- Dans la table de configuration des fichiers de données, le chemin complet des fichiers de données ne peut pas être affiché car le chemin du fichier se trouve dans le paramètre data_directory. La chaîne « (répertoire de données postgres) » est indiquée à la place.
- Dans la table d'état de connexion, les valeurs des champs f_command et f_status sont incorrectes. Ces champs indiquent <insufficient privileges>.

La connexion à la base de données en tant que superutilisateur renseigne tous les champs.

Surveillance SAP HANA

Une base de données SAP HANA peut être surveillée à partir d'un agent exécuté sur le même hôte que le serveur SAP HANA ou à partir d'un agent exécuté sur un autre hôte, tel que le serveur DPA. L'Agent DPA doit être exécuté sous Windows ou Linux.

Avant de démarrer le Discovery Wizard pour la surveillance SAP HANA

Pour que l'agent DPA collecte les données de la base de données SAP HANA, vous devez copier le fichier client SAP HANA .jar dans le répertoire des plug-in DPA.

Procédure

1. Créez un dossier appelé *plugins* dans `<DPA_install_dir>\agent\`.
2. Copiez le fichier jar SAP HANA client *ngdbc.jar* dans le dossier *plugins* dans `..\EMC\dpa\agent\`.

   Si vous utilisez un autre emplacement ou chemin d'accès, ajoutez la balise suivante : `<PLUGINSDIR>path </PLUGINSDIR>` in `dpaagent_config.xml` situé sous `<DPA_install_dir>\agent\etc`

   où *path* désigne le chemin d'accès au répertoire créé lors de l'étape 1.

   Par exemple `<PLUGINSDIR>c:\program files\emc\dpa\agent\plugins</PLUGINSDIR>`
3. Si vous souhaitez que DPA collecte les données des tâches jusqu'à 14 jours antérieures et que les rapports affichent les données directement pour SAP HANA, activez les données historiques par défaut à partir de la demande de surveillance des tâches. Dans la console web DPA, accédez à **Inventory** > **Object Library** > **[select object]** > **Data Collection**.

Autorisations de découverte de données pour SAP HANA

Pour rassembler des données sur SAP HANA, l'utilisateur de base de données doit avoir certains privilèges qui permettent à l'utilisateur d'exécuter des requêtes SELECT.

Les informations d'identifications sont utilisées par l'Agent DPA pour accéder aux tableaux suivants :

- M_BACKUP_CATALOG view
- M_BACKUP_CATALOG_FILES view

En règle générale, les privilèges accordés au rôle PUBLIC suffisent à accéder à ces données. Pour plus d'informations, consultez les informations fournisseur concernant les privilèges nécessaires à l'exécution des requêtes SELECT.

Surveillance des applications à l'aide de solutions basées sur le Cloud

Cette section décrit comment surveiller des applications à l'aide de DPA lorsqu'il est déployé sur des solutions basées sur le Cloud.

Surveillance des applications sur Amazon Web Services

DPA prend en charge le déploiement de DPA sur site et au sein d'Amazon Web Services pour la découverte et la surveillance d'applications de sauvegarde et de surveillance prises en charge sur site ou au sein d'Amazon Web Services. Le *Guide de*

compatibilité de Data Protection Advisor fournit des informations sur les versions des applications de sauvegarde et de surveillance prises en charge.

Avant de commencer

- Veillez à configurer l'agent de collecte de données de DPA dans le même espace Amazon Web Services que les objets que vous souhaitez surveiller à l'aide d'Amazon Web Services.
- Si vous configurez DPA pour surveiller des applications déployées sur des solutions basées sur le Cloud à l'aide d'un VPN, veiller à ce que les ports et protocoles soient disponibles sur le VPN. Si vous utilisez des ports non standards pour ouvrir des ports non standards avec votre fournisseur de services Cloud ou avec Amazon Web Services. Paramètres des ports DPA fournit des informations sur les ports DPA standards.

Procédure

1. Déployez DPA dans votre environnement Amazon Web Services.

   Installation de DPA à la page 31 fournit des informations sur l'installation de DPA. Reportez-vous à la documentation d'Amazon Web Services pour les besoins de produits spécifiques.

2. Découvrez l'application prise en charge sur l'instance DPA au sein d'Amazon Web Services.

   Les sections de ce chapitre fournissent des informations. Par exemple, Surveillance de NetWorker à la page 175 fournit des informations sur la découverte et la surveillance de NetWorker.

Surveillance d'applications sur Microsoft Azure

DPA prend en charge le déploiement de DPA au sein d'Azure pour la découverte et la surveillance des applications de sauvegarde et de surveillance prises en charge. Le *Guide de compatibilité de Data Protection Advisor* fournit des informations sur les versions des applications de sauvegarde et de surveillance prises en charge.

Procédure

1. Déployez DPA dans votre environnement Azure.

   Installation de DPA à la page 31 fournit des informations sur l'installation de DPA. Reportez-vous à la documentation d'Azure pour les besoins de produits spécifiques.

2. Découvrez l'application prise en charge sur l'instance DPA au sein d'Azure.

   Les sections de ce chapitre fournissent des informations. Par exemple, Surveillance de NetWorker à la page 175 fournit des informations sur la découverte et la surveillance de NetWorker.

Surveillance des hôtes

Cette section décrit la surveillance des hôtes.

DPA offre deux options lors de la découverte de l'hôte :

- La surveillance du système hôte, pour surveiller la configuration, les performances et l'état du système d'exploitation.
- La surveillance de la réplication, pour effectuer une analyse de la réplication de stockage.

Surveillance des systèmes d'exploitation

Utilisez le système hôte de l'assistant de découverte pour surveiller la configuration, les performances et l'état du système d'exploitation. Plusieurs modules de DPA collectent différents types d'informations, comme décrit dans le tableau suivant.

Tableau 36 Modules de surveillance du système

Module	Description :
Host	Collecte des informations de base concernant le type de système d'exploitation.
Disk	Collecte des informations de configuration, d'état et de performances sur les disques de l'hôte.
Fibre Channel HBA	Collecte des informations de configuration, d'état et de performances sur les adaptateurs HBA Fibre Channel configurés sur l'ordinateur.
File system	Collecte des informations de configuration, d'état et de performances sur les systèmes de fichiers montés sur l'hôte.
Memory	Collecte des informations de configuration, d'état et de performances sur la mémoire de l'hôte.
NetInt	Collecte des informations de configuration, d'état et de performances sur les cartes d'interface réseau dans l'hôte.
Process	Collecte des informations sur tout processus en cours d'exécution sur l'hôte.
Processor	Collecte des informations de configuration, d'état et de performances sur tous les CPU de l'hôte.

Collecte des données des systèmes d'exploitation UNIX

Pour effectuer la surveillance du système sur des ordinateurs UNIX, installez un agent sur l'hôte à surveiller. Il n'est pas possible de collecter des informations système à distance à partir d'ordinateurs UNIX.

Découverte des hôtes d'agent pour UNIX, pour la collecte des données

Les hôtes UNIX sont découverts à l'aide de SSH ou de telnet/ftp avec un accès root.

S'il n'est pas possible d'utiliser des données d'identification « root » (racine) avec DPA en raison des critères de sécurité, sudo peut être un moyen d'élever temporairement les données d'identification de l'utilisateur au niveau « racine » pour certaines commandes configurées dans le fichier de sudo.

Modification du fichier de sudo pour la découverte de stockage DPA
Un utilisateur peut se connecter à un hôte UNIX en tant qu'utilisateur non root et employer sudo pour exécuter avec succès des commandes SCSI dans le cadre de la

découverte d'informations sur le stockage de l'hôte. Voici un exemple de ce qui doit être ajouté au fichier de sudo.

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a
sudoers file.
#
# Host alias specification
# User alias specification
# Cmnd alias specification
# Defaults specification
# User privilege specification
root    ALL=(ALL) ALL
# Uncomment to allow people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL
# Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
# Samples
# %users  ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users  localhost=/sbin/shutdown -h now
user_alias ALL = (ALL) PASSWD: /var/tmp/IllumAgent/apolloreagent
# Defaults specification
# User privilege specification
root ALL=(ALL) ALL
CMGU ALL=NOPASSWD:CMGEMC
# Uncomment to allow people in group wheel to run all commands
# %wheel ALL=(ALL) ALL
# Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
# Samples
# %users ALL=/sbin/mount /cdrom,/sbin/umount /cdrom
# %users localhost=/sbin/shutdown -h now
```

#cmguser ALL=(ALL) NOPASSWD: ALL

Collecte des données des systèmes d'exploitation Windows

Pour collecter des données de performance à partir d'un hôte Windows, vous devez installer l'infrastructure de gestion Windows (WMI) sur l'hôte Windows que vous surveillez.

Il est possible de collecter toutes les informations de surveillance du système à distance à partir d'ordinateurs Windows à l'exception des informations sur les adaptateurs HBA Fibre Channel. Pour collecter des informations sur les adaptateurs HBA Fibre Channel, l'agent doit être installé sur l'ordinateur. Surveillance à distance d'un hôte Windows à la page 203 fournit des informations supplémentaires sur les étapes requises pour surveiller un hôte Windows à distance.

Pour configurer la surveillance d'un système sur lequel un agent est installé, attribuez les demandes de surveillance du système à l'hôte ou au groupe à surveiller.

Découverte des hôtes d'agent pour Windows, pour la collecte des données

Si la découverte d'applications s'effectue sans agent, la découverte d'hôtes Windows utilise le protocole RPC pour l'analyse de réplication et WMI pour les informations système.

Vérification de la communication RPC

Procédure

1. Ouvrez la boîte de dialogue Exécuter à partir du menu **Démarrer** de Windows.

2. Type :

   ```
   net use \\<nom du serveur>\admin$ /user:<nom d'utilisateur>
   ```

3. Cliquez sur **Enter**. Entrez le mot de passe.
4. Une connexion qui aboutit doit renvoyer le message suivant : `The command completed successfully`.
5. Supprimez le mappage réseau. Type :

   ```
   net use \\servername\admin$ /delete
   ```

Vérification de la communication WMI
Procédure

1. Ouvrez la boîte de dialogue Exécuter à partir du menu **Start** de Windows.
2. Entrez WBEMtest et cliquez sur **Connect** dans la boîte de dialogue Testeur WMI.
3. Dans le champ **Connect**, entrez `\\<servername>\root\cimv2`.
4. Dans les champs **Credentials**, saisissez le nom d'utilisateur et le mot de passe employés pour se connecter à l'hôte d'application que vous surveillez.
5. Cliquez sur **Connect** pour revenir à la boîte de dialogue Testeur WMI. Cliquez sur **Query**.
6. Dans le champ **Enter Query**, entrez :

   ```
   select * from win32_processor
   ```

7. Cliquez sur **Apply**.

   Si WMI peut se connecter, les données de l'hôte d'application s'affichent.

Surveillance à distance d'un hôte Windows
Il est possible de collecter toutes les informations système à distance à partir d'un ordinateur Windows à l'exception des informations sur les adaptateurs HBA Fibre Channel. Pour surveiller un ordinateur Windows à distance, vous devez installer un agent sur un autre ordinateur Windows. Vous ne pouvez pas surveiller à distance un ordinateur Windows à partir d'un agent exécuté sur un ordinateur UNIX.

Pour surveiller un hôte Windows à partir d'un autre ordinateur Windows, le service d'agent de doit être exécuté en tant qu'administrateur sur l'ordinateur effectuant la surveillance. Modification des paramètres de connexion du service de l'agent à la page 203 fournit plus d'informations à ce sujet.

Modification des paramètres de connexion du service de l'agent
Si cela s'impose, procédez à une vérification. Pour modifier les paramètres de connexion du service de l'agent :

Procédure

1. Démarrez le gestionnaire de contrôle des services Windows : **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**).
2. Sélectionnez le service d'agent DPA.
3. Cliquez avec le bouton droit et sélectionnez **Properties** dans le menu.
4. Dans la boîte de dialogue **Properties**, sélectionnez l'onglet **Log On**.
5. Sélectionnez **This account**.
6. Saisissez le nom d'utilisateur et le mot de passe d'administrateur pour le service à exécuter.

7. Cliquez sur **OK** pour redémarrer le service.

Surveillance de l'activité d'un ordinateur distant

Procédure

1. Créez un objet hôte pour l'ordinateur à surveiller dans la console Web. Le nom de l'objet est le nom d'hôte de l'hôte distant. Le nom d'hôte doit pouvoir être résolu à partir de l'ordinateur sur lequel l'agent devant surveiller l'objet est exécuté.
2. Attribuez des demandes à cet objet pour spécifier les données à collecter.
3. Marquez chaque demande comme une demande proxy et saisissez les détails.
4. Pour compléter les détails de proxy, entrez le nom de l'hôte pour l'agent dans le champ **Proxy Host**.
5. Créez des données d'identification Windows pour le compte administrateur sur l'ordinateur en cours de surveillance. Ce compte peut porter le nom d'un administrateur local ou celui d'un administrateur de domaines.
6. Informez l'agent qui va surveiller le serveur des modifications en chargeant à nouveau l'agent.

Surveillance d'un hôte pour les données système

Surveillez un hôte d'application pour les données système à partir d'un agent s'exécutant sur l'hôte ou sur un autre hôte dans l'environnement.

Avant de démarrer le Discovery Wizard pour surveiller un hôte pour les données système

Les données du système peuvent uniquement être collectées à partir de systèmes UNIX par un agent local de l'hôte UNIX.

Configuration pour l'analyse de réplication

Utilisez l'assistant de découverte pour effectuer une analyse de réplication de stockage.

Avant de commencer

- Pour la configuration de la sauvegarde et de la restauration ProtectPoint, assurez-vous que vous disposez de la capacité de découverte d'applications ou que vous avez défini la balise de surveillance de réplication.
- Pour la configuration de la sauvegarde ProtectPoint, assurez-vous que vous synchronisez l'heure, à 1 minute près au maximum, de l'hôte qui est protégé par ProtectPoint avec l'hôte Solutions Enabler qui gère la baie de stockage vers laquelle l'application est mappée.
- Assurez-vous que la communication entre l'hôte surveillé et le traitement de la capacité de restauration est activée :
  - Pour la surveillance à distance des serveurs Windows, les services RPC doivent être activés et être accessibles pour l'agent de restauration.
  - Pour la surveillance à distance des applications UNIX/Linux, SSHD doit être activé et accessible pour l'agent de restauration.
  - Pour la surveillance à distance des applications UNIX/Linux, les services FTP/Telnet doivent être activés et accessibles pour l'agent de restauration.

Surveillance de Microsoft Exchange Server

Pour découvrir Microsoft Exchange Server, vous devez découvrir l'hôte sur lequel Microsoft Exchange Server s'exécute. Dans une optique de capacité de restauration,

un serveur Exchange peut être surveillé à partir d'un agent installé sur le même hôte que le serveur Exchange ou d'un agent installé à distance.

Remarque

Microsoft Exchange peut uniquement faire l'objet d'une surveillance pour une analyse de réplication et pour obtenir des informations sur le système depuis l'hôte du serveur Exchange.

Avant de démarrer le Discovery Wizard pour la surveillance de Microsoft Exchange Server
Le compte utilisé pour connecter DPA au serveur Exchange doit être un utilisateur de domaine disposant de droits d'administrateur en lecture seule et de droits d'administrateur local. DPA ne prend pas en charge l'analyse de réplication pour deux banques d'informations Exchange sur un cluster. Pour vous connecter à l'application Exchange, vous devez disposer de droits d'administrateur Exchange en lecture seule. Pour récupérer les informations des disques depuis Windows, vous devez être un utilisateur du système d'exploitation doté de droits d'administrateur local.

Surveillance d'Oracle pour l'analyse de la réplication
Pour surveiller une base de données Oracle en vue d'une analyse de réplication, l'agent doit se connecter à la base de données en tant qu'utilisateur Oracle en mesure d'effectuer des sélections sur les tables et les vues suivantes :

- DBA_DATA_FILES
- DBA_TEMP_FILES
- DBA_TABLESPACES
- V_$DATAFILE
- V_$LOGFILE
- V_$CONTROLFILE
- V_$LOG_HISTORY
- V_$ARCHIVED_LOG
- V_$INSTANCE
- V_$DATABASE
- V_$PARAMETER
- DICT
- DBA_TAB_COLUMNS

Lors de la surveillance d'Oracle sur une plate-forme Windows, l'utilisateur du système d'exploitation spécifié dans les informations d'identification doit appartenir au groupe ORA_DBA. Sous UNIX, si vous utilisez l'authentification UNIX, vous n'avez pas besoin de définir des informations d'identification dans la base de données.

Mise à jour des statistiques Oracle
Pour collecter des chiffres précis concernant le nombre de lignes et la taille des tables et index, il est important de mettre à jour régulièrement les statistiques Oracle. La documentation Oracle contient de plus amples détails sur la façon de configurer une tâche de mise à jour des statistiques Oracle.

Vous pouvez notamment exécuter la commande suivante pour mettre à jour les statistiques Oracle sur un schéma :

```
exec dbms_stats.gather_schema_stats(ownname => '***SCHEMANAME***',
estimate_percent => 5, cascade => true, options => 'GATHER');
```

Surveillance de RecoverPoint
Vous devez utiliser un agent installé à distance (le serveur DPA, par exemple) pour surveiller RecoverPoint.

Lors de la découverte de RecoverPoint, DPA prend en charge la découverte d'une seule IP de gestion. En outre, DPA prend en charge la surveillance de l'IP de gestion uniquement et pas de l'IP de RPA. Assurez-vous de surveiller l'IP de gestion et non l'IP de RPA.

Surveillance du stockage primaire

Cette section explique comment surveiller le stockage primaire.

DPA sépare le stockage primaire selon les catégories suivantes :

- Serveurs de fichiers
- Baies de stockage pour l'analyse de la réplication
- Serveurs de gestion de disques

Surveillance des serveurs de fichiers

Cette section explique comment surveiller les serveurs de fichiers.

Surveillance d'EMC File Storage

EMC File Storage doit être surveillé par un agent qui s'exécute sur un ordinateur distant, par exemple, le serveur DPA.

Remarque

EMC File Storage est aussi couramment appelé Celerra File Storage.

Configuration des baies de stockage pour l'analyse de la réplication

DPA surveille les baies de stockage VNX Block, CLARiiON, Symmetrix et VPLEX Si ces baies de stockage sont répliquées avec RecoverPoint, une configuration supplémentaire est requise pour activer l'analyse de réplication complète.

Port pour les baies EMC VPLEX
DPA se connecte au VPLEX sur le port TCP 443.

Découverte de baies VPLEX
Les baies de stockage VPLEX peuvent être surveillées à partir du serveur DPA, ou à distance à partir d'un hôte pour lequel l'agent DPA est installé.

DPA découvre toutes les baies de stockage gérées et crée des objets dans l'inventaire de la bibliothèque d'objets.

Port pour les baies VNX Block /CLARiiON
DPA se connecte à VNX Block/CLARiiON sur le port TCP 443. Toutefois, si VNX Block/CLARiiON est configuré pour utiliser le port 2163, utilisez le port 2163.

Découverte des baies VNXBlock/CLARiiON
Les baies de stockage VNXBlock/CLARiiON doivent être surveillées à distance à partir d'un serveur proxy ou, en dernier recours, à partir d'un agent s'exécutant sur un autre hôte, tel que le serveur DPA. On l'appelle également hôte SE ou Connector.

L'hôte SE peut être utilisé pour la découverte via un agent DPA, celui-ci étant installé sur l'hôte SE, ou via un mécanisme sans agent, ce qui oblige un utilisateur privilégié à saisir ses informations d'identification.

DPA découvre toutes les baies de stockage gérées et crée des objets dans l'inventaire de la bibliothèque d'objets.

Vous devrez fournir le nom de l'hôte sur lequel EMC Solutions Enabler est installé.

Découverte des baies Symmetrix
Les baies de stockage Symmetrix doivent être surveillées à distance à partir d'un agent s'exécutant sur un hôte différent (le serveur DPA, par exemple).

Pour configurer plusieurs hôtes et plusieurs baies de stockage, utilisez le Discovery Wizard. DPA découvre toutes les baies de stockage gérées et crée des objets dans l'inventaire de la bibliothèque d'objets.

Vous devez fournir le nom de l'hôte sur lequel Solutions Enabler est installé.

Afin que Solutions Enabler puisse voir les groupes de périphériques qui y sont stockés localement par défaut, vous devez ouvrir `Global Name Services` dans le fichier d'options de Solutions Enabler, en procédant comme suit :

1. Ouvrez le fichier d'options sous `/./emc/API/symapi/config/`
2. Trouvez la ligne

   ```
   #SYMAPI_USE_GNS = ENABLE
   ```

   et supprimez les remarques pour obtenir : **`SYMAPI_USE_GNS = ENABLE`**
3. Enregistrez le fichier.
4. Vérifiez que le service GNS est en cours d'exécution en exécutant la commande `stordaemon list`.
5. Exécutez la commande `symcfg disco`.

Exécution d'une découverte sans hôte sur Symmetrix et VNX/CLARiiON
La découverte de l'hôte au moyen d'une surveillance de la réplication nécessite l'installation d'un agent local sur l'hôte ou le déploiement d'un agent à distance avec des informations d'identification pour l'accès à l'hôte. L'une comme l'autre de ces méthodes peut être empêchée par les règles de sécurité du client.

Pour utiliser l'option sans agent, vous devez fournir les informations d'identification de l'hôte Solutions Enabler. Les conditions requises pour la découverte sans hôte sont les mêmes que celles qui sont décrites dans la section Découverte des baies Symmetrix à la page 207.

Configuration des baies de stockage qui utilisent RecoverPoint pour collecter les données de la réplication
Si vos baies de stockage VNX/CLARiiON ou Symmetrix sont répliquées avec EMC RecoverPoint, DPA fournit une analyse de la réplication pour les opérations de réplication RecoverPoint.

Afin d'effectuer une analyse de la réplication pour RecoverPoint, vous devez configurer les baies de stockage VNX/CLARiiON ou Symmetrix, ainsi que l'hôte RecoverPoint dans DPA, suivant l'ordre approprié.

Procédure

1. Utilisez le Discovery Wizard pour créer l'objet hôte pour l'hôte Solutions Enabler qui est connecté à la baie de stockage répliquée avec RecoverPoint.
2. Découvrez les baies rattachées à l'hôte.
3. Configurez les baies Symmetrix ou VNX/CLARiiON à l'aide du Discovery Wizard.
4. Importez les données de la règle de réplication à partir des baies de stockage.

5. Configurez la surveillance des données des dispositifs EMC RecoverPoint selon la procédure décrite dans la section Surveillance de RecoverPoint à la page 206.
6. Assurez-vous que la demande de configuration RecoverPoint a été attribuée à l'objet d'appliance RecoverPoint qui gère la réplication pour la baie de stockage. Exécutez cette demande.
7. Une fois que la demande de configuration RecoverPoint a été exécutée et après un délai suffisant, DPA doit avoir commencé à collecter les données d'analyse de la réplication pour RecoverPoint. Les rapports peuvent être exécutés à partir des objets de baie de stockage et la zone **Replication Analysis** affichera le mappage du stockage et des points de restauration.

Avant de démarrer le Discovery Wizard pour la surveillance d'EMC File Storage

Le module EMC File Storage collecte les informations d'EMC File Storage via une API XML et directement à partir de la Control Station d'EMC File Storage. Vous devez créer un administrateur doté de privilèges spécifiques sur EMC File Storage :

Procédure

1. Connectez-vous à l'interface du navigateur Web du gestionnaire d'EMC File Storage en tant qu'administrateur.

   Vous pouvez également utiliser l'interface de ligne de commande pour créer un administrateur DPA.
2. Accédez à **Security** > **Administrators**.
3. Créez un administrateur avec, par exemple, un nom d'utilisateur « DPA ».
4. Sélectionnez **Local Only Account**, puis saisissez et confirmez un mot de passe pour l'administrateur.
5. Sélectionnez un **Primary Group** de niveau de privilèges « opadmin » au minimum. DPA n'a pas besoin de privilèges plus élevés que ceux attribués par opadmin.
6. Activez les options d'accès du client suivantes :
   - XML API v2 allowed
   - Control Station shell allowed
7. Cliquez sur le bouton **OK**.

Résultats

Les informations d'identification DPA utilisées pour se connecter à EMC File Storage doivent contenir le nom d'utilisateur et le mot de passe de l'administrateur EMC File Storage que vous avez créé.

Surveillance des serveurs de gestion des disques

Cette section explique comment surveiller les serveurs de gestion des disques.

Surveillance de HP Command View.

Surveillez une baie de disques HP EVA à l'aide de HP Command View à partir d'un agent s'exécutant sur l'hôte Command View, ou à distance à partir d'un agent s'exécutant sur un autre hôte (tel que le serveur DPA).

Le nom d'utilisateur et le mot de passe employés pour la collecte de données doivent correspondre au nom d'utilisateur et au mot de passe définis sur le serveur

CommandView CIM. Vous pouvez les configurer à l'aide de l'interface de gestion CommandView.

DPA collecte les données auprès de HP Command View par SMI-S sur le port 5989 sécurisé par défaut.

Surveillance du stockage de protection

Cette section explique comment surveiller le stockage de protection.

Surveillance de Data Domain

DPA surveille les dispositifs de sauvegarde Data Domain. Pour DDOS 4.8, seules les informations de configuration et d'état des lecteurs de bande et des bibliothèques de bandes sont retournées. Vous devez activer la demande d'analyse de Data Domain sur les systèmes Data Domain sur lesquels vous souhaitez collecter les données.

Avant de démarrer le Discovery Wizard pour la surveillance de Data Domain

Le SNMP sur le port 161 et le SSH sur le port 22 doivent être activés sur l'appliance de sauvegarde Data Domain. Vous devez également définir la chaîne de communauté SNMP. Vous pouvez effectuer cette opération à partir de la ligne de commande.

Avant de commencer

- Assurez-vous de bien disposer des droits du rôle utilisateur pour exécuter les demandes SSH sur le système Data Domain.
- Assurez-vous que vous disposez des privilèges d'administrateur d'utilisateurs pour exécuter PCR (Physical Capacity Reporting) pour la surveillance de Data Domain OS 5.7 ou version ultérieure.

Procédure

1. Connectez-vous à la console du dispositif Data Domain à l'aide du compte sysadmin.
2. Saisissez la commande suivante pour vérifier la configuration existante :

   `snmp show ro-communities`

   `snmp add ro-community <string> hosts <host IP address>`
   Où *<string>* est la chaîne de communauté sélectionnée (par exemple, public) et *<host IP address>* est l'adresse IP de l'agent DPA que vous utilisez pour surveiller le système Data Domain. Vous devez désactiver SNMP puis le réactiver pour que la nouvelle chaîne soit prise en compte.

   ```
   snmp disable
   snmp enable
   ```

   Si vous n'utilisez pas de chaîne de communauté « publique », vous devez changer la chaîne de communauté utilisée dans les informations d'identification de Data Domain.

   Les paramètres SNMP peuvent également être définis via l'onglet **System Settings** de l'interface Data Domain Enterprise Manager.
3. Modifiez les informations d'identification SSH DPA de Data Domain pour spécifier un nom d'utilisateur et un mot de passe SSH configurés sur le périphérique Data Domain. Accédez à **Admin** > **System** > **Manage Credentials** dans la console Web DPA.

Obligatoire :

- Pour garantir la configuration de la collecte des données SSH RCP lors de la surveillance de Data Domain OS 5.7 ou version ultérieure.
  - Lors de l'exécution de la demande, il collecte les statistiques pour la période d'interrogation de la commande, puis il crée le planning de mesure de capacité physique sur le Data Domain. Le Data Domain recueille ensuite les statistiques. Les statistiques sont recueillies, collectées et envoyées au serveur DPA lorsque la demande suivante est exécutée. Par conséquent, la première fois que la demande s'exécute, aucune donnée n'est collectée sur les rapports ; les données sont collectées et signalées uniquement lors de la deuxième exécution de la demande. Pour plus d'informations, reportez-vous à la section Procédure qui suit l'installation de DPA à la page 65.
  - La période d'interrogation de la commande est arrondie à des journées entières. La valeur de la période d'interrogation de la commande sera définie à deux fois la valeur de la période d'interrogation, sous réserve que la période d'interrogation de la commande soit d'au moins deux jours. Par exemple, si la période d'interrogation est inférieure ou égale à 24 heures, DPA collecte les statistiques pendant deux jours. Si la période d'interrogation est définie sur 3 jours, le DPA collecte des statistiques pendant 6 jours.
- pour obtenir les informations de la LUN à partir de Data Domain, comme les informations sur les périphériques, les groupes de périphériques, les pools, les images statiques et les groupes d'accès pour la restauration et la sauvegarde de ProtectPoint SnapVX. Configuration de DPA pour la sauvegarde et la restauration de ProtectPoint SnapVX à la page 210 fournit des informations.

entre autres informations.

Configuration de DPA pour la sauvegarde et la restauration de ProtectPoint SnapVX

Vous devez configurer DPA pour associer les informations collectées sur l'hôte de l'environnement DPA aux informations collectées sur le VMAX3 de l'environnement DPA, et associer ensuite ces informations aux informations collectées sur le Data Domain de l'environnement DPA.

Avant de commencer

- Assurez-vous que vous synchronisez l'heure, à 1 minute près au maximum, de l'hôte qui est protégé par ProtectPoint avec l'hôte Solutions Enabler qui gère la baie de stockage vers laquelle l'application est mappée.
- *Guide de compatibilité de Data Protection Advisor* fournit des informations sur les versions prises en charge et les exigences du système d'exploitation pour :
  - ProtectPoint
  - Solutions Enabler
  - VMAX3
  - Data Domain

Procédure

1. Configurez l'hôte pour l'analyse de la réplication.

   Pour plus d'informations, reportez-vous à la section . Assurez-vous que vous pouvez utiliser l'application de découverte ou que vous avez paramétré la balise

de surveillance de la réplication. Cette opération est nécessaire pour configurer la sauvegarde et la restauration de ProtectPoint.

2. Découvrez l'hôte de VMAX3 et l'hôte SE.

   Pour plus d'informations, reportez-vous à la section Découverte des baies Symmetrix à la page 207.

3. Découvrez l'hôte Data Domain.

   Pour plus d'informations, reportez-vous à la section Surveillance de Data Domain à la page 209. Assurez-vous que vous fournissez bien les informations d'identification SSH à l'assistant de découverte Data Domain. Cette opération est nécessaire pour obtenir les informations de la LUN à partir de Data Domain, comme les informations sur les périphériques, les groupes de périphériques, les pools, les images statiques et les groupes d'accès.

À effectuer

Si vous le souhaitez, vous pouvez ajouter de nouvelles règles de protection à votre règle de protection des données afin que des alertes sur les points de restauration manquants Linked, StaticImage et SnapVX soient générées.

Surveillance de StorageTek ACSLS Manager

StorageTek ACSLS Manager ne peut pas être surveillé à distance. Un agent DPA doit être installé sur l'hôte ACSLS AIX ou ACSLS Solaris.

Avant de démarrer Discovery Wizard pour la surveillance de StorageTek ACSLS Manager

L'agent doit être installé et en cours d'exécution sur le serveur StorageTek ACSLS Manager à surveiller.

Une fois l'agent installé, vérifiez que la valeur ACS_HOME dans le fichier DPA.config correspond à l'emplacement d'installation d'ACSLS. Vérifiez que la valeur ACSDBDIR dans le fichier DPA.config correspond au chemin d'accès au dossier de base de données ACSLS (le chemin par défaut est export/home/ACSDB 1.0).

Surveillance de bibliothèques de bandes

DPA peut collecter des informations sur les bibliothèques de bandes et les lecteurs de ces bibliothèques de bandes. Si vous spécifiez un nom d'hôte, assurez-vous que le nom de la bibliothèque de bandes puisse être résolu à partir de l'hôte surveillant la bibliothèque de bandes.

Avant de démarrer le Discovery Wizard pour la surveillance des librairies de bandes

Les données d'identification de la librairie de bandes doivent contenir la chaîne de communauté en lecture seule pour la librairie de bandes dans le champ **Password** de la boîte de dialogue **Credential Properties**. Si la chaîne de communauté n'est pas modifiée pour la librairie de bandes, définissez-la sur **Public**.

Sélectionnez **Admin** > **System** > **Manage Credentials** pour modifier les informations d'identification de la librairie de bandes qui sont créées après l'utilisation du Discovery Wizard pour créer un objet de librairie de bandes.

Surveillance de la librairie de bandes IBM System Storage TS 3500

Utilisez l'interface Web Tape Library Specialist pour activer les demandes SNMP (Simple Network Management Protocol) pour la librairie de bandes IBM System Storage TS 3500. Pour activer les demandes SNMP :

Procédure

1. Entrez l'adresse IP Ethernet dans la ligne URL du navigateur.
2. Sélectionnez **Manage Access** > **SNMP Settings**. Dans le champ **SNMP Trap Setting**, affichez les paramètres actuels, puis cliquez pour activer les demandes SNMP.
3. Vérifiez que le champ **SNMP Requests Setting** est défini sur **Enabled**.

Surveillance de la librairie de bandes IBM TotalStorage 3583

Configurez la RMU (Remote Management Unit) pour activer le protocole SNMP pour la librairie de bandes IBM TotalStorage 3583. Pour activer le protocole SNMP :

Procédure

1. Dans la RMU, cliquez sur **Configuration**.
2. Dans la zone SNMP Configuration, effectuez les opérations suivantes :
   - Pour activer la fonction, sélectionnez **ON** dans le champ **SNMP Enabled**.
   - Pour activer ou désactiver les alertes SNMP, sélectionnez **ON** ou **OFF** dans le champ **Alerts Enabled**.
   - Dans le champ **Manager**, entrez l'adresse du serveur SNMP.
   - Dans le champ **Public Name**, entrez le nom de la communauté SNMP en lecture seule.
   - Dans le champ **Private Name**, entrez le nom de la communauté SNMP en lecture/écriture.
3. Cliquez sur **Submit** puis examinez les modifications.
4. Entrez le mot de passe, puis cliquez sur **Confirm**. Redirigez le navigateur si nécessaire.
5. Cliquez sur **Done** pour redémarrer.

Surveillance de la librairie de bandes IBM TotalStorage 3584

Pour activer le protocole SNMP depuis l'interface Web de la librairie de bandes IBM TotalStorage 3584 :

Procédure

1. Depuis l'écran Welcome de l'interface Web Tape Library Specialist, sélectionnez **Manage Access** > **SMNP Settings**.
2. Dans le champ **SNMP Trap Setting**, consultez les paramètres actuels, puis cliquez sur le bouton pour activer ou désactiver les demandes SNMP.
1. Vous pouvez également activer les demandes SNMP à partir du panneau de commande :
3. Sur l'écran Activity du panneau de commande de la librairie de bandes, sélectionnez **MENU** > **Settings** > **Network** > **SNMP** > **Enable/Disable SNMP Requests** > **ENTER**.

   L'écran indique l'état actuel des demandes SNMP.
4. Cliquez sur **UP** ou sur **DOWN** pour spécifier ENABLED ou DISABLED pour la messagerie SNMP, puis cliquez sur **ENTER**.

   Pour accepter le nouveau paramètre et revenir à l'écran précédent, cliquez sur **BACK**.

   L'écran Enable/Disable SNMP Requests indique les nouveaux paramètres.

Surveillance de l'autochargeur de bande Oracle SL24 et de la bibliothèque de bandes SL48

Configurez l'interface de gestion à distance (RMI) pour activer le protocole SNMP pour l'autochargeur de bande Oracle StorageTek SL24 ou pour la bibliothèque de bandes SL48. Pour activer le protocole SNMP :

Procédure

1. Dans la RMI, accédez à **Configuration** > **Network**.
2. Assurez-vous que la case **SNMP Enabled** est cochée.
3. La chaîne **Community Name** doit être contenue dans les informations d'identification utilisées pour se connecter à cette bibliothèque de bandes dans DPA.
4. Cliquez sur **Submit**, puis examinez les modifications.

Surveillance de la bibliothèque de bandes HP StorageWorks

Configurez l'utilitaire NeoCenter pour activer le SNMP pour la bibliothèque de bandes. Pour activer le protocole SNMP :

Procédure

1. Démarrez l'utilitaire NeoCenter depuis l'hôte.
2. Sélectionnez **Configure** dans le menu de l'écran principal. La boîte de dialogue **Configure** apparaît.
3. Cliquez sur l'onglet **SNMP Traps**.
4. Dans l'un des champs **Trap Address** disponibles, saisissez l'adresse IP du serveur DPA.

Surveillance des switches et périphériques d'E/S

Cette rubrique explique comment surveiller les switches et périphériques d'E/S.

Surveillance des switches Fibre Channel

DPA collecte les informations relatives aux ports (y compris la configuration, l'état de la connectivité et le débit) sur les switches Fibre Channel.

Lorsque vous spécifiez un nom d'hôte, assurez-vous que le nom du switch peut être résolu sur l'hôte de l'agent.

Avant de démarrer le Discovery Wizard pour la surveillance de switches Fibre Channel

Pour veiller à ce que les switches Brocade renvoient toutes les données, vérifiez que le Fibre Channel Alliance MIB est chargé et activé sur le switch. Il se peut que, par défaut, le MIB ne soit pas installé sur le switch. Pour activer la prise en charge FA-MIB sur des switches Brocade, connectez-vous en tant qu'administrateur et exécutez la commande snmpmibcapset. Définissez le paramètre FA-MIB sur Yes. Cliquez sur Enter pour accepter la valeur par défaut pour les autres paramètres.

En voici quelques exemples :

```
telnet <switch>
> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
 FE-MIB SW-MIB FA-MIB SW-TRAP FA-TRAP
```

```
 FA-MIB (yes, y, no, n): [yes]
 SW-TRAP (yes, y, no, n): [enter]
 FA-TRAP (yes, y, no, n): [enter]
 SW-EXTTRAP (yes, y, no, n): [enter]
>
```

Surveillance des switches IP

Lorsque vous spécifiez un nom d'hôte, assurez-vous que le nom du switch peut être résolu sur l'hôte de l'agent.

Avant de démarrer le Discovery Wizard pour la surveillance de switches IP

Les données d'identification de switch IP doivent contenir la chaîne de communauté SNMP pour le switch IP dans le champ **Password** de la boîte de dialogue **Credential Properties**. Si la chaîne de communauté n'a pas été modifiée pour le switch IP, définissez-la sur Public.

Sélectionnez **Admin** > **System** > **Manage Credentials** pour modifier les données d'identification du switch IP créées après avoir utilisé le Discovery Wizard pour créer un objet de switch IP.

Surveillance du directeur d'E/S Xsigo

Lorsque vous spécifiez un nom d'hôte pour le directeur d'E/S Xsigo, assurez-vous que le nom d'hôte ou l'adresse IP du directeur peut être résolu(e) sur l'hôte de l'agent.

Avant de démarrer le Discovery Wizard pour la surveillance du directeur d'E/S Xsigo

Les informations d'identification SNMP du directeur Xsigo doivent contenir la chaîne de communauté SNMP pour le directeur dans le champ **Password** de la boîte de dialogue Credential. Sauf si la chaîne de communauté a été modifiée sur le directeur, définissez-la sur public.

Sélectionnez **Admin** > **System** > **Manage Credentials** pour modifier les informations d'identification SNMP par défaut du directeur Xsigo si nécessaire, ou pour en créer de nouvelles.

Gestion de la virtualisation

Cette section explique comment surveiller un environnement virtualisé.

Surveillance de l'environnement VMware

Surveillez votre environnement VMware à partir d'un agent qui s'exécute sur le serveur VirtualCenter ou à distance à partir d'un agent qui s'exécute sur un hôte différent, comme le serveur DPA.

- Le Discovery Wizard peut être utilisé pour ajouter un serveur vCenter à DPA. Accédez à **Admin** > **System** > **Discovery Wizard** > **Virtualization Management** .
- Pour ajouter un serveur vCenter, vous devez fournir le nom d'hôte et les informations d'identification vCenter d'un utilisateur vCenter.
- Vous pouvez choisir de surveiller l'hôte vCenter seulement ou de surveiller également les machines virtuelles connectées à l'hôte vCenter.
  - Si vous choisissez de surveiller les machines virtuelles, DPA interroge le serveur vCenter et affiche une liste des machines virtuelles. Le processus de

découverte peut prendre un certain temps si le nombre de machines virtuelles configurées sur le serveur vCenter est important.

- Pour chaque machine virtuelle, vous pouvez choisir de découvrir l'hôte dans DPA. En découvrant l'hôte, vous l'ajoutez à l'inventaire DPA.
- Pour chaque machine virtuelle sélectionnée pour la découverte, vous pouvez choisir d'activer l'option Host System Monitoring qui permet de collecter des données de configuration, de performance et d'analyse, ou l'option Replication Monitoring qui permet une analyse de la réplication.
- Pour chaque machine virtuelle sélectionnée avec l'option Host System Monitoring, vous pouvez spécifier l'agent DPA à utiliser pour surveiller la machine virtuelle. Il est possible de modifier l'agent DPA pour plusieurs machines à la fois. Pour cela, il vous suffit de cliquer tout en maintenant la touche CTRL enfoncée ou de cliquer tout en maintenant la touche MAJ enfoncée pour sélectionner plusieurs systèmes.
  - Pour procéder à une surveillance du système hôte, les machines virtuelles Windows peuvent utiliser un agent DPA à distance, par exemple l'agent DPA installé sur le serveur DPA, ou encore un agent local, comme l'agent DPA installé sur chaque machine virtuelle Windows.
  - Pour procéder à une surveillance du système hôte, les machines virtuelles UNIX/Linux utilisent obligatoirement un agent DPA installé sur la machine virtuelle, sur un agent local.
- Si vous choisissez une surveillance de l'hôte pour chaque VM, vous devez fournir des informations d'identification Windows pour chaque machine virtuelle Windows surveillée avec un agent distant. Les informations d'identification peuvent appartenir à un administrateur local ou à un administrateur de domaine. Vous pouvez modifier les informations d'identification de plusieurs machines à la fois. Pour cela, il vous suffit de cliquer tout en maintenant la touche CTRL enfoncée ou de cliquer tout en maintenant la touche MAJ enfoncée pour sélectionner plusieurs systèmes. Vous ne devez pas fournir ces informations d'identification si vous surveillez le vCenter.
- Les machines virtuelles découvertes s'affichent sous l'objet vCenter dans DPA et sont également ajoutées par défaut au groupe Configuration / Servers / Application Servers. Vous pouvez apporter des changements et ajouter des groupes pour les machines virtuelles qui apparaissent. Accédez à **Admin** > **System** > **Discovery Wizard** > **Destination Group.**

- Le dernier écran du Discovery Wizard vCenter présente un récapitulatif des options sélectionnées. En cliquant sur **Finish**, vous ajoutez les objets à DPA et vous activez les options de surveillance sélectionnées.

Surveillance de RecoverPoint pour les VM

Vous devez utiliser un agent installé à distance (le serveur DPA, par exemple) pour surveiller RecoverPoint pour les VM. L'Agent DPA doit être exécuté sous Windows ou Linux.

Lors de la découverte de RecoverPoint pour les VM, DPA prend en charge la découverte d'une seule IP de gestion. En outre, DPA prend en charge la surveillance de l'IP de gestion uniquement et pas de l'IP de RPA. Assurez-vous de surveiller l'IP de gestion et non l'IP de RPA.

Avant de démarrer le Discovery Wizard pour la surveillance de RecoverPoint

DPA doit pouvoir se connecter à l'interface de ligne de commande (CLI) de l'environnement RecoverPoint via une connexion SSH sécurisée sur le port 22. DPA se

connecte à l'appliance RecoverPoint en utilisant le compte « admin » CLI par défaut, mais cette opération est possible pour tout utilisateur défini disposant des privilèges suffisants pour exécuter une commande CLI à distance via SSH ; le compte de surveillance suffit.

Toutefois, DPA ne doit pas se connecter avec l'utilisateur RecoverPoint « boxmgmt » car cet utilisateur est réservé au démarrage automatique du gestionnaire d'installation RecoverPoint.

Si vous exécutez RecoverPoint 4.1, lorsque l'utilisateur par défaut est « monitor », vous devez créer un nouvel utilisateur, car l'utilisateur par défaut spécifié dans DPA n'existe plus. Si vous ne créez pas de nouvel utilisateur après l'installation de RecoverPoint 4.1, la demande contenant les informations d'identification de RecoverPoint effectuée à partir de DPA échoue.

Surveillance des clusters

Cette section explique comment surveiller les clusters.

Surveillance du cluster de basculement Microsoft Server

Pour découvrir le cluster de basculement Microsoft Server, vous devez installer l'agent sur chaque ordinateur qui se trouve dans le cluster. Le document *Guide de compatibilité de Data Protection Advisor* fournit des informations concernant les versions prises en charge.

Vous devez découvrir le cluster de basculement Microsoft Server avec un agent à distance au sein du Discovery Wizard DPA. Cet agent doit être installé sur une machine du cluster. DPA propose deux options de découverte :

- **Monitor Cluster and hosts which are included in cluster** : si vous sélectionnez cette option, DPA sélectionne automatiquement le cluster avec les demandes Cluster Configuration et Cluster Status.
  DPA attribue les demandes Host Monitoring, Host Configuration et Host status à tous les hôtes inclus dans le cluster.
- **Monitor only Cluster** : si vous sélectionnez cette option, DPA sélectionne automatiquement le cluster avec les demandes Cluster Configuration et Cluster Status.

Remarque

Les hôtes qui sont inclus dans le cluster ne disposeront pas de demandes attribuées.

Surveillance de Veritas Cluster Server et Veritas Infoscale Availability

Pour découvrir Veritas Cluster Server et Veritas Infoscale Availability, vous devez installer l'agent sur chaque ordinateur qui se trouve dans le cluster. Le document *Guide de compatibilité de Data Protection Advisor* fournit des informations concernant les versions prises en charge.

Vous devez découvrir Veritas Cluster Server et Veritas Infoscale Availability avec un agent à distance au sein du Discovery Wizard DPA. Cet agent doit être installé sur une machine du cluster. DPA propose deux options de découverte :

- **Monitor Cluster and hosts which are included in cluster** : si vous sélectionnez cette option, DPA sélectionne automatiquement le cluster avec les demandes Cluster Configuration et Cluster Status.
  DPA attribue les demandes Host Monitoring, Host Configuration et Host status à tous les hôtes inclus dans le cluster.

- **Monitor only Cluster** : si vous sélectionnez cette option, DPA sélectionne automatiquement le cluster avec les demandes Cluster Configuration et Cluster Status.

Remarque

Les hôtes qui sont inclus dans le cluster ne disposeront pas de demandes attribuées.

Découverte d'un hôte ou d'un objet manuellement

Cette procédure ne s'applique pas lors de la découverte des baies CLARiiON, Symmetrix, VNX ou VPLEX.

Remarque

Les étapes affichées varient en fonction de l'objet que vous découvrez.

Procédure

1. Effectuez l'une des opérations suivantes :
   - Accédez à **Inventory** > **Object Search**.
   - Accédez à **Admin** > **Run Discovery Wizard**.
2. Dans **Objects to Discover**, sélectionnez une des options suivantes :
   - **Host**, puis sélectionnez l'hôte.
   - **Primary Storage**, puis sélectionnez stockage de fichiers ou VPLEX.
   - **Protection Storage**, puis sélectionnez Data Domain, Disk Library, NetApp NearStore ou bibliothèque de bandes.
   - **Switch**, puis sélectionnez le switch Fibre Channel, IP ou Xsigo.
3. Sélectionnez l'option pour découvrir l'hôte ou l'objet manuellement.
4. Identifiez l'hôte d'application par son hostname ou adresse IP, alias, système d'exploitation, informations d'identification, agent de collecte de données à distance ou ports. Si vous découvrez le stockage primaire, le stockage de protection ou les switch, passez à l'étape 8.
5. Sélectionnez **Host System Monitoring** ou **Replication Monitoring** pour chaque hôte que vous souhaitez découvrir. L'option de surveillance de la réplication est disponible uniquement si vous possédez une licence de capacité de stockage. Si vous ne sélectionnez pas d'option lors de la découverte, vous pouvez ajouter des demandes ultérieures avec des options.
6. Indiquez si un agent de collecte de données local ou distant collectera des données pour cette application. Si vous avez sélectionné **Host System Monitoring** et que votre hôte utilise Linux, UNIX ou d'autres plates-formes non Windows, sélectionnez agent de collecte de données local. Pour les agents de collecte des données à distance, sélectionnez l'hôte sur lequel l'agent est installé.

   Remarque

   Si vous aviez spécifié un agent de collecte de données pour RecoverPoint, RecoverPoint for VMs, ou VPLEX dans la zone **Viewing and editing Data Collection defaults**, l'agent est affiché ici par défaut.

Pour ajouter ou modifier un agent, spécifiez les champs décrits dans le tableau suivant.

Champ	Description
Hostname	Nom de l'hôte sur lequel l'agent de collecte de données est installé.
Nom d'affichage	Nom de l'hôte sur lequel l'agent de collecte de données est installé.
Système d'exploitation	Système d'exploitation de l'hôte sur lequel l'agent de collecte de données est installé.
Surveillance du système hôte	Sélectionnez cette option pour surveiller la configuration, les performances et l'état pour cet hôte.
Surveillance de la réplication	Sélectionnez cette option pour effectuer une analyse de réplication pour cet hôte.

7. Si vous avez sélectionné surveillance du système hôte et agent de collecte de données à distance ou sans agent, sélectionnez ou définissez le credential de l'hôte d'application.

   Remarque

   Si vous aviez spécifié un credential pour RecoverPoint, RecoverPoint for VMs, ou VPLEX dans la zone **Viewing and editing Data Collection defaults**, le credential est affiché ici par défaut.

8. (facultatif) Testez la connexion à l'objet. Si le test échoue à cause d'erreurs de l'hôte ou de credential, cliquez sur **Back** pour les résoudre, puis testez à nouveau.
9. (facultatif) Ajoutez l'objet à un ou plusieurs groupes. Appuyez sur **Ctrl** ou **Maj** et cliquez pour sélectionner plusieurs objets.
10. (facultatif) Si vous avez défini des attributs personnalisés, sélectionnez les attributs que vous souhaitez appliquer aux objets découverts. Créez des attributs dans **Admin** > **Manage Custom Attributes**.
11. Cliquez sur **Finish** pour démarrer la tâche de découverte, qui ajoute des objets à la librairie d'objets et aux groupes de destination sélectionnés.

À propos de la collecte de données de tâches après la découverte

Découvrez-en plus sur la collecte de données de tâches après avoir découvert certaines applications internes à DPA.

Les informations contenues dans cette section s'appliquent aux applications suivantes :

- NetWorker
- Avamar
- TSM
- HP Data Protector

- Commvault Simpana
- NetBackup
- ArcServ
- DB2
- SAP HANA
- RMAN
- MSSQL

En ce qui concerne les applications ci-dessus, notez les points suivants :

- Lorsqu'un nouveau serveur est découvert, DPA rassemble les données des tâches jusqu'à 14 jours antérieures si vous activez cette fonction.
- L'heure d'interrogation est actuellement fixée au jour suivant et les données seront collectées pour le lendemain lors de la prochaine demande de surveillance des tâches.
- Le temps d'interrogation actuel est avancé un jour à la fois à partir de 14 jours antérieurs. À chaque fois que la demande de surveillances des tâches s'exécute, les données du jour même sont collectées jusqu'à ce que deux semaines de données aient été collectées. La collecte de données reprend ensuite son fonctionnement normal.
- La valeur de temps d'interrogation par défaut est de 1 jour et est configurable par l'utilisateur dans la section d'options de demande de surveillances des tâches.
- Lors de la configuration de la collecte de données, la **fréquence** doit toujours être une valeur inférieure à **la période maximale des données recueillies par chaque demande**. Dans le cas contraire, la demande ne rattrape pas l'heure actuelle et elle prend davantage de retard à chaque exécution et ne collecte pas les données restantes.

Les Options de demande de collecte de données par module fournissent des informations supplémentaires.

Objets et groupes surveillés

Présentation des objets

DPA découvre les applications et les périphériques de votre environnement de protection de données et stocke ces entités logiques et physiques en tant qu'objets dans la bibliothèque d'objets. Les objets découverts sont regroupés dans les catégories suivantes dans la bibliothèque d'objets :

- Applications
- Hôtes
- Stockage
- Switches

Les règles suivantes s'appliquent aux objets :

- Deux objets ne peuvent pas avoir le même nom.
- Le nom d'un objet ne peut pas être identique à l'alias d'un autre objet.

La bibliothèque d'objets vous permet de visualiser les objets et leurs attributs.

Recherche d'objets

Vous pouvez rechercher des objets pour modifier les demandes de collecte des données de plusieurs objets simultanément.

Procédure

1. **Select Inventory** > **Object search**.
2. Saisissez les critères de recherche :
   - Dans le champ **Name**, saisissez le nom de l'objet. Par exemple, le nom d'hôte, le nom de l'application ou le nom du switch.
   - Dans le champ **Types**, sélectionnez le type d'objet. Vous pouvez choisir des types d'objet de niveau supérieur, tels que Host et Switch ; Backup Server, Backup Client, Backup Pool sous Backup Application ; tous les types d'objet d'application.
   - Dans le champ **Groups**, sélectionnez le groupe d'objets ou Smart Group.
   - Dans le champ **Groups**, sélectionnez **Not In** si vous souhaitez rechercher des objets qui ne sont pas inclus dans un groupe, y compris un Smart Group. Notez que **In** est sélectionné par défaut.
   - Dans le champ **Requests**, filtrez par demande. Si vous souhaitez rechercher par demandes non attribuées, sélectionnez **Not Assigned**. Notez que **Assigned** est sélectionné par défaut.
   - Dans le champ **Agent**, sélectionnez l'agent de collecte de données.
   - Dans le champ **Attributes**, sélectionnez l'attribut. Dans la boîte de dialogue **Select Attributes**, si vous souhaitez rechercher par attributs non attribués, sélectionnez **Not Assigned**. Notez que **Assigned** est sélectionné par défaut. Si vous sélectionnez Not Assigned, les colonnes Value et Clear sont désactivées.

   Notez ce qui suit concernant la recherche de client de sauvegarde, pool de sauvegarde sous Backup Application :
   - Les options de recherche **Requests** et **Agent** ne sont pas disponibles avec la recherche de clients et de pools de sauvegarde.
   - Les demandes et attributions de collecte de données ne sont pas disponibles dans les résultats des recherches de clients et de pools de sauvegarde.

   Les champs **Types** et **Groups** sont organisés de la même façon que dans l'arborescence de configuration de la portée du rapport. Si vous saisissez plusieurs critères de recherche, ils seront liés par AND.
3. Cliquez sur **Search**.

   La recherche affiche jusqu'à 500 résultats. Pour limiter le nombre de résultats à moins de 500, limitez vos critères de recherche.

Affichage d'objets

Sélectionnez **Inventory** > **Object Library**.

Affichage et modification d'attributs pour plusieurs objets

Utilisez cette procédure pour sélectionner plusieurs objets renvoyés par une recherche d'objets et pour afficher et modifier les attributs attribués à plusieurs objets en une seule opération.

Procédure

1. Recherchez les objets que vous souhaitez afficher ou dont vous souhaitez modifier les attributs.

   Recherche d'objets à la page 220 Pour plus d'informations, reportez-vous à la section .

2. Sélectionnez les objets renvoyés par la recherche et appuyez sur le bouton droit de la souris pour sélectionner **Set Attributes**.

   La fenêtre **Attributes – Multiple Objects** s'affiche.

3. Pour modifier les attributs des objets sélectionnés, cochez les cases en face de la colonne **Name**, puis cliquez sur **OK**.

Modification de la collecte des données pour les objets

Dans le cadre du processus de découverte, le DPA Discovery Wizard attribue des demandes de collecte des données directement à un objet lors de la création de l'objet. Pour modifier les demandes de collecte des données par défaut d'un objet donné :

Recherche d'objets à la page 220 fournit des informations supplémentaires sur la modification des demandes de collecte des données.

Procédure

1. Sélectionnez **Inventory** > **Object Library.**
2. **Sélectionnez un hôte, puis cliquez sur l'onglet** > **Data collection** > **.**
3. Cliquez sur **Propriétés**.
4. Sélectionnez une demande et cliquez sur **Edit**.

Résultats

Gestion des paramètres par défaut de collecte des données à la page 105 fournit des informations sur les demandes de collecte des données par défaut. L'ensemble *Aide en ligne de Data Protection Advisor* fournit des procédures permettant d'ajouter, de modifier et d'afficher les demandes de collecte des données.

Groupes

Un groupe est un ensemble d'objets. Par exemple, vous pouvez créer un groupe d'objets utilisés par une application. Ainsi, lorsque vous appliquez une règle à ce groupe, elle est appliquée à tous les objets qu'il contient.

Remarque

Un objet peut être membre de plusieurs groupes.

Groupe de configuration

Le groupe de configuration est créé par défaut. Il est créé avec une structure initiale qui regroupe l'environnement de protection des données dans des serveurs, des switches et du stockage. Tous les hôtes, périphériques et applications de protection des données découverts par le Discovery Wizard sont d'abord ajoutés au groupe de

configuration. Les objets supprimés du groupe de configuration ne sont pas supprimés. Les objets supprimés du groupe de configuration apparaissent sous Objects Not In Groups.

Création de groupes

Procédure

1. Accédez à **Inventory** > **Group Management**.
2. Dans l'inventaire d'objets, sélectionnez **Groups**, puis cliquez sur **Create Group**.
3. Saisissez le nom du nouveau groupe.
4. Dans l'inventaire d'objets, sélectionnez l'hôte ou le groupe d'hôtes que vous souhaitez inclure dans le groupe.
5. Copiez et collez les hôtes dans le groupe que vous avez créé.

   Assurez-vous de ne pas couper ou supprimer les hôtes de leur emplacement d'inventaire d'objets d'origine.

Attributs d'objets

Les attributs d'objets enrichissent les informations dont DPA dispose sur un objet. Une fois créé, un attribut personnalisé peut être activé pour les objets valides, selon les paramètres d'attribut personnalisé définis. De même, il est possible de lui attribuer une valeur.

Lors de la création ou de la modification d'un objet, les attributs sont filtrés pour être associés à un ou plusieurs types d'objet spécifique, et seulement aux objets dont un attribut existant correspond à une valeur donnée.

Par exemple, un attribut Asset Tag peut être créé pour représenter un identifiant de ressource pour les composants physiques d'un environnement d'exploitation (par exemple, des hôtes, des baies de stockage ou des switches). Il n'est pas nécessaire que l'attribut Asset Tag puisse être attribué à des composants logiques tels que des instances de base de données ou des processus.

Dans la définition de l'attribut, Asset Tag est configuré pour être associé à un sous-ensemble de types d'objet physique. Vous pouvez affiner la configuration de cet attribut de sorte qu'il soit associé uniquement à des types d'objet physique possédant un attribut Business Unit, par exemple.

Smart Groups

Les Smart Groups permettent aux utilisateurs disposant de privilèges d'administration de créer des groupes alimentés de façon dynamique avec les informations des résultats des rapports DPA. Un Smart Group exécute un rapport personnalisé, puis crée des objets en fonction des résultats de ce rapport.

Les Smart Groups présentent l'avantage de fournir des niveaux élevés de flexibilité. Les administrateurs peuvent configurer des Smart Groups pour créer dynamiquement des listes d'objets correspondant à des critères métier et techniques spécifiques.

Création de Smart Groups

Pour plus d'informations sur la création de Smart Groups, consultez le *Aide en ligne de Data Protection Advisor*. Pour plus d'informations, reportez-vous aux sections Smart Group multiniveau à la page 223 et Smart Groups à niveau unique à la page 224.

Procédure

1. Sélectionnez **Inventory** > **Group Management.**
2. Cliquez sur **Create Group**, puis sur **Create Smart Group**.
3. Spécifiez un nom pour le Smart Group dans le champ **Smart Group Name**.
4. Spécifiez le fuseau horaire du Smart Group.
5. Sélectionnez une option : **Single-level Smart Group** ou **Multilevel Smart Group** et cliquez sur **Configure Smart Group Level**.
6. Spécifiez le paramètre **Generation Frequency** :
   - Si vous souhaitez que DPA génère le Smart Group à une heure planifiée, sélectionnez le type de fréquence **Once a day at** ou **Schedule**.
   - Pour générer le Smart Group lors de sa création ou de sa modification, sélectionnez le type de fréquence **On demand**.
7. Renseignez les champs pour chaque objet de rapport sélectionné et cliquez sur **OK**.
8. Si vous voulez configurer le Smart Group pour stocker et générer des rapports sur les nœuds de contenu, définissez **Enable History** sur **On**.

   Par défaut, l'option **Enable History** est définie sur **Off**.
9. Cliquez sur l'une des options suivantes :
   - **Save and Run** si le type de fréquence de génération est défini sur **Once a day at** ou **Schedule**.
   - **OK** si le type de fréquence de génération est défini sur **On demand**.

Smart Group multiniveau

À la différence d'un Smart Group à niveau unique, qui affiche uniquement 1 niveau d'objets enfants en fonction du Smart Group, le Smart Group multiniveau peut créer plusieurs niveaux d'objets enfants à partir d'un seul Smart Group. Cela vous permet également de configurer les champs que vous souhaitez utiliser en fonction des niveaux et les types d'objet que vous souhaitez créer. Vous pouvez créer un nombre illimité de niveaux. Si vous le souhaitez, vous pouvez bénéficier d'un mappage complet de votre environnement DPA en utilisant les Smart Groups multiniveaux.

Par exemple, un rapport utilisé dans le Smart Group affichant les données du tableau suivant peut être configuré, pour afficher la configuration d'objet présentée dans l'illustration ci-dessous, lors de l'exécution.

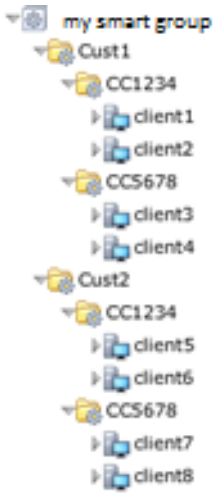
Tableau 37 Exemple de Smart Group multiniveau

Client	Centre de coûts	Client
Cust1	CC1234	Client1
Cust1	CC1234	Client2
Cust1	CC5678	Client3
Cust1	CC5678	Client4
Cust2	CC1234	Client5
Cust2	CC1234	Client6
Cust2	CC5678	Client7

Tableau 37 Exemple de Smart Group multiniveau (suite)

Client	Centre de coûts	Client
Cust2	CC5678	Client8

Figure 4 Exemple de configuration d'une bibliothèque d'objets d'un Smart Group multiniveau



Vous pouvez attribuer des stratégies de refacturation et des règles de protection des données au Smart Group ou aux objets enfants affichés, et visualiser la date de la dernière actualisation ou de la dernière génération de la structure. Par défaut, les générations Smart Groups sont quotidiennes. De plus, étant donné que les groupes hiérarchiques peuvent être intégrés avec des sources de données externes, vous pouvez créer une seule hiérarchie de Smart Groups afin de créer une structure d'objets qui existe déjà dans un système externe ou une base de données.

Seuls les utilisateurs disposant d'autorisations pour voir le Smart Group peuvent le voir, le développer, et exécuter des rapports sur celui-ci.

Smart Groups à niveau unique

Un Smart Group à niveau unique créé un ensemble d'objets à partir d'un rapport contenu dans un seul niveau de hiérarchie. Vous pouvez lui attribuer les mêmes éléments qu'aux objets standards, y compris les analyses et rapports planifiés. DPA peut alors générer des alertes et des rapports pour un Smart Group qui produit des objets.

Par exemple, une institution financière peut utiliser une convention selon laquelle les deux premiers caractères de chaque client de sauvegarde indiquent l'entité à laquelle ils sont attribués. Si les deux premiers caractères sont a et m, le client de sauvegarde appartient au groupe Asset management. En raison de la nature des activités, un grand nombre de clients sont créés, renommés ou supprimés quotidiennement. Au lieu de perdre du temps à mettre à jour la configuration du groupe chaque jour, l'administrateur DPA peut créer un Smart Group utilisant le rapport Backup Client Configuration existant pour répertorier chaque client de sauvegarde. Dans le Smart Group, il peut filtrer les résultats pour récupérer uniquement les clients qui commencent par a et m.

Comme DPA met à jour automatiquement la liste des configurations de clients chaque fois qu'il obtient des données du serveur de sauvegarde, cette liste est actualisée avec toutes les modifications effectuées dans l'environnement de sauvegarde.

Voici d'autres exemples :

- tous les clients de sauvegarde qui contiennent exch ;
- tous les hôtes disposant d'un lecteur E ;
- tous les objets ayant connu des alertes de gravité 1 au cours du dernier jour écoulé.

Historique Smart Group

L'historique Smart Group permet de stocker et de générer tous les rapports sur les nœuds de contenu.

Le paramètre Smart Group History vous permet de générer des rapports sur les modifications des Smart Groups, afin que les fournisseurs de services puissent proposer des facturations historiques précises.

Si le paramètre Enable History est activé, chaque fois que le Smart Group est généré par la suite, l'historique est consigné. Si ce paramètre est désactivé, tout l'historique est supprimé et seul l'état actuel est consigné lorsque le Smart Group est actualisé. Par défaut, le paramètre Enable History est défini sur **Off**.

Collecte des données de sauvegarde historiques à l'aide de la console Web DPA

Vous pouvez collecter les données de sauvegarde historiques sur Avamar, BackupExec, DB2, HP DataProtector, NetWorker, NetBackup, Oracle RMAN, SAP HANA et TSM.

Lorsque vous collectez les données de sauvegarde historiques à l'aide de la console Web DPA, tenez compte des points suivants :

- Vous ne pouvez pas collecter les données de sauvegarde historiques au niveau de l'hôte. Vous devez descendre d'un niveau dans l'arborescence de configuration, à l'objet d'application. Par exemple, pour collecter les données historiques à partir de NetWorker, vous devez choisir l'objet d'application Networker sous l'objet de niveau hôte.
- Vous pouvez uniquement collecter des sauvegardes historiques à partir de demandes JobMonitor.

Procédure

1. Dans la console Web, sélectionnez **Inventory** > **Group Management**.
2. Dans l'arborescence de configuration, sélectionnez l'objet d'application pour lequel vous souhaitez collecter des données de sauvegarde historiques.

   La fenêtre **Details** de l'objet d'application s'ouvre.
3. Dans la fenêtre des détails de l'hôte, sélectionnez l'onglet **Data Collection**.
4. Dans le champ **Data Collection**, sélectionnez JobMonitor request.
5. Cliquez avec le bouton droit de la souris sur **Run** et sélectionnez **Gather historical data**.
6. Dans la fenêtre **Gather historical data**, cliquez sur **OK**.

   Les mêmes options de données et d'informations d'identification sont disponibles que pour la demande elle-même.
7. Cliquez sur **Close** sur la boîte de dialogue qui s'affiche pour confirmer que DPA collecte les données de sauvegarde historiques.

8. Cliquez sur **History** pour afficher les tests collectés. Les lignes mises en surbrillance orange indiquent les résultats d'une collecte de sauvegardes historiques.

Configuration des stratégies, des règles et des alertes

Présentation des politiques et des alertes

DPA contient des politiques et des règles personnalisables qui contrôlent la façon dont DPA génère des alertes, mesure les performances de sauvegarde et de réplication, et détermine les valeurs du reporting de refacturation.

Stratégies

Les politiques DPA sont des données utilisateur concernant la façon dont la sauvegarde et la réplication doivent fonctionner dans l'environnement (politiques de capacité de restauration et de protection des données) ou sur le coût des opérations de stockage et de protection des données (politiques de refacturation).

Les rapports de capacité de restauration, de sauvegarde et de gestion des niveaux de service indiquent la façon dont les opérations exécutées dans l'environnement sont comparées aux paramètres des politiques : écarts dans la chaîne de restauration pour une baie de stockage ou objectif d'un point de restauration non atteint par un serveur de sauvegarde, par exemple.

DPA fournit les types de politique suivants :

- Politiques d'analyse : une ou plusieurs règles principalement utilisées pour générer des alertes. Les alertes s'affichent par défaut dans la section **Alerts**. Vous pouvez modifier la politique pour envoyer des événements aux e-mails, aux scripts, aux traps SNMP ou aux logs d'événements Windows. Pour plus d'informations, reportez-vous à la section Stratégies et génération d'événements à la page 257.
- Politiques de protection : ensemble de données utilisateur concernant le fonctionnement de la sauvegarde et de la réplication dans l'environnement. Ces politiques sont constituées de règles de capacité de restauration et de protection. Elles sont principalement utilisées pour générer des alertes. Les alertes s'affichent par défaut dans la section **Alerts**.
- Politiques de refacturation : utilisées pour déterminer le coût des opérations de stockage et de protection des données des rapports de refacturation.

Par défaut, les politiques d'analyse, de protection et de refacturation sont désactivées pour tous les objets et les groupes.

Politiques d'analyse

Une politique d'analyse consiste en une ou plusieurs règles attribuées à un objet ou un groupe. Les règles contiennent la logique permettant de déterminer le moment où une alerte doit être émise. Le moteur d'analyse compare les données surveillées aux conditions d'une règle et déclenche des alertes lorsqu'une règle concorde. Les règles basées sur des événements déclenchent une alerte en réponse aux données lues par le serveur DPA. Les règles planifiées comparent régulièrement les données du datastore DPA à des règles pour détecter une correspondance. Les alertes peuvent contenir des informations textuelles dynamiques et comporter des liens vers des rapports. Seules les politiques d'analyse peuvent générer des alertes.

Modèle de règle d'analyse

Un modèle de règle d'analyse est un ensemble d'instructions définissant la logique de la règle. Lorsqu'un modèle de règle est ajouté à une politique d'analyse, le moteur d'analyse effectue certaines opérations, puis affiche les événements résultants dans la section **Alerts** de la console Web.

Un modèle de règle se compose du nom de la règle, ainsi que des détails qui précisent comment cette règle est exécutée.

Par exemple, un modèle de règle peut être créé pour surveiller si un système de fichiers risque de dépasser 90 % de taux d'utilisation dans l'heure suivante.

Une règle d'analyse contient plusieurs règles qui s'appliquent à différents types d'objet. Le moteur d'analyse exécute uniquement les règles applicables à un objet donné. Par exemple, si l'objet est un switch, le moteur d'analyse exécute uniquement les règles de la politique qui s'appliquent aux switches.

Règles basées sur des événements ou règles planifiées

Les règles basées sur des événements fonctionnent en réponse aux données diffusées en continu et en temps réel dans le serveur DPA et déclenchent des alertes. Il existe cinq types de conditions pour les règles basées sur des événements :

- Filtre de condition : déclencher une alerte pour une condition définie ; par exemple, échec d'une sauvegarde. Le filtre de la condition est la condition la plus courante pour les règles basées sur des événements.
- Absence d'événement : déclencher une alerte si un événement ne se produit pas pendant la période définie ; par exemple, l'agent est désactivé.
- Prévision : déclencher une alerte si un événement se produit pendant une période définie ; par exemple, le système de fichiers se remplit.
- Modification de la configuration : déclencher une alerte en cas de modification de votre configuration ; par exemple, changement de l'état actif ou inactif, de la version, du type de système d'exploitation, de champs spécifiques, d'augmentation ou de diminution d'un certain pourcentage.
- Modification d'inventaire : déclencher une alerte s'il existe un nouveau type de nœud créé automatiquement ; par exemple, de nouvelles instances RMAN.

Les règle planifiées s'exécutent régulièrement et vérifient si une alerte doit être générée. Selon le type de planning que vous avez défini pour collecter les données, les alertes peuvent être envoyées des heures après que le problème ait été détecté sur le serveur DPA.

Pour les règles planifiées et les règles basées sur des événements, vous devez créer une stratégie qui contient une règle, appliquer la stratégie à un groupe de nœuds applicables, et vous assurer que les nouvelles données reçues pour les nœuds auxquels la stratégie s'applique contiennent des entités qui remplissent les conditions des règles. La console Web DPA fournit un éditeur de règle riche qui vous permet de créer, de modifier et de personnaliser les règles planifiées ainsi que celles basées sur des événements, selon vos besoins. Pour plus d'informations, reportez-vous à la section Création d'une règle d'analyse à la page 228.

Instructions pour les composants de règles d'analyse

Tenez compte des principaux composants suivants lorsque vous créez des règles d'analyse : la catégorie de la règle pour laquelle vous définissez l'alerte, le type d'objet que vous souhaitez surveiller et pour lequel vous créez l'alerte, et les attributs de l'objet sur lequel vous déclenchez des alertes.

DPA contient un solide référentiel de modèles de règle d'analyse règles système. Avant de créer une règle d'analyse personnalisée, vérifiez qu'il n'en existe pas une adaptée à vos besoins. Accédez à **Policies** > **Analysis Policies** > **System Rule Templates**. Si vous sélectionnez un modèle de règle système et que vous le modifiez, DPA efface les personnalisations utilisées pour créer la stratégie, ce qui signifie que vous ne voyez pas la façon dont DPA génère la règle.

Catégorie de règle d'analyse
Les catégories sont un moyen pour DPA de stocker les règles d'analyse. Elles constituent également un moyen pour filtrer et rechercher les règles d'analyse que vous avez créées. Il n'existe aucune règle absolue quant au choix d'une catégorie pour les règles d'analyse que vous créez. Si vous créez une règle d'analyse personnalisée, sélectionnez dans le menu déroulant une catégorie qui vous permet de bien mémoriser ou de trouver la règle que vous définissez. Le *Aide en ligne de Data Protection Advisor* fournit des informations sur les catégories de politiques d'analyse.

Type d'objet et attributs
Le type d'objet et les attributs que vous sélectionnez dépendent du scénario sur lequel vous souhaitez déclencher l'alerte ; par exemple, les objets que vous surveillez et les données collectées à leur sujet. Si vous avez besoin d'aide avec les données collectées sur les objets que DPA surveille, le *Guide de référence pour la collecte des données de Data Protection Advisor* fournit des informations sur les objets et les attributs, où les noms de table au sein de chaque fonction de module correspondent à un objet, et les noms de champ au sein de chaque table correspondent à un attribut. Dans le type d'objet et le déclencheur d'alerte, vous pouvez configurer et filtrer davantage ces informations pour la règle.

Création d'une règle d'analyse

Utilisez l'éditeur de règle DPA pour créer un modèle de règle d'analyse. Vous trouverez ci-dessous un aperçu général du processus. *Aide en ligne de Data Protection Advisor* fournit des instructions détaillées sur la création, la modification ou la copie d'un modèle de règle d'analyse.

Il s'agit d'une procédure générale pour créer une règle d'analyse. Des exemples spécifiques pour les règles d'analyse planifiées et basées sur des événements suivent.

Procédure

1. Dans la console Web DPA, accédez à **Policies** > **Analysis Policies** > **Rules Templates**.
2. Cliquez sur **Create Rule Template**.

   L'éditeur de règle s'affiche.
3. Indiquez un nom et une description pour l'alerte déclenchée par cette règle.
4. Sélectionnez une catégorie associée à la règle.

   Aide en ligne de Data Protection Advisor fournit des informations sur les catégories et les descriptions de règles.
5. Indiquez s'il s'agit d'une règle basée sur des événements ou d'une règle planifiée.

   Les règles basées sur des événements déclenchent une alerte en réponse aux données lues par le serveur DPA. Une règle planifiée s'exécute régulièrement et vérifie si une alerte doit être générée.

   Si la règle est une règle planifiée, définissez les **valeurs par défaut des paramètres de rapport**.

6. Sélectionnez les types d'objet appropriés :
   - par hiérarchie
   - par fonction
7. Indiquez quand et comment l'alerte doit être déclenchée.

   Notez que DPA ne prend pas en charge l'option pour tester le déclenchement `Lack of event` pour `Number of samples`, même si l'option s'affiche toujours comme valide dans la console Web DPA. DPA prend en charge l'option `Number of samples` pour `Time window`.

Création de règles basées sur des événements pour un filtre de condition

Les règles basées sur des événements fonctionnent en réponse aux données diffusées en continu et en temps réel dans le serveur DPA et déclenchent des alertes pour une condition définie ; par exemple, en cas d'échec de la sauvegarde. La condition de filtre est la condition la plus courante pour les règles basées sur des événements.

La procédure ci-dessous est consacrée à la création d'une règle pour déclencher une alerte pour une sauvegarde ayant échoué.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle en rapport avec la condition que vous définissez pour la règle.

   Par exemple, **`échec de la sauvegarde`**

   Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.

   Une règle de modèle système appelée Backup Failed existe. Vous pouvez la modifier si vous le souhaitez. Cet exemple montre comment le créer intégralement.
3. Dans le champ **Category**, dans le menu déroulant, sélectionnez la catégorie appropriée la plus adaptée à la règle que vous mettez en place.

   Par exemple, **Data Protection**.

   Dans ce cas, Data Protection est la catégorie la plus appropriée parce que vous souhaitez des alertes pour les données qui ne sont pas protégées.
4. Configurer le type d'objet. Dans cet exemple, nous voulons des alertes sur les sauvegardes qui ont échoué sur chaque client de sauvegarde. Nous allons donc sélectionner l'objet Backupjob.
   a. Dans **Object Type**, cliquez sur **Select**.

      La fenêtre **Select Object Types** s'ouvre.

   b. Développez Backup Applications, développez l'objet BackupClient, puis sélectionnez **Backupjob** dans la liste **Select Object Type** et cliquez sur **Select Object Type**.

      Vous pouvez utiliser la fonction de filtrage pour trouver facilement l'objet depuis lequel vous souhaitez surveiller.

      Le type d'objet que vous sélectionnez varie selon le scénario à partir duquel vous souhaitez déclencher l'alerte.

5. Configurez le déclenchement d'alertes. Dans cet exemple, nous voulons examiner uniquement les tâches en échec. Par conséquent, nous sélectionnons le déclencheur et définissons des filtres de condition pour trouver uniquement les tâches ayant échoué :
   a. Dans **Alert Trigger**, cliquez sur **Select**.

      La fenêtre **Select Alert Trigger** s'ouvre.

   b. Sélectionnez le bouton radio **Conditions Filter**, puis cliquez sur **Select and Edit Filter**.

      La fenêtre **Edit Filter** s'ouvre.

   c. Cliquez sur **Select Attribute**.

      La fenêtre **Select Attribute** s'ouvre.

   d. Assurez-vous que le bouton radio **Attribute** est sélectionné, puis cliquez sur **Browse**.

      La fenêtre **Browse Attributes** s'ouvre.

   e. Dans Backupjob Category, sélectionnez la ligne avec le paramètre AttributeName **Status**, cliquez sur **Select Attribute**, puis cliquez sur **OK**.

      Vous pouvez utiliser la fonction de filtre pour trouver facilement la catégorie et le paramètre Attributename souhaités.

   f. Cliquez sur **Select Operator** et définissez une valeur de **Is**, puis cliquez sur **OK**.

   g. Cliquez sur **Select Value**, sélectionnez le bouton radio **Static Value**, sélectionnez la valeur **failed** dans la liste déroulante, puis cliquez sur **OK**.

   h. Cliquez sur **OK** dans la fenêtre **Select Attribute**, puis cliquez sur **OK** dans la fenêtre **Edit Filter**.

   Le scénario pour lequel vous configurez l'alerte a une incidence sur sa configuration et, le cas échéant, sur la manière dont vous déclenchez l'alerte règle.

6. Configurer l'alerte :
   a. Dans **Alert**, cliquez sur **Select**.

      La fenêtre **Edit Alert** s'ouvre.

   b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.

   c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

   d. Dans l'onglet Associated Reports, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez générer lors de l'alerte.

7. Cliquez sur une des options d'enregistrement.

Création de règles basées sur des événements pour un changement de configuration

Les règles basées sur des événements fonctionnent en réponse aux données diffusées en continu et en temps réel dans le serveur DPA et déclenchent des alertes pour tout type de modification de la configuration. Par exemple, les changements d'état actif ou inactif, de version, de type de système d'exploitation, de champs spécifiques,

l'augmentation ou la diminution d'un certain pourcentage d'une mesure que DPA surveille.

Cette procédure est consacrée au changement d'état du client, d'actif à inactif.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle adapté au changement de configuration pour lequel vous déclenchez l'alerte.

   Par exemple, `état actif du client modifié`

   Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.
3. Dans le champ **Category**, sélectionnez **Change Management** dans la liste déroulante.
4. Configurer le type d'objet :
   a. Dans **Object Type**, cliquez sur **Select**.

      La fenêtre **Select Object Types** s'ouvre.

   b. Développez Backup Applications, puis sélectionnez **Backup Client** à partir de la liste **Select Object Type** et cliquez sur **Select Object Type**.
5. Configurer le déclencheur d'alertes. Dans cet exemple, nous voulons indiquer n'importe quel client qui est passé d'actif à inactif. Nous allons donc sélectionner le déclencheur approprié.
   a. Dans **Alert Trigger**, cliquez sur **Select**.

      La fenêtre **Select Alert Trigger** s'ouvre.

   b. Sélectionnez le bouton radio **Change Control**, puis cliquez sur **Select and Edit Filter**.

      La fenêtre **Edit Alert Trigger - Change Control** s'ouvre.

   c. Sélectionnez **ClientConfig** dans la liste déroulante.

   d. Cochez la case en regard de **Active**, puis cliquez sur **OK**.

      Notez que cette configuration de la règle génère une alerte pour toutes les modifications dans ce champ, pas uniquement pour un changement d'état actif à inactif.

   Aucun filtre de condition n'est nécessaire parce que nous voulons examiner le changement de configuration sur tous les clients.
6. Configurer l'alerte :
   a. Dans **Alert**, cliquez sur **Select**.

      La fenêtre **Edit Alert** s'ouvre.

   b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.

   c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

   d. Dans l'onglet Associated Reports, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez générer lors de l'alerte.

7. Cliquez sur une des options d'enregistrement.

Création de règles basées sur des événements pour l'absence d'événement

Les règles basées sur des événements fonctionnent en réponse aux données lues par le serveur DPA en temps réel qui déclenchent une alerte si un événement n'a pas lieu pour la période définie ; par exemple, l'agent est arrêté.

La procédure est consacrée à la création d'une règle pour générer une alerte lorsque l'agent de production est arrêté et continuer à générer l'alerte à chaque heure, si l'agent de production est encore arrêté.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle adapté à l'absence d'événement pour lequel vous définissez la règle.

   Par exemple, `arrêt de l'agent DPA`

   Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.
3. Dans le champ **Category**, sélectionnez dans le menu déroulant la catégorie appropriée la plus adaptée à la règle que vous mettez en place.

   Par exemple, **administratif**.
4. Configurer le type d'objet. Dans cet exemple, nous voulons générer une alerte lorsque des agents se sont arrêtés. Par conséquent, nous allons sélectionner le AgentStatus.
   a. Dans **Object Type**, cliquez sur **Select**.

      La fenêtre **Select Object Types** s'ouvre.
   b. Développez l'objet Host, puis sélectionnez **AgentStatus** dans la liste **Select Object Type** et cliquez sur **Select Object Type**.

      Vous pouvez utiliser la fonction de filtrage pour trouver facilement l'objet que vous souhaitez surveiller.

      Le type d'objet que vous sélectionnez varie selon le scénario à partir duquel vous souhaitez déclencher l'alerte.
5. Configurer le déclencheur d'alertes. Dans cet exemple, nous voulons examiner uniquement les agents de production qui se sont arrêtés. Par conséquent, nous allons sélectionner le déclencheur et définir les filtres de condition afin de rechercher uniquement les agents arrêtés :
   a. Dans **Alert Trigger**, cliquez sur **Select**.

      La fenêtre **Select Alert Trigger** s'ouvre.
   b. Cliquez sur le bouton radio **Event/Data Collection Did Not Occurr**, puis cliquez sur **Select and Edit Alert Trigger**.

      La fenêtre **Edit Alert Trigger** s'ouvre.
   c. Pour l'option 1, sélectionnez les éléments à surveiller, sélectionnez les boutons radio pour **Event did not occur** et **AgentStatus**.
   d. Pour l'option 2, cliquez sur le bouton radio en regard de **Keep Generating**.

e. Pour l'option 3, si vous souhaitez spécifier un type de nom d'hôte avec une convention de dénomination, par exemple, *prod* en mode production, cliquez sur le bouton radio **Edit Conditions Filter**, puis cliquez sur**Select Attribute**.

f. Assurez-vous que le bouton radio **Attribute** est sélectionné pour le champ **Value Type**, puis cliquez sur **Browse** pour le champ **Attribute**.

g. Dans **Browse Attributes**, sélectionnez l'attribut **name**, puis cliquez sur **OK**.

h. Cliquez sur **Select Operator** et définissez une valeur de **Contains**, puis cliquez sur **OK**.

i. Cliquez sur **Select Value**, sélectionnez le bouton radio **Static Value**, dans le champ **Value** saisissez `prod`, puis cliquez sur **OK**.

j. Cliquez sur **OK** dans la fenêtre **Edit Filter**.

k. Pour l'option 4, cliquez sur le bouton radio en regard de **Time Period** et sélectionnez **Static Value** dans la liste déroulante, sélectionnez **1** dans la liste déroulante des nombres et **hours** dans la liste déroulante de la période de temps, puis cliquez sur **OK**.

Le scénario pour lequel vous configurez l'alerte a une incidence sur la configuration et, le cas échéant, sur la manière dont vous filtrez davantage de déclencheur d'alerte de règle.

6. Configurer l'alerte :

a. Dans **Alert**, cliquez sur **Select**.

La fenêtre **Edit Alert** s'ouvre.

b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.

c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

d. Dans l'onglet Associated Reports, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez générer lors de l'alerte.

7. Cliquez sur une des options d'enregistrement.

Création de règles basées sur des événements pour la modification de l'inventaire

Les règles basées sur des événements fonctionnent en réponse aux données diffusées en continu et en temps réel dans le serveur DPA et déclenchent des alertes si un nouveau type de nœud est créé automatiquement.

La procédure est consacrée à la création d'une règle pour générer une alerte lorsqu'une instance de client de sauvegarde RMAN est créée automatiquement.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle adapté à la condition que vous définissez pour la règle.

   Par exemple, `nouvelle base de données RMAN sauvegardée dans le catalogue de restauration centralisé`

   Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.

3. Dans le champ **Category**, sélectionnez dans le menu déroulant la catégorie appropriée la plus adaptée à la règle que vous mettez en place.

   Par exemple, **Configuration**.

4. Configurer le type d'objet. Dans cet exemple, nous voulons créer des alertes sur les nouvelles instances de client de sauvegarde RMAN. Nous allons sélectionner l'objet OracleRMANBackupclient.

   a. Dans **Object Type**, cliquez sur **Select**.

      La fenêtre **Select Object Types** s'ouvre.

   b. Développez l'hôte, développez les Applications et les bases de données, développez l'Application Oracle puis sélectionnez **OracleRMANBackupclient** dans la liste **Select Object Type** et cliquez sur **Select Object Type**.

      Vous pouvez utiliser la fonction de filtrage pour trouver facilement l'objet que vous souhaitez surveiller.

      Le type d'objet que vous sélectionnez varie selon le scénario à partir duquel vous souhaitez déclencher l'alerte.

5. Configurer le déclenchement d'alertes. Dans cet exemple, nous voulons examiner uniquement les objets nouvellement créés. Par conséquent, nous sélectionnons le déclencheur et définissons des filtres de condition pour trouver uniquement les modifications de l'inventaire :

   a. Dans **Alert Trigger**, cliquez sur **Select**.

      La fenêtre **Select Alert Trigger** s'ouvre.

   b. Sélectionnez le bouton radio **Inventory Changes**, puis cliquez sur **Select and Edit Filter**.

      La fenêtre **Edit Alert Trigger - inventory Change** s'ouvre.

   c. Dans l'option 1 **Select operations to monitor**, assurez-vous que **Created** est sélectionné, puis cliquez sur **OK**.

   Le scénario pour lequel vous configurez l'alerte a une incidence sur la configuration et comment, le cas échéant, vous filtrez davantage déclencheur alerte règle.

6. Configurer l'alerte :

   a. Dans **Alert**, cliquez sur **Select**.

      La fenêtre **Edit Alert** s'ouvre.

   b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.

   c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

   d. Dans l'onglet Associated Reports, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez générer lors de l'alerte.

7. Cliquez sur une des options d'enregistrement.

Création de règles basées sur des événements pour la prédiction

Les règles basées sur des événements fonctionnent en réponse aux données diffusées en continu et en temps réel dans le serveur DPA et déclenchent des alertes lorsqu'un événement se produit dans une période définie.

La procédure est consacrée à la création d'une règle pour une alerte lorsqu'il est prévu qu'un serveur Avamar atteigne 90 % d'utilisation au cours des 24 heures qui suivent.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle adapté à la condition que vous mettez en place pour la règle.

   Par exemple, **`Serveur Avamar 90 % prévus dans les 24 prochaines heures`**

   Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.

   Une règle de modèle système appelée Backup Failed existe. Vous pouvez la modifier si vous le souhaitez. Cet exemple montre comment le créer intégralement.
3. Dans le champ **Category**, sélectionnez dans le menu déroulant la catégorie appropriée la plus adaptée à la règle que vous mettez en place.

   Par exemple, **Resource Utilization**.
4. Configurer le type d'objet. Dans cet exemple, nous voulons alerter les serveurs de sauvegarde Avamar. Par conséquent, nous allons sélectionner l'objet Backup Application.
   a. Dans **Object Type**, cliquez sur **Select**.

      La fenêtre **Select Object Types** s'ouvre.
   b. Développez des Backup Applications, développez le serveur de sauvegarde, puis sélectionnez **Backup Application** dans la liste **Select Object Type** et cliquez sur **Select Object Type**.

      Vous pouvez utiliser la fonction de filtrage pour trouver facilement l'objet que vous souhaitez surveiller.

      Le type d'objet que vous sélectionnez varie selon le scénario à partir duquel vous souhaitez déclencher l'alerte.
5. Configurer le déclencheur d'alertes. Dans cet exemple, nous voulons examiner uniquement des serveurs de sauvegarde spécifiques qui atteignent un taux d'utilisation cible pendant une période définie. Par conséquent, nous allons sélectionner le déclencheur et définir des filtres de conditions pour rechercher uniquement un comportement prédictif :
   a. Dans **Alert Trigger**, cliquez sur **Select**.

      La fenêtre **Select Alert Trigger** s'ouvre.
   b. Cliquez sur le bouton radio **Predictive Time**, puis cliquez sur **Select and Edit Filter**.

      La fenêtre **Edit Filter** s'ouvre.

c. Pour l'option 1, Select attribute to predict, cliquez sur **Browse**.

La fenêtre **Select Attribute** s'ouvre.

d. Dans le Type d'objet BackupApplication, sélectionnez la ligne avec le paramètre AttributeName **Utilisation**, cliquez sur **Select Attribute**, puis cliquez sur **OK**.

Vous pouvez utiliser la fonction de filtrage pour trouver facilement la catégorie et l'Attributename souhaités.

e. Pour l'option 2, Set threshold, sélectionnez **Static Value** et saisissez `90` ou faites défiler jusqu'à cette valeur.

f. Pour l'option 3, Specify when to send alert, sélectionnez **Static Value**, puis sélectionnez **1** et **Days**dans les listes déroulantes.

g. Ignorez l'option 4 ; il n'existe aucun filtre de condition pour cet exemple.

h. Pour l'option 5, Select prediction method, conservez la sélection par défaut.

i. Cliquez sur **OK**.

Le scénario pour lequel vous configurez l'alerte a une incidence sur la configuration et, le cas échéant, sur la manière dont vous filtrez davantage le déclencheur d'alerte de règle.

6. Configurer l'alerte :

a. Dans **Alert**, cliquez sur **Select**.

La fenêtre **Edit Alert** s'ouvre.

b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.

c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

d. Dans l'onglet Associated Reports, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez générer lors de l'alerte.

7. Cliquez sur une des options d'enregistrement.

Création de règles planifiées

Les règles planifiées comparent régulièrement les données du datastore DPA à des règles pour détecter une correspondance avec un problème spécifique que vous souhaitez suivre. Pour ce faire, il utilise un rapport. Vous pouvez utiliser un rapport de modèle système ou un rapport personnalisé.

La procédure est consacrée à la création d'une règle pour générer une alerte pour les clients de sauvegarde ayant échoué lors de trois tentatives.

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **Custom Rule Templates**, puis cliquez sur **Create Custom Rule Template**.
2. Renseignez le champ **Name/Alert Message** avec un nom de règle adapté à la condition que vous mettez en place pour la règle.

Par exemple, **`planification en fonction de trois échecs de tentatives de sauvegarde`**

Vous pouvez également saisir une description de la condition, si vous le souhaitez. Cette opération est facultative.

Une règle de modèle système appelée Backup Failed existe. Vous pouvez la modifier si vous le souhaitez. Cet exemple montre comment la créer intégralement.

3. Dans le champ **Type**, sélectionnez **Scheduled** dans la liste déroulante.
4. Dans le champ **Category**, sélectionnez dans le menu déroulant la catégorie appropriée la plus adaptée à la règle que vous mettez en place.

   Par exemple, **Data Protection**.
5. Sélectionnez le rapport. Dans cet exemple, nous voulons générer une alerte lorsqu'un client de sauvegarde a connu des échecs lors de trois tentatives. Par conséquent, nous allons sélectionner le rapport Three Strike Failed Client.
   a. Dans **Select Report Template**, cliquez sur **System Report Templates**.
   b. Sélectionnez **Three Strike Failed Client** dans la liste **System Template Name** et cliquez sur **Select Template and Edit Options**.

      Vous pouvez utiliser la fonction de filtrage pour trouver facilement l'objet que vous souhaitez surveiller.

      Le type d'objet que vous sélectionnez varie selon le scénario à partir duquel vous souhaitez déclencher l'alerte.
6. Configurer les options.
   a. Dans Number of Alert, sélectionnez les options qui répondent le mieux à vos besoins.

      Si vous sélectionnez **Generate a separate alert for each row**, DPA envoie une alerte différente pour chaque client. Ces informations sont utiles, car elles sont granulaires. Toutefois, si vous créez des alertes pour un grand nombre de clients, vous pouvez recevoir un grand nombre d'alertes.

      Si vous sélectionnez **Generate one alert for all rows**, DPA envoie une alerte pour les nœuds de niveau supérieur. Cette fonction est utile si vous souhaitez moins d'alertes parce que vous avez un grand nombre de clients ; toutefois, ces informations sont moins granulaires.
   b. Dans les paramètres Default, cliquez sur **Select Schedule** et sélectionnez une des options Manage Schedule ou cliquez sur **Create Schedule** afin de créer votre propre planification qui définit les modalités d'exécution de la règle.

      Nous vous recommandons de ne pas sélectionner **Always** dans les options Manage Schedule, car cette option surcharge le serveur.
   c. Veillez à passer en revue le choix de la période de temps et conservez le choix par défaut ou modifiez ce choix.
   d. Cliquez sur **OK**.
7. Configurer l'alerte :
   a. Dans **Alert**, cliquez sur **Select**.

      La fenêtre **Edit Alert** s'ouvre.
   b. Dans l'onglet **Alert Fields**, sélectionnez le niveau de gravité dans le menu déroulant.
   c. Dans l'onglet **Description & Resolution**, configurez les informations de description et de résolution que vous souhaitez envoyer avec l'alerte.

d. Dans l'onglet **Associated Reports**, sélectionnez un rapport de modèle système ou créez un rapport personnalisé que vous souhaitez voir généré lors de l'alerte.

e. Dans l'onglet **Rule Object**, veillez à sélectionner l'**Object Type** et à sélectionner **Name Field** et **CSub Name Field** dans les listes déroulantes.

8. Cliquez sur une des options d'enregistrement.

Ajout d'une règle d'analyse à une politique d'analyse

Lorsqu'un modèle de règle est ajouté à une politique d'analyse, le moteur d'analyse effectue certaines opérations, puis affiche les événements résultants dans la section **Alerts** de la console Web.

Les politiques d'analyse peuvent contenir plusieurs règles d'analyse qui s'appliquent à différents types d'objet. DPA applique automatiquement les règles appropriées de la politique d'analyse en vigueur à un objet. Par exemple, DPA applique les règles destinées aux switches uniquement à ces derniers, et non aux serveurs de sauvegarde.

Fichier log des actions du moteur d'analyse

Le fichier `actions.log` contient un enregistrement pour chaque notification d'action réussie du moteur d'analyse.

Les actions du moteur d'analyse peuvent être :

- email
- SNMP
- scrpt
- Windows event log

Le fichier `actions.log` contient uniquement les informations sur les actions réussies. Il ne comporte pas les informations relatives aux échecs ou les avertissements signalant des actions échouées. L'emplacement par défaut du fichier `actions.log` est `$instalationDir\services\logs`. Cet emplacement ne peut pas être configuré par l'utilisateur.

Catégories de règles de politique d'analyse

Planification de la capacité
Les politiques d'analyse de planification des capacités génèrent des alertes relatives à des événements qui indiquent que des ressources pourraient bientôt être épuisées. Le tableau suivant décrit ces tâches.

Attribution d'alertes aux politiques d'analyse des pools et des baies de stockage
Lorsque vous attribuez les politiques d'analyse ci-dessous à des objets, les niveaux de gravité recommandés sont les suivants :

- Le pool de stockage se remplit - Gravité 3
- Le pool de stockage se remplit - Gravité 2
- La baie de stockage se remplit - Gravité 1

Tableau 38 Planification de la capacité

Règle	Description	Paramètres
Remplissage du système de fichiers	Génère des alertes si l'utilisation d'un système de	Utilisation maximale prévue - 100 %

Tableau 38 Planification de la capacité (suite)

Règle	Description	Paramètres
	fichiers va dépasser 90 % au cours des 2 prochaines semaines.	Nombres d'heures à prévoir - 336
Nombre insuffisant de licences client de sauvegarde	Génère des alertes si la licence permet uniquement de surveiller moins de 25 ordinateurs supplémentaires.	Nombre maximal de licences client - 25
Le pool de stockage se remplit	Génère des alertes lorsque la tendance croissante indique que le pool va manquer d'espace pendant la période sélectionnée.	Espace libre minimal autorisé - 0 Nombre de jours à prévoir - 90
Le pool de stockage est rempli	Génère des alertes lorsqu'il n'y a plus d'espace dans le pool pour allouer physiquement une nouvelle LUN.	Capacité consommée initiale - 3
La baie de stockage se remplit	Génère des alertes lorsqu'il n'y a plus d'espace pour allouer une nouvelle LUN dans le pool et qu'il ne reste aucun disque disponible dans la baie de stockage.	Capacité consommée initiale - 2
Le nombre de bandes vierges diminue	Génère des alertes si le nombre de bandes vierges dans un pool de bandes risque de devenir insuffisant au cours des 6 prochaines semaines.	Nombre maximal prévu - 0 Nombres d'heures à prévoir - 1008
La base de données TSM se remplit	Génère une alerte si le système estime que le niveau d'utilisation de la base de données TSM atteindra 100 % de sa capacité au cours des 2 prochaines semaines.	Nombres d'heures à prévoir - 336 Utilisation maximale prévue - 100
Utilisation de la base de données TSM élevée	Génère une alerte si le système estime que le niveau d'utilisation du fichier journal de restauration TSM atteindra 100 % de sa capacité au cours des 2 prochaines semaines.	Nombres d'heures à prévoir - 336 Utilisation maximale prévue - 100

Gestion des changements

Les politiques d'analyse de gestion des changements génèrent des alertes relatives à des modifications survenues dans l'environnement. Le tableau suivant décrit ces tâches.

Tableau 39 Gestion des changements

Règle	Description :	Paramètres
Configuration du client de sauvegarde modifiée	Génère des alertes si la configuration d'un client de sauvegarde a été modifiée.	S/o
Configuration du périphérique de sauvegarde modifiée	Génère des alertes si la configuration d'un périphérique de sauvegarde a été modifiée.	S/o
Configuration du groupe de sauvegarde modifiée	Génère des alertes si la configuration d'un groupe de sauvegarde a été modifiée.	S/o
Niveau du microprogramme du disque modifié	Génère des alertes si le niveau du microprogramme du disque a été modifié.	S/o
Numéro de série du disque modifié	Génère des alertes si le numéro de série d'un disque a été modifié.	S/o
Système d'exploitation d'objet modifié	Génère des alertes si le système d'exploitation d'un objet a été modifié.	S/o
RPA RecoverPoint actif modifié	Génère une alerte si le RPA actif a été modifié depuis la dernière exécution de l'analyse.	S/o
RecoverPoint pour VMs Consistency Group Copy est désactivé	Vous alerte si un RecoverPoint pour la copie de groupes de cohérence de machines virtuelles est désactivé.	S/o
État du lien RPA RecoverPoint modifié	Génère une alerte si l'état du lien RPA a été modifié depuis la dernière exécution de l'analyse.	S/o
Niveau du microprogramme du lecteur de bande modifié	Génère des alertes si le niveau du microprogramme d'un lecteur de bande a été modifié.	S/o
Numéro de série du lecteur de bande modifié	Génère des alertes si le numéro de série d'un lecteur de bande a été modifié.	S/o

Configuration

Les politiques d'analyse de configuration surveillent l'environnement afin de détecter les problèmes de configuration des périphériques et des applications. Le tableau suivant décrit ces tâches.

Tableau 40 Configuration

Règle	Description	Paramètres
Client de sauvegarde inactif	Génère des alertes si un client de sauvegarde n'est pas programmé pour s'exécuter.	S/o
Export du serveur de fichiers et LUN sur le même volume	Génère des alertes si un export du serveur de fichiers est sur le même volume qu'une LUN.	S/o
LUN sur un volume donné	Génère des alertes si une LUN a été configurée sur le volume vol0.	Volume - vol0
Incompatibilité de négociation automatique d'IP	Génère des alertes en cas d'incompatibilité de négociation automatique entre un hôte et son port de switch.	S/o
Incompatibilité de duplex d'IP	Génère des alertes en cas d'incompatibilité de duplex entre l'objet et le switch.	S/o
Mémoire virtuelle insuffisante	Génère des alertes si la quantité de mémoire virtuelle sur un ordinateur est inférieure à 1,5 fois la mémoire physique.	S/o
Priorité de volume autre que normale	Génère des alertes quand la priorité de volume est définie sur une autre option que normale.	S/o

Protection des données

Les politiques d'analyse de protection des données surveillent l'environnement afin de détecter les exceptions liées aux problèmes de sauvegarde et de restauration. Le tableau suivant décrit les tâches gérées.

Tableau 41 Protection des données

Règle	Description	Paramètres
Estimation trop élevée de la durée de restauration de l'application	Génère des alertes si la durée de restauration d'une application est estimée à plus de 12 heures.	Objectif de temps de restauration : 12 heures
RTO de l'application manqué	Alerte si une application n'a pas été sauvegardée avec succès pendant plus de 72 heures.	Objectif de point de restauration : 72 heures
Échec de la sauvegarde	Alerte générée en cas d'échec d'une sauvegarde.	S/o

Tableau 41 Protection des données (suite)

Règle	Description	Paramètres
Aucune sauvegarde réussie en une minute	Alerte générée en cas d'échec d'une sauvegarde deux fois consécutives.	Nombre maximal d'échecs : 2
Sauvegarde supérieure à la moyenne	Génère une alerte si la taille d'une tâche de sauvegarde correspond au double de sa taille moyenne au cours des 14 derniers jours.	Jours d'historique : 14 jours Écart : 100 %
Aucune sauvegarde pendant plusieurs jours	Alerte générée si aucune sauvegarde n'a été effectuée pour un hôte au cours des 3 derniers jours.	Nombre maximal de jours sans sauvegarde : 3
Exécution d'une sauvegarde en même temps qu'une opération du serveur	Génère une alerte si des sauvegardes ont été réalisées pendant une période donnée, chevauchant l'une opérations suivantes exécutée sur le serveur de sauvegarde : • Supprimer des volumes • Expirations • Copies de pool de stockage • Moves • Sauvegarde de base de données • Migrations • Réclamations	Aucune.
La sauvegarde couvre plusieurs bandes	Alerte générée si une sauvegarde couvre plus de 3 bandes.	Nombre maximal de bandes : 3
Sauvegarde complète inférieure à la moyenne	Génère des alertes si une sauvegarde complète est inférieure à 50 % de sa taille habituelle.	Jours d'historique : 14 jours Écart : 50 %
Aucune sauvegarde complète pendant plusieurs jours	Génère une alerte si aucune sauvegarde complète n'a été effectuée pour un hôte au cours des 14 derniers jours.	Nombre maximal de jours sans sauvegarde : 14
Miroir non mis à jour pendant un certain nombre d'heures	Génère des alertes si un miroir de disque distant n'a pas été mis à jour pendant au moins 2 jours.	Exposition maximale : 48 heures

Tableau 41 Protection des données (suite)

Règle	Description	Paramètres
Trop de sauvegardes sans une sauvegarde complète	Génère des alertes si une tâche de sauvegarde a été exécutée plus de sept fois depuis la dernière sauvegarde complète.	Nombre maximal de sauvegardes non complètes : 7
Pas de données d'amorçage NetWorker générées	Génère une alerte si aucune amorce de NetWorker n'a été exécutée au cours des dernières 48 heures.	Nombre maximal d'heures sans données d'amorçage : 48 heures par défaut
Exécution d'une sauvegarde de base de données TSM en même temps qu'une opération du serveur	Génère une alerte si un processus de sauvegarde de base de données a été exécuté alors qu'une autre activité était en cours sur le serveur de sauvegarde, notamment une autre sauvegarde.	Aucune.
Une sauvegarde de la base de données TSM a été effectuée	Génère une alerte si une sauvegarde de la base de données TSM a eu lieu au cours des dernières 24 heures, ou renvoie l'heure de la dernière sauvegarde TSM si aucune sauvegarde n'a été effectuée.	Durée - 24 heures

Octroi de licences

Les politiques d'analyse des licences surveillent l'environnement et génèrent des alertes relatives à des problèmes de licences. Le tableau suivant décrit ces règles de façon détaillée.

Tableau 42 Octroi de licences

Règle	Description :	Paramètres
La licence a expiré	Génère une alerte si une licence dans DPA a expiré.	s.o.
Expiration proche de la licence	Génère une alerte si une licence expire au cours de la semaine suivante.	Nombre minimal de jours avant expiration : 7 jours par défaut

Performances

Les politiques d'analyse des performances surveillent l'environnement et génèrent des alertes en relation avec les problèmes de performances. Le tableau suivant décrit ces tâches en détail.

Tableau 43 Performances

Règle	Description	Paramètres
Sauvegarde plus lente que la moyenne	Génère une alerte si les performances d'une sauvegarde sont inférieures de 50 % à sa moyenne au cours des 2 dernières semaines.	Jours d'historique - 14 Écart - 50 %
Saturation de la procédure de sauvegarde	Génère une alerte si une sauvegarde est exécutée pendant plus de 18 heures.	Temps d'exécution maximal - 18 heures
Pourcentage faible d'opérations réussies dans le cache du serveur de fichiers	Génère des alertes si le pourcentage d'opérations réussies dans le cache d'un serveur de fichiers devient inférieur à 80 %.	Pourcentage minimal d'opérations réussies dans le cache - 80 %
Sauvegarde complète réussie mais lente	Génère une alerte si une sauvegarde complète est exécutée à moins de 300 Ko/s.	Vitesse minimale prévue - 300 Ko/s

Provisioning

Les politiques d'analyse de provisionnement génèrent des alertes relatives à des événements qui peuvent nécessiter des opérations de provisionnement. Le tableau suivant décrit les tâches.

Tableau 44 Provisioning

Règle	Description	Paramètres
Espace de snapshots du système de fichiers sous-utilisé	Génère des alertes si la pointe d'utilisation des snapshots au cours des 14 derniers jours est inférieure à 80 %.	Jours pour examiner l'utilisation - 14 Pointe d'utilisation des snapshots minimale - 80 %

Capacité de Restauration

Les règles d'analyse de la capacité de restauration émettent des alertes relatives à la capacité de restauration. Le tableau suivant décrit ces tâches.

Tableau 45 Capacité de Restauration

Règle	Description :	Paramètres
Vérification DR Host Visibility pour TF/Snap	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour MirrorView/A	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.

Tableau 45 Capacité de Restauration (suite)

Règle	Description :	Paramètres
Vérification DR Host Visibility pour MirrorView/S	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour RecoverPoint/A	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour RecoverPoint/S	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour SanCopy	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour SRDF/S continu	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification DR Host Visibility pour SRDF/S à un point dans le temps	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Exposition de la capacité de restauration	Exposition de la capacité de restauration	s.o.
Vérification de groupe de cohérence pour SRDF/A continu	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification de groupe de cohérence pour SRDF/A à un point dans le temps	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification de groupe de cohérence pour SRDF-S/EDP continu	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le	s.o.

Tableau 45 Capacité de Restauration (suite)

Règle	Description :	Paramètres
	groupe de cohérence est activé.	
Vérification de groupe de cohérence pour SRDF-S/EDP à un point dans le temps	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification DR Host Visibility pour SRDF/A	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour SRDF/S	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour SV/Clone	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour SV/Snap	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour TF/Mirror	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification DR Host Visibility pour TF/Clone	que les périphériques du point de restauration sont mappés, masqués et visibles par l'hôte de reprise après sinistre	s.o.
Vérification de groupe de cohérence de SRDF-A/EDP continu	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification de groupe de cohérence pour SRDF-A/EDP à un point dans le temps	Vérifie que les périphériques du point de restauration sont configurés dans le même groupe de cohérence et que le groupe de cohérence est activé.	s.o.
Vérification de la réplication de périphérique cohérente	Vérification (conformément aux bonnes pratiques). Une	s.o.

Tableau 45 Capacité de Restauration (suite)

Règle	Description :	Paramètres
pour SV/Clone à un point dans le temps	alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	
Vérification de la réplication de périphérique cohérente pour SV/Snap à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour TF/Mirror à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour TF/Clone à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour TF/Snap à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour MirrorView/A à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour MirrorView/S à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.

Tableau 45 Capacité de Restauration (suite)

Règle	Description :	Paramètres
Vérification de la réplication de périphérique cohérente pour RecoverPoint/A à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour RecoverPoint/S à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour SanCopy à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Vérification de la réplication de périphérique cohérente pour SNAPVX à un point dans le temps	Vérification (conformément aux bonnes pratiques). Une alerte est générée si l'opération de cohérence n'a pas été émise, mais est toutefois recommandée par le fournisseur.	s.o.
Violations de cohérence des applications	Inconsistent Replication: l'application n'était pas en mode de sauvegarde lors du processus de réplication	s.o.
Application Not in Backup mode	L'application n'est pas en mode de sauvegarde lors de la création de la réplication	s.o.
Consistency Group is disabled	Le groupe de cohérence est désactivé.	s.o.
Invalid Replication	Les images d'objet ont échoué ou n'ont pas respecté le planning	s.o.
Logs not on Disk	Le fichier log de l'application n'est pas détecté sur disque	s.o.
Not all the devices are part of a replication group	Le périphérique ne fait pas partie d'un groupe de réplication	s.o.

Tableau 45 Capacité de Restauration (suite)

Règle	Description :	Paramètres
Not Protected Logs	Inconsistent Replication: Le fichier est requis pour la restauration, mais n'a pas été protégé	s.o.
Partially Replicated	Objet répliqué partiellement	s.o.
La réplication continue est interrompue	La réplication continue est interrompue	s.o.
Storage Object Not Protected	L'objet de stockage d'application n'est pas protégé	s.o.
The link status for a continuous replication is down	Le lien pour une application continue présente un état défaillant	s.o.

Utilisation des ressources

Les politiques d'analyse d'utilisation des ressources génèrent des alertes relatives à des événements survenus en raison de problèmes d'utilisation des ressources dans l'environnement. Le tableau suivant décrit ces tâches en détail.

Tableau 46 Utilisation des ressources

Règle	Description	Paramètres
Utilisation élevée globale des snapshots	Génère une alerte si une utilisation globale des snapshots est supérieure au seuil spécifié.	Utilisation globale des snapshots maximale - 90 % par défaut
CPU bloqué	Génère une alerte si l'utilisation du CPU sur un hôte est supérieure à 90 % au cours des 30 dernières minutes.	Utilisation maximale du CPU - 90 % par défaut Nombre de minutes - 30 minutes
Disque bloqué	Génère une alerte si un disque sur un hôte est occupé à plus de 90 % au cours des 30 dernières minutes.	Pourcentage d'occupation du disque maximal - 90 % Nombre de minutes - 30 minutes par défaut
Utilisation élevée du port Fibre Channel	Génère une alerte si un port Fibre Channel dépasse 70 % de son débit maximal.	Utilisation maximale - 70 %
Port Fibre Channel sans BB credits	Génère une alerte si le nombre de buffer credits d'un port Fibre Channel devient insuffisant.	S/o
Utilisation élevée des fichiers du système de fichiers	Génère une alerte si le nombre de fichiers d'un système de fichiers est	Utilisation maximale des fichiers du système de fichiers - 90 %

Tableau 46 Utilisation des ressources (suite)

Règle	Description	Paramètres
	supérieur à 90 % du nombre maximal autorisé.	
Utilisation élevée des snapshots du système de fichiers	Génère une alerte si l'utilisation des snapshots du système de fichiers est supérieure à 90 %.	Utilisation maximale des snapshots du système de fichiers - 90 % par défaut
Utilisation du système de fichiers élevée et en hausse	Génère une alerte si l'utilisation d'un système de fichiers est supérieure à 90 % et en hausse.	Utilisation maximale du système de fichiers - 90 % par défaut
Utilisation élevée de la mémoire	Génère une alerte si l'utilisation de la mémoire sur un hôte est supérieure à 90 %.	Utilisation maximale de la mémoire - 90 % par défaut
Utilisation élevée du réseau	Génère une alerte si une interface réseau dépasse 70 % de son débit nominal.	Utilisation maximale - 70 % par défaut
Utilisation élevée du log RecoverPoint	Génère une alerte si l'utilisation du log pour un RPA dépasse un seuil d'avertissement ou critique donné.	Seuil d'avertissement Seuil critique
Utilisation élevée du log RecoverPoint	Génère une alerte si l'utilisation du SAN pour un RPA dépasse un seuil d'avertissement ou critique donné.	Seuil d'avertissement Seuil critique
Utilisation élevée du WAN du RPA RecoverPoint	Génère une alerte si l'utilisation du WAN pour un RPA dépasse un seuil d'avertissement ou critique donné.	Seuil d'avertissement Seuil critique
Décalage de réplication RecoverPoint élevé	Génère une alerte si le décalage de réplication ou de données dépasse un seuil d'avertissement ou critique donné.	Seuil d'avertissement pour le décalage de réplication Seuil critique pour le décalage de réplication Seuil d'avertissement pour le décalage de données Seuil critique pour le décalage de données
Utilisation de la base de données TSM élevée	Génère une alerte si l'utilisation de la base de données TSM dépasse 90 %.	Utilisation maximale de la base de données TSM - 90 %

Tableau 46 Utilisation des ressources (suite)

Règle	Description	Paramètres
Durée du processus d'expiration supérieure aux prévisions	Génère une alerte si l'exécution du processus d'expiration TSM dure plus d'une heure, ou si sa durée est supérieure (de plus de 25 %) à la durée moyenne d'exécution observée au cours des sept derniers jours.	% d'augmentation - 25 % Période - 7 Durée maximale - 1
Utilisation du log de restauration TSM élevée	Génère une alerte si l'utilisation de la base de données TSM dépasse 90 %.	Utilisation maximale du log de restauration - 90 %

Contrats de niveau de service

Les politiques d'analyse des contrats de niveau de service (SLA) génèrent des alertes relatives au non-respect du SLA. Le tableau suivant décrit les tâches liées au SLA.

Tableau 47 Contrat de niveau de service

Règle	Description	Paramètres
Sauvegarde réussie mais échec des conditions SLA	Génère une alerte si une sauvegarde a été réussie mais hors de sa fenêtre de sauvegarde.	S/o

État

Les politiques d'analyse des catégories d'état génèrent des alertes en cas de problème relatif à l'état actuel d'un périphérique surveillé ou de l'application correspondante. Le tableau suivant décrit les tâches liées à l'état.

Tableau 48 État

Nom	Description :	Règle	Paramètres
Erreurs du serveur de sauvegarde	Génère une alerte lorsqu'une erreur de serveur de sauvegarde est consignée (TSM uniquement).	Erreurs du serveur de sauvegarde	s.o.
Copie de groupe de cohérence pour la liaison de machines virtuelles interrompue	Copie de groupe de cohérence de RecoverPoint pour les machines virtuelles activée et liaison interrompue.	Copie de groupe de cohérence pour la liaison de machines virtuelles hors tension	Entité ; CgCopyStatus Condition "enabled is false (or 0- please check)" champs : les transferts de données ne sont pas « Active »

Tableau 48 État (suite)

Nom	Description :	Règle	Paramètres
CPU hors ligne	Génère une alerte si un CPU est hors ligne.	CPU hors ligne	s.o.
Échec du heartbeat d'un agent	Génère une alerte si un agent ne parvient pas à envoyer son heartbeat.	Échec du heartbeat d'un agent	s.o.
Message de fichier log d'agent	Génère une alerte en cas de message consigné dans les fichiers log des agents.	Messages de log d'agent	s.o.
Échec du disque	Génère une alerte en cas d'échec d'un disque.	Échec du disque	s.o.
Un basculement sur incident d'une EDL s'est produit	Génère une alerte si un basculement sur incident d'une appliance EDL vers une autre se produit.	Un basculement sur incident d'une EDL s'est produit	s.o.
Ventilateur inactif	Génère une alerte si un ventilateur sur un périphérique est inactif.	Ventilateur inactif	s.o.
Changement d'état du port Fibre Channel	Génère une alerte en cas de changement d'état d'un port Fibre Channel.	Changement d'état du port Fibre Channel	s.o.
Moins de 75 % de périphériques de sauvegarde disponibles	Génère une alerte si moins de 75 % de périphériques de sauvegarde sont disponibles sur un serveur de sauvegarde.	Moins de x % de périphériques de sauvegarde disponibles	Disponibilité des périphériques de sauvegarde la plus basse - 75 % par défaut
Plus de 3 périphériques de sauvegarde indisponibles	Génère une alerte si plus de 3 périphériques de sauvegarde sont indisponibles sur un serveur de sauvegarde.	Nombreux périphériques de sauvegarde indisponibles	Nombre maximal de périphériques indisponibles - 3
Changement d'état de l'interface réseau	Génère une alerte si une interface réseau reçoit un événement de lien actif ou inactif.	Changement d'état de l'interface réseau	s.o.

Tableau 48 État (suite)

Nom	Description :	Règle	Paramètres
Objet redémarré	Génère une alerte en cas de redémarrage d'un hôte.	Objet redémarré	s.o.
État d'objet non actif	Génère une alerte si l'état d'un objet passe à un autre état que l'état actif.	État d'objet non actif	s.o.
Bloc d'alimentation inactif	Génère une alerte si un bloc d'alimentation est inactif.	Bloc d'alimentation inactif	s.o.
Éditeur en attente	Alerte générée si la file d'attente de Publisher n'a pas changé depuis la dernière interrogation.	File d'attente de l'éditeur en attente	s.o.
Message de fichier journal de serveur	Alerte en cas de message dans les fichiers journaux de serveur.	Message de fichier journal de serveur	s.o.
Nettoyage requis du lecteur de bande	Génère une alerte si un lecteur de bande doit être nettoyé.	Nettoyage requis du lecteur de bande	s.o.
Lecteur de bande non OK	Génère une alerte si un lecteur de bande indique un état autre qu'OK.	Lecteur de bande non OK	s.o.
Librairie de bandes non OK	Génère une alerte si une librairie de bandes indique un état autre qu'OK.	Librairie de bandes non OK	s.o.
Sonde inactive	Génère une alerte si une sonde devient inactive.	Sonde inactive	s.o.
Surchauffe du thermomètre	Génère une alerte si un thermomètre sur un périphérique indique que celui-ci est en surchauffe.	Surchauffe du thermomètre	s.o.
En attente de bandes inscriptibles pendant plus de 30 minutes	Génère une alerte si un serveur de sauvegarde attend depuis plus de 30 minutes une bande inscriptible.	En attente de périphériques inscriptibles	Nombre maximal de périphériques en attente - 0 par défaut Nombre de minutes avant l'alerte - 30 minutes par défaut

Tableau 48 État (suite)

Nom	Description :	Règle	Paramètres
Le ventilateur Xsigo fonctionne à moins de 90 % de sa vitesse normale	Génère une alerte si la vitesse d'un ventilateur sur un directeur Xsigo est inférieure à 90 % de la vitesse normale.	La vitesse du ventilateur Xsigo est inférieure à la vitesse attendue	Pourcentage à vérifier - 90 % par défaut.

Dépannage

Les politiques d'analyse de dépannage permettent de résoudre les problèmes relatifs à l'environnement. Le tableau suivant décrit ces tâches.

Tableau 49 Dépannage

Règle	Description	Paramètres
Échec de la sauvegarde en raison d'erreurs au niveau du réseau client	Génère une alerte en cas d'échec d'une sauvegarde sur un client alors que les erreurs réseau sont en augmentation.	S/o
Échec de la procédure de sauvegarde en raison d'une utilisation élevée du CPU client	Génère une alerte en cas d'échec d'une sauvegarde sur un client alors que l'utilisation du CPU sur l'ordinateur est supérieure à 90 %.	Utilisation maximale du processeur - 90 % par défaut
Échec de la procédure de sauvegarde en raison d'une utilisation élevée de la mémoire client	Génère une alerte en cas d'échec d'une sauvegarde sur un client alors que l'utilisation de la mémoire sur ce client est supérieure à 90 %.	Utilisation maximale de la mémoire - 90 par défaut
Échec de la sauvegarde en raison d'une utilisation élevée du CPU serveur	Génère une alerte en cas d'échec d'une sauvegarde sur un client alors que l'utilisation du CPU sur le serveur de sauvegarde est supérieure à 90 %.	Utilisation maximale du processeur - 90 % par défaut
Échec de la sauvegarde en raison d'une utilisation élevée de la mémoire serveur	Génère une alerte en cas d'échec d'une sauvegarde alors que l'utilisation de la mémoire sur le serveur de sauvegarde est supérieure à 90 %.	Utilisation maximale de la mémoire - 90 % par défaut
Échec de la sauvegarde en raison d'erreurs au niveau du réseau serveur	Génère une alerte en cas d'échec d'une sauvegarde alors que les erreurs réseau sont en augmentation sur le serveur de sauvegarde.	S/o

Tableau 49 Dépannage (suite)

Règle	Description	Paramètres
Échec du disque pendant un certain nombre d'heures	Génère une alerte en cas d'échec d'un disque pendant plus de 48 heures. Sous Linux et Solaris.	Nombre maximal d'heures d'échec - 48 heures par défaut
Erreurs signalées au niveau du port Fibre Channel	Génère une alerte si un port Fibre Channel indique des erreurs.	S/o
Plus de x % d'erreurs signalées au niveau du port Fibre Channel	Génère une alerte si plus de 1 % des trames transitant via un port Fibre Channel présentent des erreurs.	Pourcentage maximal d'erreurs - 1 % par défaut
Erreurs signalées au niveau de l'interface réseau	Génère une alerte si des erreurs sont détectées sur une interface réseau.	S/o
Plus de x % d'erreurs signalées au niveau de l'interface réseau	Génère une alerte si plus de 1 % des paquets transitant via une interface réseau présentent des erreurs.	Pourcentage maximal d'erreurs - 1 % par défaut
Erreurs signalées au niveau du lecteur de bande.	Génère une alerte en cas de hausse du nombre d'erreurs sur un lecteur de bande.	Inclure les erreurs récupérables - False par défaut

Politiques de protection

Les politiques de protection sont utilisées dans le cadre des contrats de niveau de service et du reporting d'exposition pour calculer si une sauvegarde a été exécutée dans sa fenêtre de sauvegarde et si une application ou un hôte remplit ses objectifs de temps de restauration (RTO) et de point de restauration (RPO). Les politiques de protection déterminent également la façon dont une application, un hôte ou un périphérique doit être répliqué ou sauvegardé. Les politiques sont attribuées à des objets et sont constituées d'un ensemble de règles qui régissent les éléments suivants :

- Pour la réplication, le type de copie, le niveau de réplication et le calendrier.
- Pour les sauvegardes : le niveau et le calendrier de sauvegarde.

Les rapports DPA comparent ensuite la politique de protection d'un objet à la réplication ou à la sauvegarde réelle réalisée afin d'afficher le niveau de conformité à la politique.

vérifications de la capacité de restauration

Les vérifications de la capacité de restauration sont des contrôles de cohérence supplémentaires que DPA exécute sur un environnement si vous configurez l'analyse de la capacité de restauration. Une vérification de la capacité de restauration permet d'assurer que l'environnement de stockage et de restauration est configuré selon les exigences particulières d'un utilisateur, par exemple, reprise après sinistre.

Si vous avez activé la vérification de la capacité de restauration et que DPA détecte une incohérence, une vérification de la capacité de restauration génère une exposition, comparable à celle générée par une violation de politique de protection ou une

demande de restauration. Les expositions de vérification de la capacité de restauration apparaissent dans les rapports d'exposition.

Il existe trois vérifications de la capacité de restauration système qui identifient les écarts, comme décrit dans le tableau suivant.

Tableau 50 vérifications de la capacité de restauration

Vérification de la capacité de restauration	Description
Vérification de groupe de cohérence	Vérifie si les périphériques du point de restauration sont configurés dans le même groupe de cohérence et si le groupe de cohérence est activé. S'il n'existe pas de groupe de cohérence, un écart de violation de cohérence est généré pour le point de restauration.
Vérification de réplication de périphérique cohérente	Vérifie si l'option de cohérence a été utilisée lorsque les images ont été créées, s'il y a lieu. Cette vérification fait partie des bonnes pratiques. Si l'option de cohérence n'a pas été utilisée, un écart de Consistency Violation est généré pour le point de récupération.
Vérification DR Host Visibility	Vérifie si les périphériques d'un point de restauration sont mappés, masqués et visibles pour l'hôte Disaster Recovery. Dans le cas contraire, un écart de Consistency Violation est généré.

Politiques de refacturation

Les rapports de refacturation permettent d'analyser les coûts financiers liés aux opérations de sauvegarde, de restauration et de réplication de protection des données ayant été effectuées dans l'environnement d'un client. DPA calcule un coût pour chaque client de sauvegarde et peut le refacturer à l'entité responsable de ce client ou d'un ensemble de clients.

DPA calcule la refacturation à l'aide de deux modèles : un pour la sauvegarde et la restauration des données, et un autre pour la protection et la réplication des données de stockage par RecoverPoint. DPA calcule la refacturation pour les clients sur la base des entrées associées à chaque type.

Refacturation des sauvegardes

DPA permet la refacturation du stockage par coût de Go sauvegardé et autres coûts de sauvegarde.

Le coût par Go sauvegardé utilise les entrées suivantes :

- Base Size : volume de sauvegarde de base en Go permettant d'évaluer le coût de base.
- Base Cost : coût total de la sauvegarde jusqu'au volume de base spécifié.
- Cost of Each Additional GB : coût supplémentaire par Go pour des sauvegardes dont le volume est supérieur à celui de base.

DPA calcule les autres coûts de sauvegarde en fonction de la stratégie de refacturation et utilise les entrées suivantes :

- Cost Per Backups : coût par sauvegarde (calculé à partir de la stratégie de refacturation).
- Cost per GB Retained : coût par gigaoctet stocké (calculé à partir de la stratégie de refacturation).
- Cost Per Restores : coût par restauration (calculé à partir de la stratégie de refacturation).
- Cost Per GB Restored : coût par gigaoctet restauré (calculé à partir de la stratégie de refacturation).
- Cost Per Tape : coût par bande utilisée pour la sauvegarde (calculé à partir de la stratégie de refacturation)

Refacturation du stockage

DPA permet la refacturation du stockage par coût de Go stocké, par coût de Go répliqué, et par snapshot.

Le coût par Go stocké utilise les entrées suivantes :

- Cost Based On : refacturation en fonction du stockage utilisé ou du stockage alloué
- Base Size : quantité d'espace de stockage de base allouée, en Go.
- Base Cost : prix unique pour le volume de base.
- Cost of Each Additional GB : tarification par Go une fois le volume de base dépassé.

Le coût par Go répliqué utilise les entrées suivantes :

- Base Size : quantité d'espace de stockage de base allouée, en Go.
- Base Cost : prix unique pour le volume de base.
- Cost of Each Additional GB : tarification par Go une fois le volume de base dépassé.

Les snapshots utilisent les entrées suivantes :

- Cost Per GB : prix par Go.

Une règle de refacturation vous permet de définir une valeur pour chacun de ces paramètres. DPA calcule le coût total pour un client en ajoutant chacun des différents éléments de coût. Par exemple, si vous voulez mettre en œuvre un modèle de refacturation dans lequel vous facturez 5 dollars pour chaque sauvegarde effectuée et 0,20 dollar pour chaque Go sauvegardé, vous pouvez définir les valeurs de ces champs dans la règle de refacturation sans définir aucune valeur pour les autres paramètres.

Vous attribuez les objets de clients de sauvegarde à un centre de coûts, ce qui permet à DPA de calculer les coûts de refacturation par centre de coûts. Il existe un centre de coûts par défaut pour les objets auxquels aucun centre de coûts n'a été attribué.

Vous pouvez créer plusieurs règles de refacturation et attribuer des règles distinctes à différents clients ou groupes de clients. Par exemple, si vous voulez calculer le coût de refacturation pour un groupe de clients de sauvegarde en fonction du nombre de sauvegardes effectuées et pour un autre groupe en fonction du nombre de bandes utilisées dans le cadre du processus de sauvegarde, vous pouvez créer deux règles de refacturation et les associer à chaque groupe de clients.

Stratégies et génération d'événements

Quand une politique d'analyse trouve une condition correspondante, DPA génère un événement. Tous les événements sont automatiquement consignés dans le datastore

DPA. Vous pouvez afficher tous les événements dans la section **Alerts** de la console Web.

Vous pouvez modifier les politiques pour :

- générer un e-mail ;
- exécuter un script ;
- envoyer un trap SNMP ;
- consigner un événement dans le log d'événements Windows.

Modification des règles dans les stratégies

Pour modifier toutes les règles d'une politique, accédez à **Policies** > **Analysis Policies** > **Edit** > **Edit Policy-based actions**.

Vous pouvez également modifier des actions pour chaque règle : Pour modifier les actions pour chaque règle :

Procédure

1. Accédez à **Policies** > **Analysis Policies** > **[sélectionnez une politique] et cliquez sur Edit**.
2. Sous Analysis Rules, sélectionnez le nom de la règle à modifier, puis cliquez sur **Edit Actions**.
3. Dans la fenêtre **Edit Actions**, assurez-vous que le bouton radio des actions basées sur la règle est sélectionné.
1. Vous pouvez aussi modifier ou remplacer toutes les règles d'une politique ou intervenir règle par règle dans la section Inventory. Ceci ne s'applique qu'aux rôles autorisés à modifier la politique.
4. Accédez à **Inventory** et sélectionnez l'objet.
5. Sélectionnez **Properties**.
6. Dans la fenêtre **Details** de l'objet, cliquez sur l'onglet **Policies**.
7. Cliquez sur **Edit Override Settings**.

   Edit Override Settings est disponible uniquement si le rôle dispose des privilèges correspondants. Dans le cas contraire, l'option est **View Settings**
8. Dans la fenêtre **Override Policy Settings** de l'objet, procédez aux changements souhaités, en intervenant règle par règle ou en utilisant une politique, puis cliquez sur **OK** lorsque vous avez terminé.

Résultats

Aide en ligne de Data Protection Advisor fournit des informations complémentaires sur la création, la modification ou la copie d'un modèle de règle d'analyse.

Paramètres permettant de générer des alertes à partir de scripts

Vous pouvez placer des scripts dans n'importe quel répertoire. Cependant, nous vous recommandons d'utiliser le répertoire `<install-dir>/services/shared/directory` car dans un environnement de clusters, les scripts doivent être placés en une seule opération. Si vous choisissez un emplacement différent, dans un environnement en cluster, vous devrez copier manuellement les scripts dans chaque serveur d'applications DPA.

Le tableau suivant décrit les paramètres du script à utiliser pour exécuter des actions.

Tableau 51 Paramètres de champ de script

Paramètre	Description :
Node	Nom du nœud auquel l'alerte s'applique.
Text	Message d'erreur textuel défini dans le groupe de règles.
Severity	Gravité de l'alerte (Critique, Erreur, Avertissement, Information).
Name	Nom de l'analyse ayant déclenché cette alerte.
Alert ID/Event ID	ID décrivant cette alerte de façon unique.
First occurrence	Horodatage indiquant l'heure à laquelle cette alerte a été déclenchée pour la première fois.
Last occurrence	Horodatage indiquant l'heure à laquelle cette alerte a été déclenchée pour la dernière fois.
Count	Nombre de fois que cette alerte a été déclenchée.
View	Nom de la vue à laquelle l'analyse est attribuée.
Node	Nom du nœud auquel l'analyse est attribuée.
Catégorie	Catégorie de la règle (valeurs possibles : Administrative, AssetManagement, CapacityPlanning, ChangeManagement, Compliance, Configuration, DataProtection, Execution, Performance, Provisioning, Recoverability, ResourceUtilization, SLA, Status, System, Troubleshooting).

Le tableau suivant décrit les arguments transmis à un script dans une action d'alerte.

Tableau 52 Arguments d'une alerte de script

Argument	Description :
$1	Nœud Événement.
$2	Message de l'événement.
$3	Gravité de l'événement (telle que définie dans les propriétés de l'analyse).
$4	Nom de l'analyse qui a déclenché l'événement.
$5	ID de l'alerte (unique pour cette exécution du script).
$6	ID de l'événement (unique pour cette alerte).
$7	Première occurrence (horodatage).
$8	Dernière occurrence.
$9	Nombre.

Tableau 52 Arguments d'une alerte de script (suite)

Argument	Description :
$10	Catégorie.
$11	Description de l'alerte.

Remarque

Si vous exécutez un script dans un environnement UNIX, vous devez encadrer les paramètres à 2 chiffres par des accolades : {xx}. Par exemple, `$ {11}`.

Modèle de règle

Une règle est un ensemble d'instructions utilisées par le moteur d'analyse DPA pour déterminer si une condition a été remplie et si une alerte doit être générée. Par exemple, la règle de remplissage du système de fichiers contient le groupe de règles qui permet de déterminer si des systèmes de fichiers risquent de dépasser le seuil à un certain moment.

Une tâche d'analyse utilise une règle pour effectuer une analyse et générer des alertes en fonction des informations de la base de données DPA. Lors de l'installation de DPA, plusieurs règles prédéfinies sont installées, qui permettent de surveiller des problèmes courants susceptibles de survenir dans l'environnement. Vous pouvez utiliser ces règles comme base d'implémentation des règles d'analyses. DPA fournit un éditeur de règle que vous pouvez utiliser pour créer des règles entièrement nouvelles.

Le terme *modèle de règle* est utilisé pour distinguer la définition de la règle de l'instance de la règle. Le modèle de règle définit la logique de la règle. Lorsqu'un modèle de règle est ajouté à une politique d'analyse, il devient une instance de règle (ou une règle) exécutée par le moteur d'analyse. Par ailleurs, lorsque des modèles de règles sont ajoutés à une politique, les utilisateurs peuvent spécifier des valeurs pour les paramètres. Cela permet de réutiliser les règles dans différentes politiques.

Par exemple

Une règle de niveau 1 peut générer une alerte lorsque l'espace disque est utilisé à 80 %. Une règle de niveau 2 peut générer une alerte lorsque l'espace disque est utilisé à 90 %. Ce comportement peut être géré à l'aide du modèle de règle qui utilise un paramètre d'utilisation.

Application de politiques

Les politiques peuvent être appliquées directement à un groupe ou un objet. Les politiques appliquées directement à un objet sont toujours prioritaires. Lorsqu'une politique est définie au niveau d'un groupe, les objets du groupe qui ne disposent pas de leur propre politique héritent de celle du groupe. Une bonne pratique consiste à appliquer la politique au niveau du groupe le plus élevé. Les politiques ne peuvent pas être appliquées aux Smart Groups.

Lorsqu'un objet est déplacé d'un groupe à un autre, la dernière politique appliquée est mise en œuvre. Par exemple, si un objet est déplacé du groupe A au groupe B, il hérite de la politique du groupe B.

Un administrateur ou tout utilisateur doté des privilèges de Edit Node peut appliquer une politique à un groupe ou un objet.

CHAPITRE 5

Désinstallation de DPA

Le présent chapitre contient les sections suivantes :

Désinstallation du logiciel

Cette section explique comment désinstaller DPA dans les environnements UNIX/Linux et Windows.

Procédure

1. Exécutez la commande suivante :

   <Répetoire_installation_DPA>/_uninstall/Uninstall_Data_Protection_Advisor

   Ajoutez `-i silent` à la commande pour une désinstallation en mode silencieux. Le programme de désinstallation ne demande aucune saisie.

Résultats

Lors de la désinstallation du datastore DPA, un avertissement s'affiche indiquant que le programme de désinstallation va supprimer les fonctions installées au cours de l'installation du produit, ainsi que la base de données.

Désinstallation à l'aide de la ligne de commande silencieuse

- Sur les machines UNIX/Linux, démarrez un shell de commande, accédez au répertoire _uninstall et entrez la commande suivante : **./Uninstall_Data_Protection_Advisor -i silent**
- Sur les machines Windows, entrez la commande suivante sur la ligne de commande : **Uninstall_Data_Protection_Advisor.exe -i silent**

Désinstallation via l'interface utilisateur Windows

Procédure

1. Sélectionnez **Start** > **Control Panel** > **Programs and Features.**
2. Sélectionnez **Data Protection Advisor** dans la liste des applications installées.

Désinstallation d'un agent uniquement

Il est impossible de désinstaller uniquement l'agent de l'installation du serveur d'applications DPA ou du serveur datastore.

Si vous souhaitez mettre à jour l'agent DPA, mettez-le à jour uniquement sur l'installation existante du serveur d'applications DPA ou du serveur datastore. Mises à niveau à la page 70 fournit des informations sur les mises à niveau.

CHAPITRE 6

Dépannage

Le présent chapitre contient les sections suivantes:

Dépannage de l'installation

L'agent DPA ne redémarre pas et ne s'enregistre pas après le changement de mot de passe de serveur DPA

Si l'agent DPA ne pas redémarre pas et ne s'enregistre pas une fois le mot de passe de serveur DPA modifié lors de l'installation, cela peut être dû au fait que le mot de passe de l'agent sur le serveur DPA a été modifié et que le mot de passe sur l'agent DPA n'a pas été modifié en conséquence.

Pour que l'agent DPA redémarre ou s'enregistre, définissez le mot de passe sur l'agent avec la même valeur que sur le serveur DPA. Pour plus d'informations, reportez-vous à la section Installation de l'agent DPA à la page 57.

Échec du démarrage du datastore DPA sur Linux après l'installation

Dans certaines circonstances, pour que le datastore démarre correctement, il est nécessaire de régler les paramètres du noyau du système exécutant le datastore DPA.

Si le datastore ne parvient pas à démarrer et que les erreurs consignées dans le fichier log de DPA référencent des segments de mémoire partagée, il peut se révéler nécessaire de régler les valeurs spécifiées dans le fichier suivant, selon les spécifications de votre système.

- Linux : essayez de régler les valeurs de SHMMAX et SHMMIN dans /etc/sysctl.conf

Échec du démarrage de la console Web DPA sur Windows Server 2012

En cas d'échec du démarrage de la console Web DPA sur Windows Server 2012, vérifiez les éléments suivants :

- La configuration de sécurité renforcée d'Internet Explorer (IE ESC) arrête le démarrage de la console Web DPA. N'arrêtez pas la notification du bloc en désactivant l'option Continue to prompt when website content is blocked car DPA ne dépassera jamais le stade Démarrage des services. Veuillez patienter. La solution consiste à désactiver la configuration IE ESC.
- Internet Explorer dans Windows Server 2012 ne prend pas en charge les systèmes Flash. La solution consiste à activer Expérience utilisateur dans Windows Server 2012.

Réglage de la mémoire après installation

Lorsque les services d'application et de datastore DPA sont installés au départ, ils ajustent automatiquement les paramètres de la mémoire en fonction de la RAM de votre système. Si par la suite vous augmentez ou réduisez la quantité de RAM installée sur l'hôte, vous devez exécuter la commande `tune` pour que les paramètres de mémoire DPA soient ajustés correctement.

Lorsque vous exécutez la commande `tune`, vous devez spécifier la quantité de RAM installée sur l'hôte. Par exemple, si la mémoire de serveur d'applications est passée à 64 Go et que la mémoire du datastore est passée à 32 Go, vous exécuterez les commandes suivantes :

- Sur le serveur d'applications : **`dpa app tune 64GB`**

- Sur le serveur de datastore : `dpa ds tune 32GB`

DPA se configure automatiquement pour utiliser une partie de la quantité de mémoire spécifiée dans la commande.

Messages d'erreur lors des mises à niveau

Si une erreur se produit lors du processus de mise à niveau, le serveur DPA s'arrête. Cette erreur peut se produire dans les circonstances suivantes :

- Erreurs dans les scripts de mise à niveau SQL
  - Résultat : le serveur s'arrête et se bloque.
  - Action suggérée : contactez le support technique EMC.
- Erreurs lors de la mise à niveau des métadonnées du système ; par exemple, les rapports système, les modèles de règle
  - Résultat : le serveur s'arrête, mais vous pouvez poursuivre la mise à niveau.
  - Action suggérée : vous pouvez ignorer ce message et poursuivre la mise à niveau du serveur DPA. Toutefois, le système DPA peut être instable. Si vous décidez de ne pas poursuivre la mise à niveau du serveur, contactez le support technique d'EMC
- Erreurs lors de la mise à niveau de données personnalisées ; par exemple, les règles d'analyse personnalisées
  - Résultat : un message d'erreur indiquant le problème, s'affiche.

```
Suggested action: You can disregard this message and continue
with the DPA server upgrade. However, you should expect the
custom rule that failed to upgrade not to work. An error is
recorded in the log file.
```

Fichiers log

Les fichiers log fournissent des informations importantes lors de la résolution des problèmes.

Remarque

La section suivante décrit les emplacements de fichier log pour une installation standard de DPA. Si le répertoire d'installation par défaut a été modifié au cours de l'installation, l'emplacement du répertoire du log sera différent.

Par défaut, les fichiers log contiennent les avertissements, les messages d'erreur et des informations. Il se peut qu'ils ne fournissent pas suffisamment d'informations pour résoudre les problèmes complexes.

Modification du niveau de détail du fichier log par défaut

Accédez à **Admin** > **System** > **Configure System Settings**.

Affichage du fichier log d'installation

Le fichier `Data_Protection_Advisor_Install_[two-digit date]_[two-digit month]__[year]_[two-digit hour]_[two-digit minute]_[two-digit seconds].log` est généré lors de l'installation et contient tous les messages

de fichier log. Dans le cas d'installations réussies, ce fichier se trouve dans le répertoire d'installation (par exemple, `/opt/emc/dpa/_install`). Dans le cas d'installations ayant échoué sur les plates-formes Unix, le fichier se trouve à la racine du lecteur système. Sur les plates-formes Windows, le fichier se trouve sur le bureau.

Affichage des fichiers log du serveur

DPA génère les fichiers log du serveur aux emplacements suivants :

- UNIX : `/opt/emc/dpa/services/logs`
- Windows : `C:\Program Files\EMC\Data Protection Advisor \services\logs`

Fichiers log du serveur

L'emplacement par défaut des fichiers log suivants est`<install_dir>\services \logs\ .`

- `Server.log` — Contient tous les commentaires du fichier log, générés à partir du serveur d'applications DPA
- `actions.log`—Contient les actions réussies du moteur d'analyse
- `reportengine.log` — Contient tous les commentaires du fichier log, générés à partir du moteur de rapports DPA
- `listener.log` — Contient tous les commentaires du fichier log, générés à partir du Listener DPA associé au serveur qui reçoit et traite les données de l'agent

Affichage des fichiers log de l'agent

Les fichiers log de l'agent sont générés aux emplacements suivants :

- UNIX : `/opt/emc/dpa/agent/logs`
- Windows : `C:\Program Files\EMC\Data Protection Advisor\agent \log\agent.log`

Gestion des fichiers log

Lorsqu'un fichier log atteint sa taille maximale et que le répertoire de fichiers log est plein, DPA supprime le fichier log le plus ancien pour ce processus et en créé un nouveau. Vous pouvez modifier la taille maximale des fichiers log ainsi que le nombre maximum de fichiers log. Le cas échéant, vous pouvez également modifier l'emplacement des fichiers log.

Activation de la méthode alternative de rotation des logs sur des machines virtuelles exécutant Windows

Les machines virtuelles exécutant Windows présentent un problème connu : la rotation des logs ne s'effectue pas à cause du verrouillage du fichier. Pour corriger ce problème, activez la méthode alternative de rotation des logs. Cette opération modifie la manière dont les logs sont utilisés. Le log le plus ancien n'est pas le fichier `agent.log`, il correspond au log ayant le numéro le plus élevé. Cela est lié au problème DPA-24288.

Procédure

1. Créez le registre de chaîne suivant :

HKLM\SOFTWARE\EMC\DPA\Agent\ALTLOGROTATE

2. Définissez la valeur sur *true*.

Données de mémoire erronées dans le fichier log du programme d'installation

Les données concernant la mémoire disponible et la mémoire totale indiquées en haut des fichiers log d'installation sont erronées. Les données de mémoire disponible et de mémoire totale correctes se trouvent un peu plus bas dans le fichier log, sous `STDERR ENTRIES`.

Les données de la mémoire totale corrigée indiquées sous `Executing IAUpdatePostgesconfFile: [INFO]` font référence aux données utilisées pour le service de datastore DPA.

Exécution d'une demande d'agent DPA en mode débogage à l'aide de la console Web DPA

La demande d'agent DPA en mode débogage, parfois appelée *modtest*, est un outil de support. Si vous rencontrez des problèmes avec l'une des valeurs par défaut de la collecte de données, un ingénieur du support technique EMC peut vous demander d'exécuter la demande d'agent en mode débogage à partir de la console Web DPA. Vous pouvez exécuter la demande d'agent DPA en mode débogage, puis télécharger le fichier ZIP directement à partir de la console Web DPA, sans avoir à passer par le serveur DPA pour le récupérer, et envoyer ce fichier ZIP pour analyse. La demande d'agent en mode débogage exécute la demande sélectionnée, ainsi qu'elle récupère la sortie et les messages de journal, au niveau journal de débogage, puis stocke par défaut le rapport XML dans un fichier ZIP à l'emplacement suivant : `<DPA_HOME>\services\shared\modtests`, où `<DPA_HOME>` est l'emplacement de l'installation DPA.

Tenez compte des points suivants lorsque vous exécutez la demande d'agent DPA en mode débogage à l'aide de la console Web DPA :

- Le test ne peut pas être exécuté si la demande de collecte est désactivée.
- Le test ne peut pas être exécuté si la demande de collecte ne s'applique pas à l'objet.
- Si vous utilisez Google Chrome, vous devez modifier le paramètre de sécurité par défaut de l'adresse URL et le positionner sur faible :
  Rendez-vous sur **Sites de confiance**, ajoutez l'URL dans la liste Sites de confiance, puis définissez la sécurité sur **faible**.

Procédure

1. Dans la console Web, sélectionnez **Inventory** > **Object Library**.
2. Dans Object Library, sélectionnez le serveur DPA sous **All hosts**.
3. Dans la fenêtre des détails de l'hôte, sélectionnez l'onglet **Data Collection** > .
4. Dans le champ **Data Collection**, sélectionnez Request.
5. Cliquez avec le bouton droit de la souris sur **Run** et sélectionnez **Run in Debug**.
6. Dans la fenêtre **Run in Debug - host/status**, sélectionnez les informations d'identification et les options de données.
7. Cliquez sur **Close** pour fermer la boîte de dialogue qui apparaît et qui confirme que le test est en cours d'exécution.

8. Cliquez sur **History** pour afficher les tests collectés. Les lignes mises en surbrillance orange indiquent les résultats d'une demande d'agent DPA en mode débogage.
9. Cliquez sur le résultat du test. Si l'écran de connexion Sécurité de Windows s'affiche, saisissez vos informations d'identification de serveur DPA, puis cliquez sur **OK**.
10. Pour accéder aux tests correctement collectés, allez à `<DPA_HOME>\services\shared\modtests`.

    Si vous utilisez un navigateur Web à distance, vous pouvez télécharger un lien vous permettant de transférer le fichier zip sur votre machine (où se trouve réellement le navigateur) si vous examinez l'historique de la demande et cliquez sur la ligne modtest orange.

Programme de suppression modtest par défaut

DPA supprime chaque semaine les fichiers modtest sur le serveur DPA, chaque dimanche à 4h00 du matin. DPA supprime tous les fichiers de résultats de test antérieurs à sept jours. Ce programme n'est pas configurable.

Générer un bundle de support

L'option Generate Support Bundle est un outil de support. Pour plus d'informations, reportez-vous à la section Generate Support Bundle à la page 101.

Résolution des problèmes de collecte des données

Cette section décrit les étapes à suivre pour diagnostiquer des problèmes lorsque vous essayez de recueillir les données. Imaginons le scénario suivant :

- DPA a été correctement installé.
- Le Discovery Wizard a été exécuté avec succès pour créer l'objet à surveiller.
- Les demandes ont été attribuées à l'objet et l'agent a été rechargé.
- Suffisamment de temps (15 minutes) s'est écoulé pour permettre à l'agent de recueillir les données.
- Un rapport approprié a été exécuté et ne renvoie aucune donnée lorsque des données doivent exister pour l'objet.

Collecte des données de résolution des problèmes : premières actions

Examinez les erreurs renvoyées par le rapport Agent Errors et prenez des mesures correctives si cela est possible (par exemple, corrigez un problème d'authentification).

Procédure

1. Assurez-vous que la période de temps sélectionnée pour le rapport est correcte.
2. Assurez-vous que les demandes appropriées ont été attribuées à l'objet.

   Sélectionnez **Inventory** > **Object Library** > **[sélectionnez un nœud]** > **Data Collection**. Vérifiez que les demandes sont correctement configurées.

3. Exécutez à nouveau la demande.

Résolution des problèmes de collecte des données Actions suivantes

Procédure

1. Si aucune erreur pouvant être résolue par l'agent n'a été signalée, sélectionnez **Admin** > **System**, cliquez sur **Configure System Settings** et vérifiez les paramètres de l'agent de collecte d'informations.
2. Si l'état indique que l'agent est actif, vérifiez que le processus est actif sur le système d'exploitation sur lequel l'agent est installé.
3. Exécutez les rapports de log de l'agent dans la console Web, suivis du rapport Agent Status et du rapport Data Collection History.
4. Exécutez à nouveau le rapport. Si le rapport continue à n'afficher aucune donnée, ouvrez le log de l'agent et recherchez les problèmes éventuels. Par exemple, une valeur incorrecte a été saisie pendant l'installation de l'agent. Fichiers log à la page 265 décrit comment afficher les fichiers log.

Préparation d'un fichier log à envoyer à EMC Support Desk

Procédure

1. Définissez le niveau de consignation du processus sur **Debug** dans System Settings, tel qu'indiqué dans la section Fichiers log à la page 265.
2. Arrêtez le processus de l'agent.
3. Accédez au répertoire dans lequel le fichier log est enregistré. Renommez ou supprimez tout fichier log existant pour le processus.
4. Redémarrez le processus.

   Le redémarrage d'un agent charge à nouveau toutes les demandes attribuées à cet agent et commence la routine de collecte des données. Cela garantit que toutes les demandes ont été tentées. Le fait de démarrer un nouveau fichier log supprime la nécessité de rechercher un problème dans des fichiers log inutilement longs.

5. Sélectionnez **Inventory** > **Object Library** > **[sélectionnez un nœud]** > **Data Collection**, puis sélectionnez **History**.

   Vous pouvez également exécuter un rapport de type Agent History.
6. Exécutez à nouveau la demande pour confirmer que les données ne sont pas collectées.
7. Sélectionnez **System Settings** > **Log Level** et définissez les paramètres sur **Info**.
8. Effectuez une copie du log pour l'envoyer à l'EMC Support Desk.

Découverte de client/stockage pour la résolution de problèmes d'analyse de la réplication

Cette section décrit les étapes que vous pouvez suivre pour diagnostiquer les problèmes lorsque vous essayez de configurer des baies de stockage VNX Block/CLARiiON ou Symmetrix pour une analyse de réplication. Imaginons le scénario suivant :

- DPA a été correctement installé.

- Le serveur DPA et l'hôte de baie de stockage répondent aux exigences, comme indiqué dans le *Guide de compatibilité de Data Protection Advisor*.
- Solutions Enabler a été installé correctement.

Découverte de client/stockage à l'aide de l'exécution à distance

Le tableau suivant décrit les problèmes pouvant être rencontrés lors de la tentative de découverte de clients ou de stockage à distance, autrement dit sans agent DPA, ainsi que les solutions proposées.

Tableau 53 Problèmes relatifs à la découverte de client/stockage et solutions associées

Problème	Solutions
Échec de la découverte de client : aucune authentification n'a été définie ou la connexion est impossible.	• Créez des informations d'identification dans DPA (Admin > System > Manage Credentials) et attribuez-les au client. • Vérifiez que le nom d'utilisateur et le mot de passe fournis avec les informations d'identification permettent de se connecter au client. • Assurez-vous que su ou sudo n'ont pas besoin de se connecter et, le cas échéant, que les paramètres corrects sont fournis dans les informations d'identification.
Échec de la découverte de client : la connexion au client via RPC a échoué ou la session de connexion spécifiée n'existe pas.	• Vérifiez que le nom d'utilisateur et le mot de passe fournis avec les informations d'identification permettent de se connecter au client. • Assurez-vous que vous avez fourni le nom d'utilisateur avec le nom de domaine : `<domain>\<username >` pour les ordinateurs distants, <computer name> \<username> pour les ordinateurs locaux. Dans la plupart des cas, `localhost \<username>` peut être utilisé. • Vérifiez que l'hôte est accessible à partir du serveur DPA par l'intermédiaire du partage d'administration : \\hostname \Admin$ • Si l'erreur persiste après avoir tenté toutes les actions citées précédemment, modifiez la valeur Log on as du service de serveur DPA entre le système local et tout autre utilisateur disposant de privilèges d'administration. Il est également possible de définir un administrateur local.
Échec de la découverte de client : la connexion au client via RPC a échoué. Le chemin réseau est introuvable.	• Vérifiez que le nom du client, l'IP ou l'alias est correctement défini et accessible depuis le serveur DPA.

Tableau 53 Problèmes relatifs à la découverte de client/stockage et solutions associées (suite)

Problème	Solutions
	• Vérifiez que l'hôte est accessible à partir du serveur DPA par l'intermédiaire du partage d'administration : `\\hostname\Admin$` Si le partage est inaccessible, vérifiez qu'il n'est pas bloqué par un pare-feu.
Échec de la découverte de client : l'utilisateur ne dispose pas des privilèges permettant d'accéder aux informations de mappage des périphériques.	• Respectez la configuration système requise pour les autorisations d'exécution à distance. • Attribuez à un utilisateur un accès administrateur aux informations d'identification. • Vérifiez que l'utilisateur qui se connecte au client dispose de privilèges « écriture et exécution » sur le chemin /var/tmp. (Unix)
Échec de la découverte de client : l'envoi du fichier de découverte au client via SCP a échoué. ou l'envoi du fichier de découverte au client via FTP a échoué.	Recherchez de l'espace disque disponible dans `/var/tmp`.
Échec de la découverte de client : Error (977). Overlapped IO operation in progress.	Vérifiez qu'aucun logiciel antivirus n'est installé sur l'hôte. En effet, un logiciel antivirus peut bloquer le fonctionnement d'irxsvs.exe. Désactivez le blocage par l'antivirus en autorisant le fichier irxsvs.exe dans le logiciel antivirus.
La découverte du client échoue et affiche l'erreur suivante : <client_name> irx errMsg: Unable to connect host:<client_name> with user:<domain>\<username> using RPC irx output: Error (1203): No network provider accepted the given network path.	Assurez-vous que les services suivants s'exécutent : serveur, navigateur de l'ordinateur et poste de travail.
Lorsque vous utilisez sudo, la demande de configuration de l'hôte peut ne pas renvoyer d'informations sur un groupe de volumes sur les hôtes AIX et afficher le message suivant : SymMapVgShow exited with code 161 (SYMAPI_C_VG_NOT_AVAILABLE) SessionId: 0 - for VG:<vg_name> with type: 2(AIX LVM) VolumeGroup information will not be parsed.	Ce problème se produit uniquement lorsque les informations d'identification sont configurées pour utiliser sudo. Ajoutez la ligne suivante au fichier sudoers : Defaults env_keep += "ODMDIR"

Découverte de client ou de stockage avec agent

Le tableau suivant décrit les problèmes susceptibles de se produire lors de la tentative de découverte de clients ou de stockage à l'aide de DPA et leurs solutions.

Tableau 54 Problèmes et solutions pour la découverte du client ou de stockage avec agent

Problème	Solution
La demande de découverte du client utilise l'exécution à distance au lieu d'utiliser l'agent installé.	Assurez-vous que l'agent est installé sur l'hôte. Assurez-vous que le serveur DPA est défini en tant que contrôleur de l'agent. Redémarrez le service Agent.

Découverte de client/stockage : problèmes généraux

Le tableau suivant décrit les problèmes généraux susceptibles de se produire lors de la tentative de découverte de client ou de stockage à l'aide de DPA.

Tableau 55 Problèmes généraux et solutions concernant la découverte de client/stockage

Problème	Solution
La découverte de client s'est achevée avec les avertissements suivants : Failed to discover application storage objects for application <application_name> on client <client_name>.	• Vérifiez que l'application est en cours d'exécution et disponible pour la connexion. • Vérifiez que l'utilisateur configuré dans les informations d'identification DPA dispose des privilèges lui permettant d'interroger les données système de l'application.
Échec de la découverte du client : connexion à une adresse IP impossible.	• Vérifiez que le port 25011 ou le port 135 du collecteur proxy Windows n'est pas bloqué par un pare-feu.
La découverte de client s'est achevée avec les avertissements suivants : Home directory was not found for application.	Sélectionnez **Admin** > **System** > **Manage Credentials**. Cliquez sur **Edit** pour modifier les informations d'identification.
Type de système de fichiers non pris en charge : <filesystem_name>.	DPA ne prend pas en charge ce type de système de fichiers. Pour éviter cet avertissement lors de la prochaine découverte de client, vous pouvez ignorer la découverte de ce système de fichiers. DPA n'affichera pas les données de restauration pour ce système de fichiers.

Tableau 55 Problèmes généraux et solutions concernant la découverte de client/stockage (suite)

Problème	Solution
Échec de la découverte de client ; l'erreur suivante s'affiche : Please verify that you have enough disk space and write permission. ou Failed to unpack file on client <client_name>.	Assurez-vous que vous disposez de suffisamment d'espace disque dans le système de fichiers racines de l'hôte en fonction des exigences du système.
La découverte de client s'est achevée avec les avertissements suivants : Can't find or no permission to execute file <home_dir>.	• Vérifiez que le répertoire `<home_dir>` qui a été découvert est présent sur le client. • Vérifiez que le fichier sqlplus stocké dans le répertoire de base qui a été découvert dispose des autorisations suffisantes pour être exécuté par DPA.
La découverte de client s'est achevée avec l'erreur suivante : Timeout waiting for agent response on client <client_name>.	1. Dans DPA, sélectionnez **Admin** > **System** > **Configure System Settings** et cliquez sur **Select Server**. 2. Modifiez le paramètre Timeout(s) en remplaçant la valeur par défaut 120 par une valeur supérieure. Autre solution : Vérifiez que deux cartes réseau sont activées sur le serveur DPA et que le client accède à ces deux cartes. Si le client ne parvient pas à accéder à l'une des cartes, désactivez la carte réseau à laquelle il ne peut pas accéder.
Lors de la connexion à ECC 6.1, la découverte de client s'est achevée avec l'erreur suivante : Erreur : l'importation de clients pour w2k3-96-52.dm1nprlab.com s'est terminée avec des erreurs. Vérifiez les messages d'erreur précédents pour plus d'informations. Connexion impossible (connexion refusée).	Exécutez un fichier batch contenant les commandes suivantes : `%ECC_INSTALL_ROOT%\tools\JRE\Nt \latest\bin\java -cp %ECC_INSTALL_ROOT%\ECCAPIServer \class;%ECC_INSTALL_ROOT% \ECCAPIServer\ecc_inf\exec \eccapiclient.jar; com.emc.ecc.eccapi.client.util.EccA piPopulateRandomPassword ApiClient` Le paramètre `classpath` supplémentaire est uniquement requis si la commande n'est pas utilisée à partir du répertoire de classes ECC.
La découverte de client ne résout pas correctement les LUN sur VFMS sur ESX 4.1. Lorsque vous essayez d'établir une corrélation entre des périphériques virtuels et le stockage	Configurez correctement les DNS sur l'ESX ou ajoutez le nom et l'adresse IP de la machine virtuelle dans le fichier des hôtes ESX.

Tableau 55 Problèmes généraux et solutions concernant la découverte de client/stockage (suite)

Problème	Solution
distant sur lequel ils résident, et que l'ESX hôte de la machine virtuelle ne peut pas résoudre le nom de la machine virtuelle (configuration DNS), la corrélation échoue et les périphériques virtuels sont affichés en tant que périphériques locaux.	
L'importation de la demande d'information CLARiiON échoue et affiche le message d'erreur suivant : "An error occurred while data was being loaded from a Clariion ClarEventGet exited with code 3593 (SYMAPI_C_CLARIION_LOAD_ERROR) "	Exécutez la commande `SYMCLI` sur l'hôte SE pour ce CLARiiON : symcfg sync -clar

Le délai de demande de configuration de l'hôte dépasse 60 minutes	Modifiez la valeur `TIMEOUT` pour qu'elle soit supérieure à 3600, par exemple 7200, dans le fichier `services/remotex/deploy/<platform>/apolloreagent.ini`, où *<platform>* correspond à l'hôte sur lequel le délai de demande a été dépassé et non au serveur DPA :
	`<REARGS>`
	`<LOGFILE>apolloreagent.log</LOGFILE>`
	`<LOGLEVEL>Info</LOGLEVEL>`
	`<WORKINGDIR>.</WORKINGDIR>`
	`<TIMEOUT>7200</TIMEOUT>`
	`</REARGS>`

Synchronisation incorrecte des heures associées aux points de restauration

S'il existe une différence d'heure entre le serveur DPA et la baie de stockage surveillée, les points de restauration peuvent s'afficher avec des heures qui ne correspondent pas aux heures attendues. Par exemple, un administrateur système exécute un point de récupération à 2h00, mais le point de restauration s'affiche à 4h00 dans DPA.

Les demandes de découverte ont une option Time Offset qui prend en compte les écarts de temps et permet aux points de récupération de s'afficher avec des heures cohérentes. Vous devez calculer le décalage exact entre le serveur DPA et l'hôte de baie de stockage.

Dans les instructions suivantes, « hôte Solutions Enabler » désigne l'hôte DPA auquel la demande SYMAPI/CLARAPI Engine Discovery a été attribuée.

Le décalage de temps est calculé en secondes.

Synchronisation des heures incorrectes pour les points de restauration sur VNX/CLARiiON

Pour calculer le décalage de temps entre le VNX/CLARiiON et le serveur DPA :

Procédure

1. Demandez l'heure de VNX/CLARiiON à l'aide de la commande navicli `getsptime`.
2. En même temps, demandez l'heure de l'hôte Solutions Enabler.
3. Si l'heure de l'hôte Solutions Enabler et l'heure du serveur DPA sont identiques (même fuseau horaire) :

   Décalage de temps = Heure de l'hôte Solutions Enabler - Heure de VNX/CLARiiON.

4. Sinon, si l'heure de l'hôte Solutions Enabler et l'heure du serveur DPA sont différentes :

   Décalage de temps = (Heure du serveur DPA - Heure de l'hôte Solutions Enabler) - Heure de VNX/Clariion.

5. Définissez le décalage de temps de la demande. Configuration du décalage de temps à la page 275 fournit des informations à ce sujet.

Synchronisation des heures incorrectes pour les points de restauration sur Symmetrix

Pour calculer le décalage de temps entre l'hôte Symmetrix et le serveur DPA :

Procédure

1. Demandez l'heure du serveur DPA.
2. En même temps, demandez l'heure de l'hôte Solutions Enabler.
3. Si l'heure de l'hôte Solutions Enabler et l'heure du serveur DPA sont différentes :

   Décalage de temps = Heure du serveur DPA - Heure de l'hôte Solutions Enabler.

4. Sinon, il n'est pas nécessaire de définir un décalage de temps pour l'hôte Symmetrix.
5. Définissez le décalage de temps de la demande.Configuration du décalage de temps à la page 275 fournit des informations à ce sujet.

Configuration du décalage de temps

Une fois que vous avez calculé le décalage de temps, définissez la valeur pour la demande. Pour définir la valeur de décalage de temps :

Procédure

1. Sélectionnez **Inventory** > **Object Library** > **[sélectionnez l'hôte Solutions Enabler]** > **Data Collection**.
2. Sélectionnez la demande pertinente et cliquez sur **Edit**.
3. Définissez le décalage de temps que vous avez calculé pour **Client-server Time Difference** (en secondes ou en minutes).
4. Cliquez sur **Apply**.

Résolution des problèmes d'échec de génération des rapports

Si vous utilisez Internet Explorer et que la génération des rapports s'interrompt lorsque vous les enregistrez et que le message `Please wait while generating`

`report` s'affiche, il se peut que l'option XMLHTTP ne soit pas activée. Pour activer l'option XMLHTTP :

Cela est lié au DCE-1546.

Procédure

1. Accédez à **Internet Options** > **Advanced**
2. Faites défiler la liste jusqu'à **Security** puis sélectionnez **Enable Native XMLHTTP Support** et cliquez sur **OK.**

Résolution des problèmes de création de rapports ou de publication

Si les rapports planifiés ne sont pas générés, ou s'ils sont générés mais ne sont pas publiés, procédez comme suit :

- S'il s'agit d'un rapport personnalisé, vérifiez que le modèle de rapport a été conçu correctement dans la zone **Run Reports**.
- Vérifiez que le modèle de rapport s'exécute correctement dans la zone **Run Reports**.
- Vérifiez que modèle de rapport a bien été sauvegardé (exporté) au format désiré.
- Consultez les erreurs et avertissements sur les rapports planifiés dans le fichier `server.log`.

Si ces étapes ne vous permettent pas de résoudre le problème, contactez le support technique EMC.

Synchronisation de l'horloge du système

Dans le cadre du processus d'authentification de l'utilisateur, DPA a besoin que l'heure de l'horloge du système de la machine client et celle du serveur ne diffèrent pas de plus d'une minute. Si les heures des horloges ne sont pas synchronisées, le message d'erreur suivant s'affiche :

```
User Authentication failed due to the times on the client and
server not matching. Ensure that the times are synchronized.
```

Pour résoudre ce problème, assurez-vous que les heures des horloges système du client et du serveur sont synchronisées.

Il est conseillé d'utiliser le NTP pour synchroniser le serveur DPA ainsi que tous les hôtes de l'agent DPA. C'est une opération indispensable pour assurer la précision de la collecte des données.