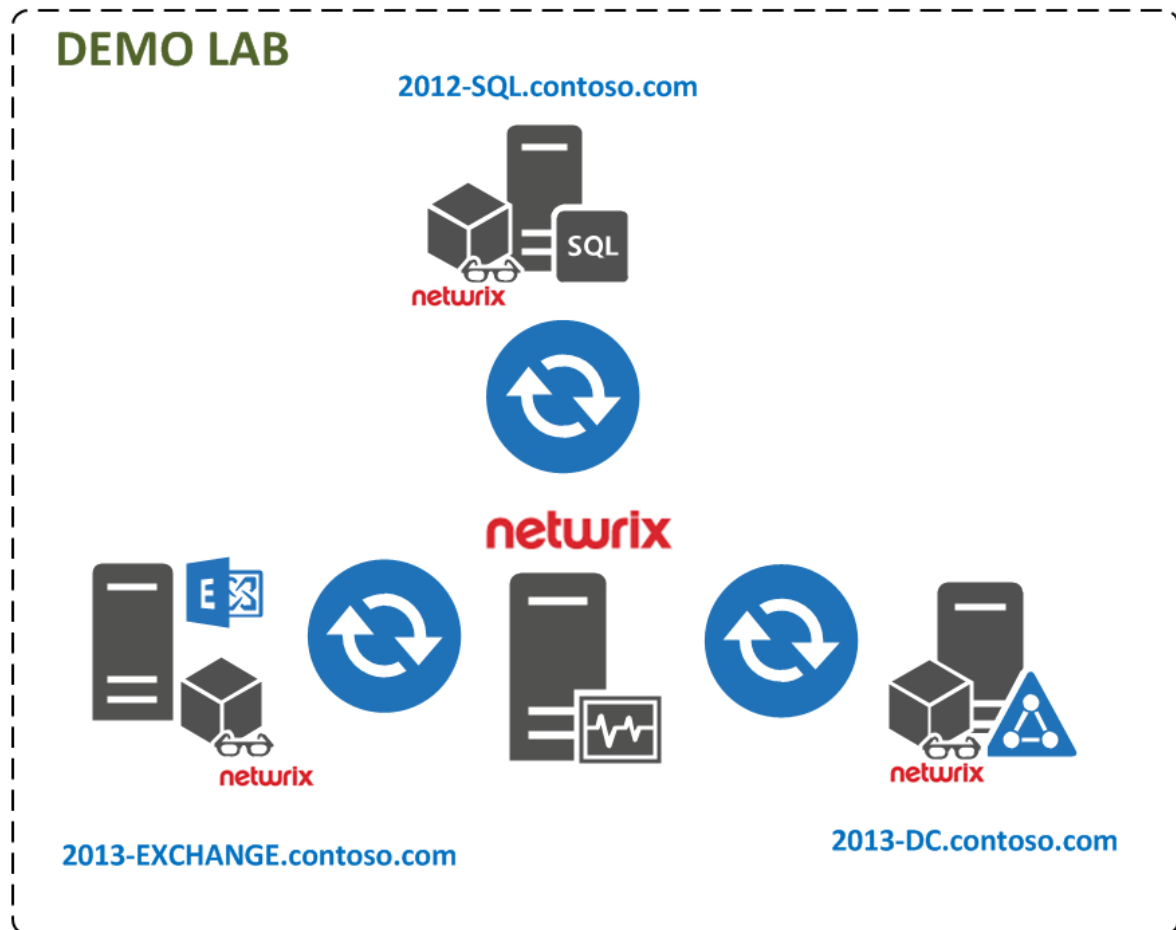


# Sommaire

---

1.	SCHEMA GLOBAL DU LAB .....	2
2.	INSTALLATION DE NETWRIX AUDITOR 6.5.....	3
3.	CONFIGURATION DE NETWRIX AUDITOR 6.5 .....	7
4.	CONSEILS EN CAS D'UNE ANALYSE EN ECHEC .....	22
5.	SCENARIO 1 : PRESENTATION DU REPORTING LORS DE LA CREATION D'OBJETS ACTIVE DIRECTORY .....	29
6.	SCENARIO 2 : INVESTIGATION SUR LA SUPPRESSION D'OBJETS ACTIVE DIRECTORY PUIS RESTAURATION .....	31
7.	ETENDUES DES POSSIBILITES AVEC LA SOLUTION NETWRIX AUDITOR.....	37
8.	BILAN.....	38

## 1. SCHEMA GLOBAL DU LAB



## 2. INSTALLATION DE NETWRIX AUDITOR 6.5

1

[Home](#) > [Products](#) > [Netwrix Auditor](#) > [Free Trial](#)

### Netwrix Auditor Free Trial Download

Please select what system(s) you need to audit:

- ☒ Active Directory
- ☐ Exchange
- ☐ File Servers
- ☐ SharePoint
- ☐ SQL Server
- ☐ VMware
- ☐ Windows Server
- ☐ All of the above

[Start the Download](#)

Télécharger la version d'essai de Netwrix Auditor pour Active Directory à cette adresse :

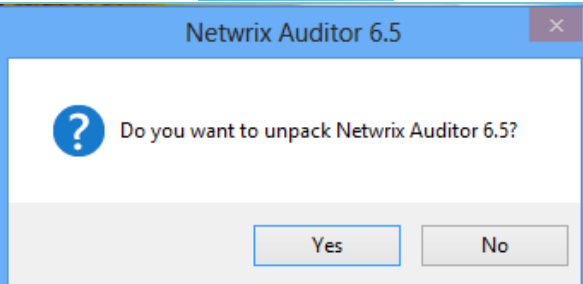
<http://www.netwrix.com/requeste.html?product=CRsuite>

2



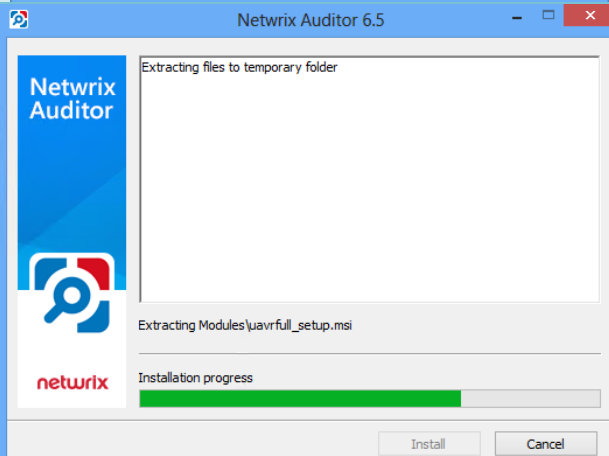
Copier le Setup d'installation sur le poste d'administration où va être installé la console Netwrix Auditor et exécuter le.

3



Ensuite, cliquer sur **Yes**.

4



L'extraction des fichiers dure pendant quelques secondes.

5

A partir de la console d'installation, il est possible de parcourir les différentes présentations et documentations techniques des divers modules de Netrix Auditor 6.5.

Cliquez ensuite sur **Install**.

6

A cette étape il manque le composant .Net Framework 3.5. Si vous avez accès à internet sur votre machine cliqué sur **Download and Install this feature**.

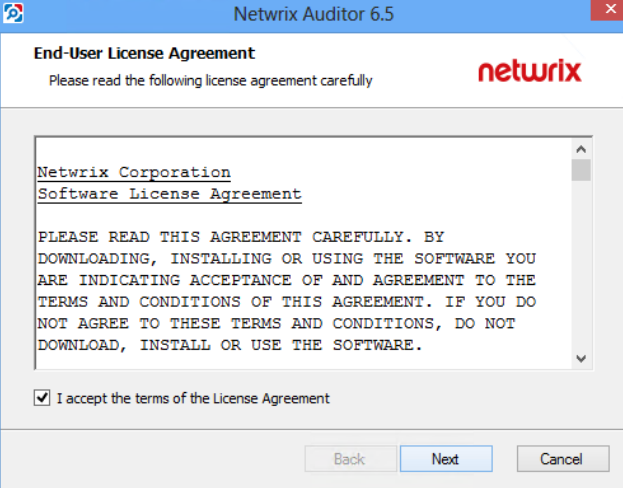
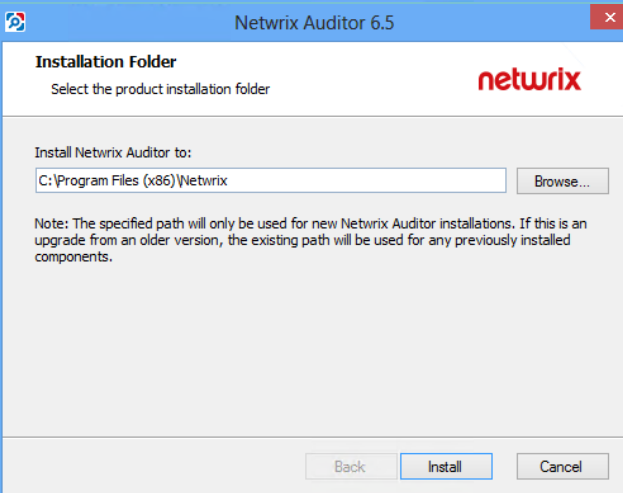
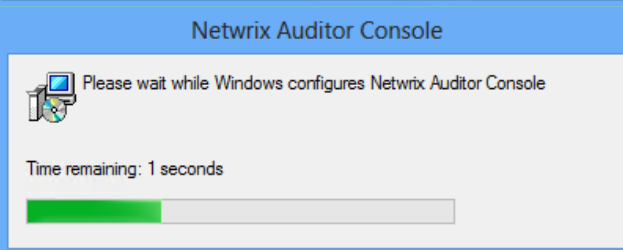
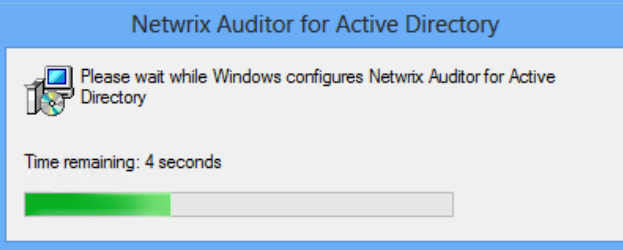
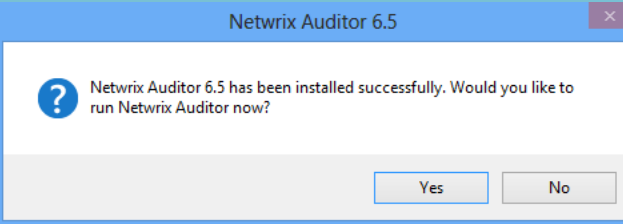
7

Dans le cas où votre poste d'administration n'a pas accès à internet, insérer l'image disque du système d'exploitation (dans mon cas : Windows 8) puis ouvrir une invite de commande en administrateur et taper :

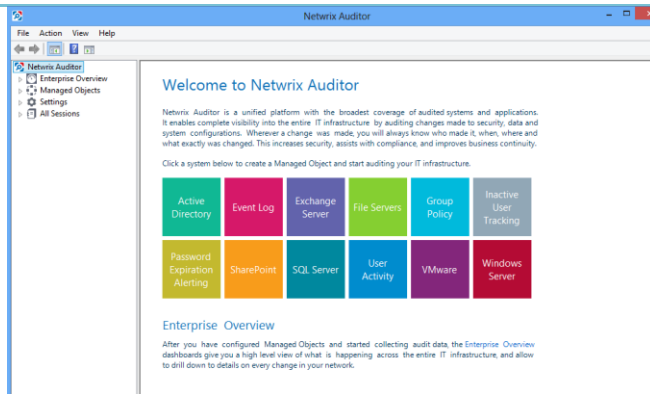
**DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:d:\sources\sxs** (mon lecteur cd ayant comme lettre D: sinon changer la lettre après /Source:x:)

8

Relancer à nouveau l'installation.

9		<p>Cocher :</p> <p><b>I accept the terms of the License Agreement</b></p> <p>Et cliquer sur <b>Next</b>.</p>
10		<p>Indiquer le chemin d'installation (en allant sur Browse.. si vous souhaitez changez le chemin par défaut) des binaires puis cliquer sur <b>Install</b>.</p>
11		<p>L'installation des différents composants débutent ..</p>
12		<p>Le temps d'installation dépend de s caractéristiques de la machine.</p>
13		<p>Après 10 minutes d'installation, on vous propose d'ouvrir la console Netwrix Auditor. Cliquez sur <b>Oui</b>.</p>

14

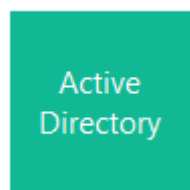


L'installation est terminée et la console s'est correctement lancée.

Passons à l'étape de configuration de Netwrix pour Active Directory.

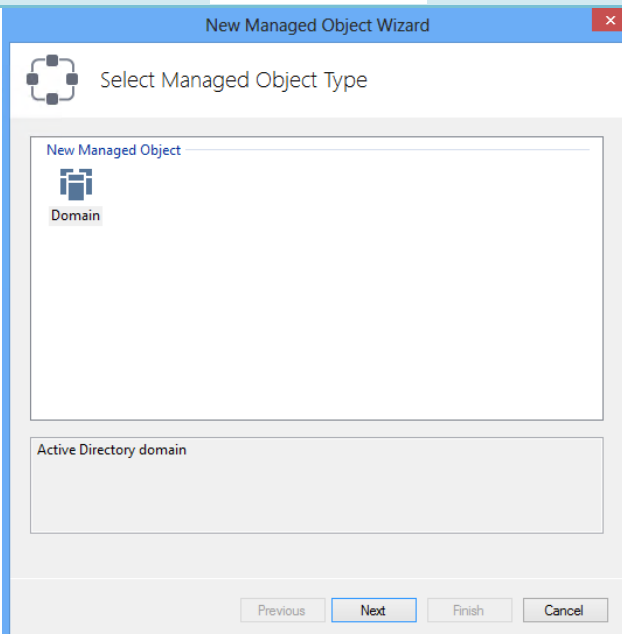
### 3. CONFIGURATION DE NETRIX AUDITOR 6.5

1



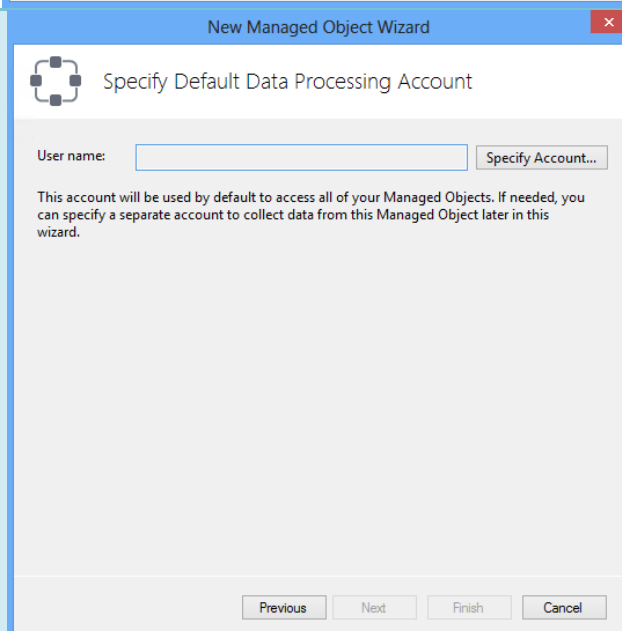
Il suffit de cliquer sur l'image Active Directory pour exécuter le setup de configuration.

2



A l'étape *Select Managed Object Type*, Cliquer sur **Next**.

3

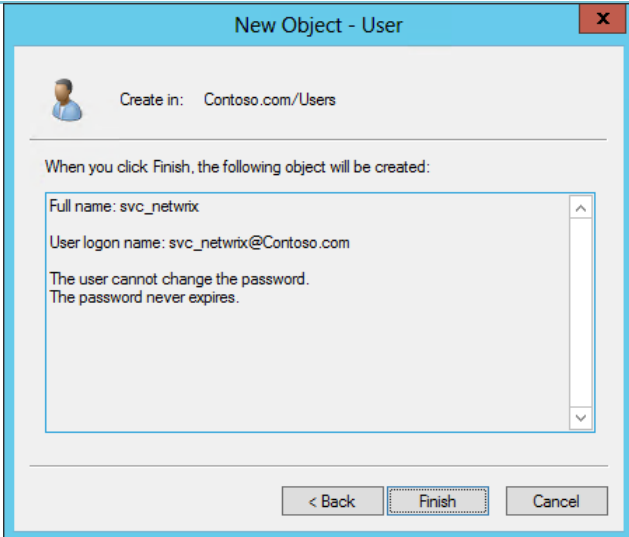


A l'étape *Specify Default Data Processing Account*, il est nécessaire de spécifier un compte de domaine pour collecter les informations.

D'après les recommandations\* le compte de service doit être dans le groupe Administrateur du domaine.

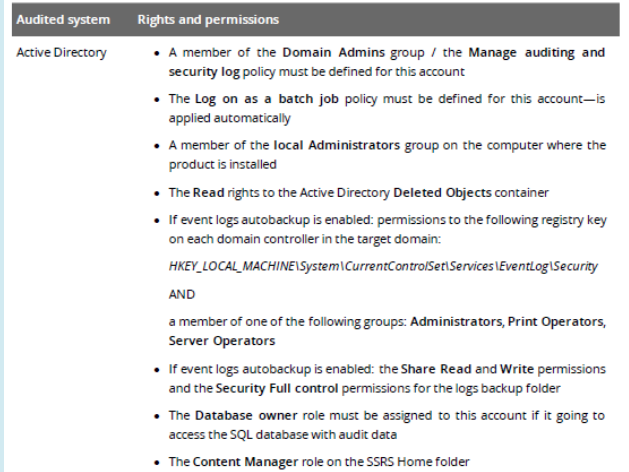
Nous allons créer un compte de service dédié à l'ensemble de la plateforme de Netwrix.

**4**



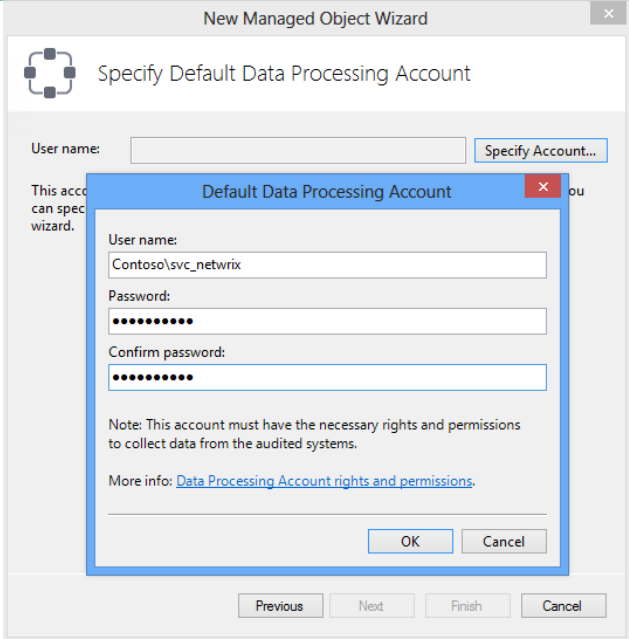
Créer votre compte de service dans la console Utilisateurs et Ordinateurs Active Directory et affecter le au groupe Domain Admins.

**5**



Voici les recommandations des permissions pour le compte de service. Ces recommandations sont à retrouver dans la documentation officielle du produit.

**6**



Revenez au setup de configuration et cliquez sur **Specify Account** puis indiquer le compte de service. Enfin, cliquez sur **OK**.



7

New Managed Object Wizard

Specify Default Data Processing Account


User name:

Specify Account...

This account

Default Data Processing Account

Netwrix Auditor

The account Contoso\svc\_netwrix has been granted the Log on as a batch job right.

OK

Note: This account must have the necessary rights and permissions to collect data from the audited systems.

More info: [Data Processing Account rights and permissions.](#)

OK

Cancel

Previous

Next

Finish

Cancel

Une fenêtre d'alerte indique que le compte de service a reçu une élévation de privilège. Cliquez sur **OK**.

8

New Managed Object Wizard

Specify Default Data Processing Account

User name:

Specify Account...

This account will be used by default to access all of your Managed Objects. If needed, you can specify a separate account to collect data from this Managed Object later in this wizard.

Previous

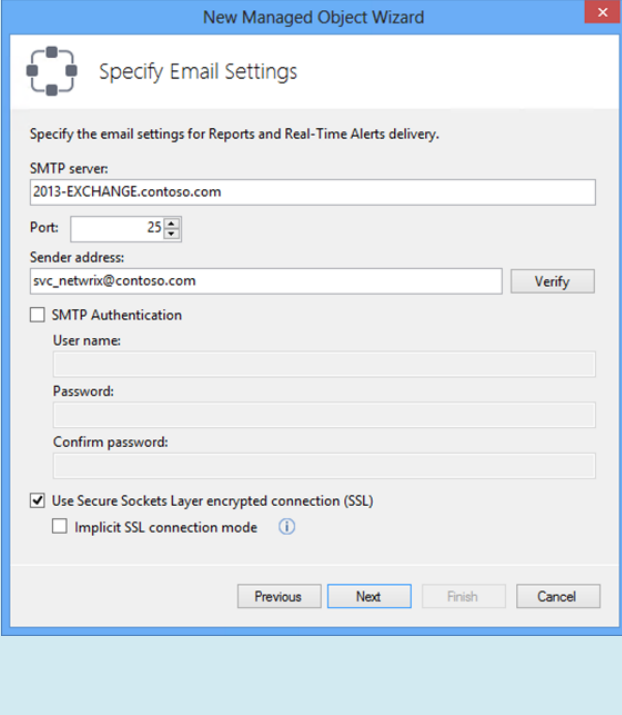
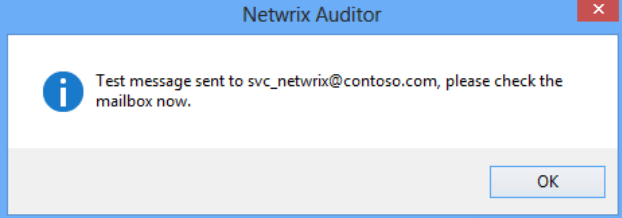
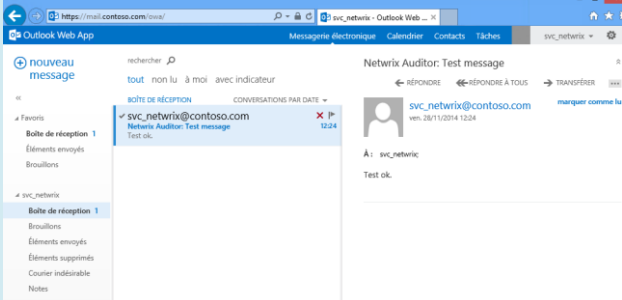
Next

Finish

Cancel

Cliquez sur **Next**.

Etude de la solution Netwrix Auditor pour Active Directory 6.5 réalisée par Nicolas BROISIN – Copyright

9		<p>Il est demandé ensuite de spécifier la configuration du serveur de messagerie pour l'envoi de rapport et alertes en temps réels.</p> <p>Pour cela, au niveau de SMTP server indiquer le nom de votre serveur de messagerie électronique ainsi que le port et si besoin l'authentification SMTP.</p> <p>Afin que la connexion entre le serveur Exchange et le poste de travail Netwrix Auditor soit sécurisé, je vous conseille de cocher la case <b>Use Secure Sockets Layer encrypted connection (SSL)</b>.</p> <p>Pour tester la bonne configuration des informations, cliquez sur <b>Verify</b></p>
10		<p>Un message d'information devrait s'afficher.</p>
11		<p>Ainsi qu'un mail de test avec comme contenu « Test ok ».</p>

12

**Specify Domain Name**

Domain name:

**Data Processing Account**

All operations with this Managed Object will be performed under this account. Make sure that it has [the necessary rights and permissions](#).

☒ Default (Contoso\svc\_netwrix)  
Note: If needed, you can change the default account later in Settings > Data Collection.

☐ Custom

User name:

Password:

Previous Next Finish Cancel

A l'étape *Specify Domain Name*, indiquer le FQDN (nom complet DNS) du domaine AD.

Sélectionner le compte de service qui sera utilisé pour la collecte des données.

Personnellement, pour mon lab je n'ai pas jugé nécessaire de créer plusieurs comptes de service. Par ailleurs, dans les best practices il est préférable de segmenter les rôles avec des comptes de service distincts.

13

**Configure Reports Settings**

☒ Enable Reports

☒ Automatically install and configure a new instance of SQL Server Express Edition

☐ Use an existing SQL Server instance with SQL Server Reporting Services

SQL Server instance:

☒ Windows Authentication

User name:

Password:

**SQL Server Reporting Services**

Report Server URL:  Verify

Report Manager URL:  Verify

Previous Next Finish Cancel

A l'étape *Configure Reports Settings*, cochez **Enable Reports** puis cliquer sur Next.

14

**Select SQL Server Instance Source**

☐ Install and configure a SQL Server instance

Automatically download, install and configure Microsoft SQL Server 2012 Express Edition with Advanced Services on this computer.

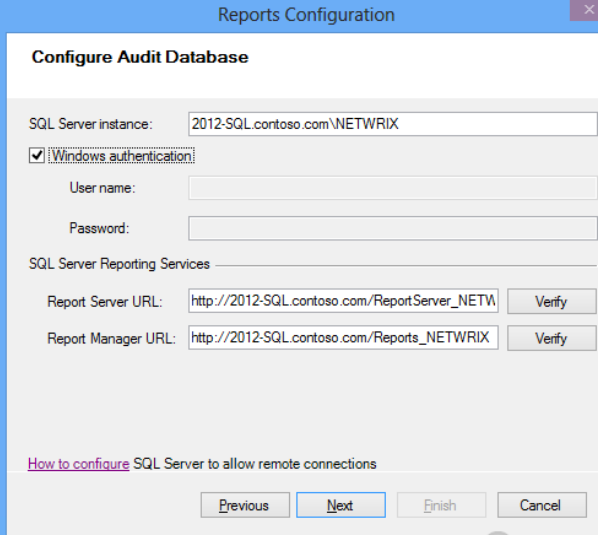

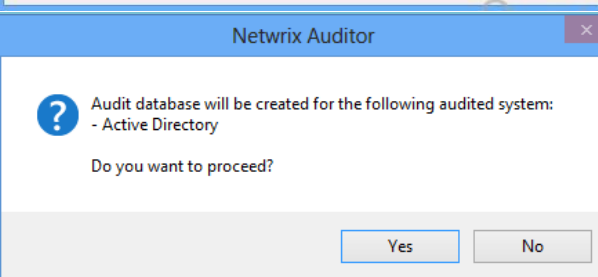
☒ Use an existing SQL Server instance

Point to an existing SQL Server instance. SQL Server Reporting Services must be installed and configured for this server.

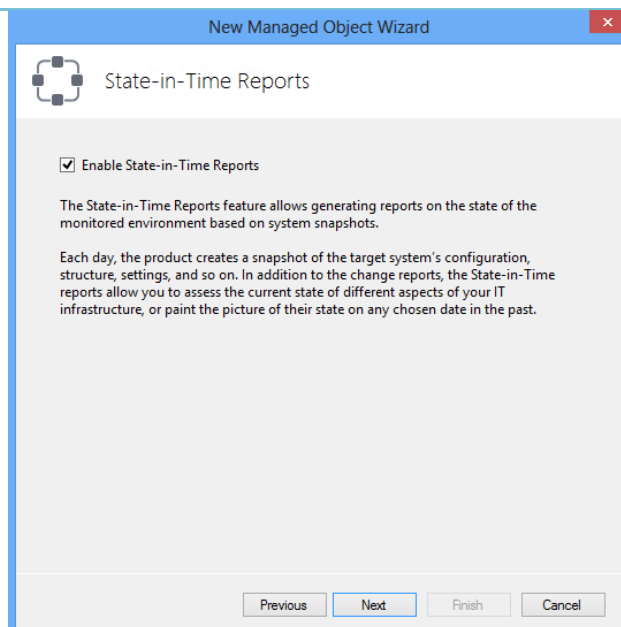
Previous Next Finish Cancel

Pour des questions de performances, j'ai préféré créer une instance dédiée sur un serveur SQL 2012.

Pour cela cocher, **Use an existing SQL Server instance**.

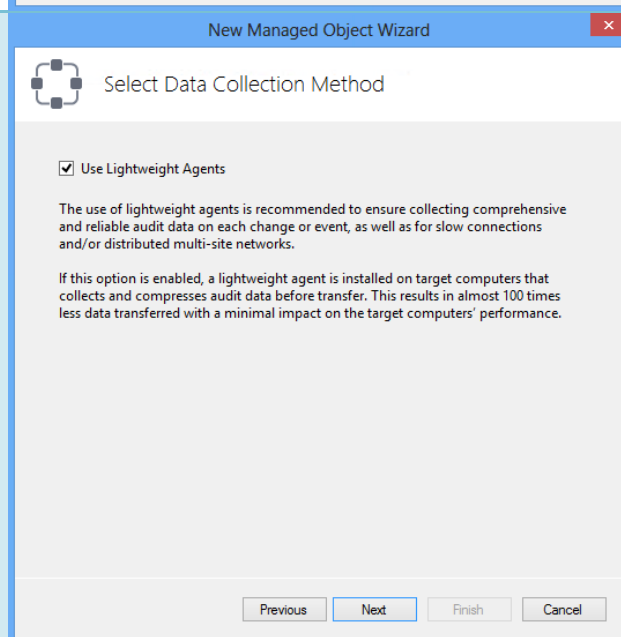
15		<p>A l'étape <i>Configure Audit Database</i>, indiquer l'instance SQL ainsi que la méthode d'authentification.</p> <p>Je n'ai pas configuré le HTTPS pour l'URL de Reporting Service. Mais pour un déploiement en production cela est préconisé.</p> <p>Cliquez sur <b>Verify</b> pour tester la bonne configuration.</p>
16		<p>La configuration de la partie base de données de Netwrix a été correctement réalisée. Cliquez sur <b>Finish</b>.</p>
17		<p>Ensuite un message apparaît pour avertir que la base de données d'Audit pour Active Directory va être créée. Cliquez sur <b>Yes</b> pour suivre le setup de configuration.</p>

18



Pour configurer les alertes en temps réel, cochez **Enable State-in-Time Reports** et cliquez sur **Next**.

19



Pour optimiser les liens réseaux, utiliser l'agent dédié en cochant **Use Lightweight Agents**. Attention à faire une exclusion Antivirus pour celui-ci sinon cela pourrait poser problèmes.

Puis cliquez sur **Next**.

20

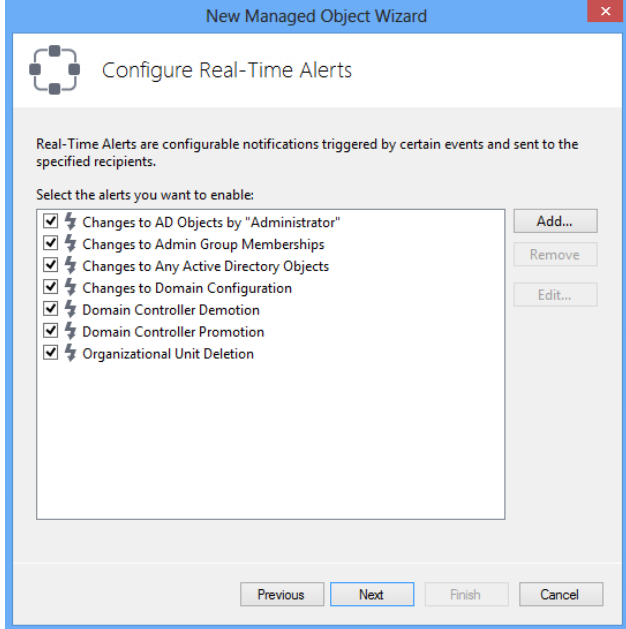
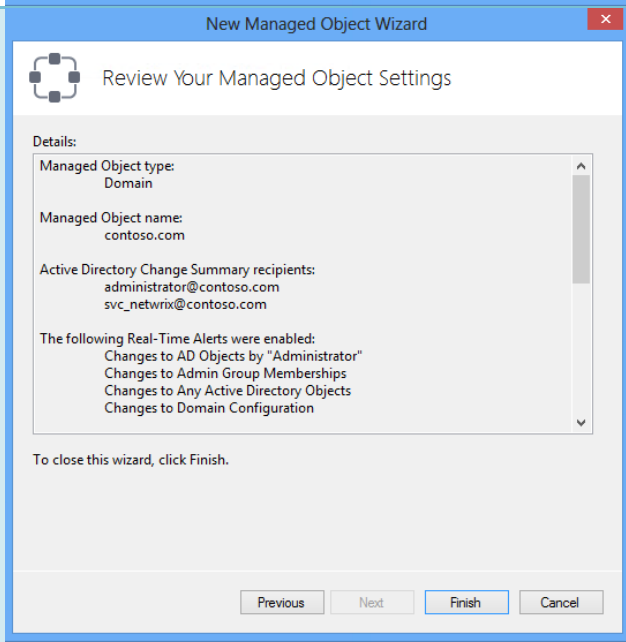
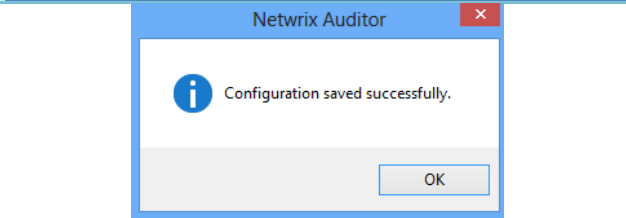
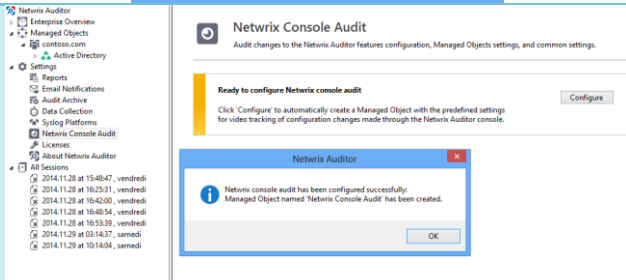
A l'étape *Configure Audit in Target Environment*, choisissez **Automatically for the selected audit systems** pour que le setup configure automatiquement les pré-requis d'audit en rajoutant les droits adéquates.

La deuxième possibilité est de le faire manuellement à l'aide de la documentation technique qui se trouve sur le site officiel de Netwrix.

Cliquez ensuite sur Next.

21

Choisissez à qui les rapports d'audit devront être envoyés. Cette liste pourra être modifiée directement dans la console.

22		<p>Configurez les alertes dont vous souhaitez être averti en temps réel.</p> <p>Il est possible de créer ses propres alertes customisés en cliquant sur <b>Add</b>.</p>
23		<p>Vérifié les informations puis cliquer sur <b>Finish</b>.</p>
24		<p>Un message d'information devrait vous informer que la configuration a été correctement enregistrée.</p>
25		<p>Ensuite configurer la console d'audit Netwrix. Pour cela, allez dans <b>Settings</b>, puis dans <b>Netwrix Console Audit</b>.</p> <p>Cliquez sur <b>Configure</b>, un message vous informe que la Console a été correctement configuré.</p>

26



## Netwrix Console Audit

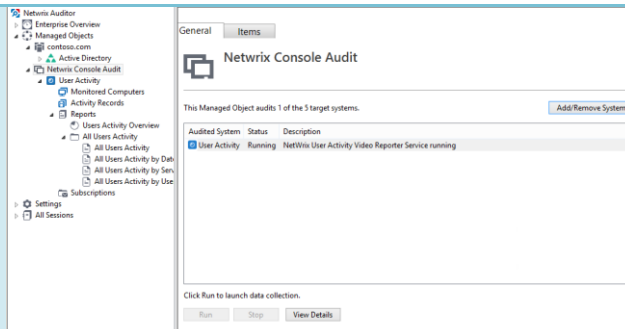
Audit changes to the Netwrix Auditor features configuration, Managed Objects settings, and common settings.

### Netwrix console audit is turned on

To view audit data (i.e. video records showing how changes to the Netwrix Auditor settings were made), navigate to Managed Objects -> Netwrix Console Audit -> User Activity -> Activity Records.

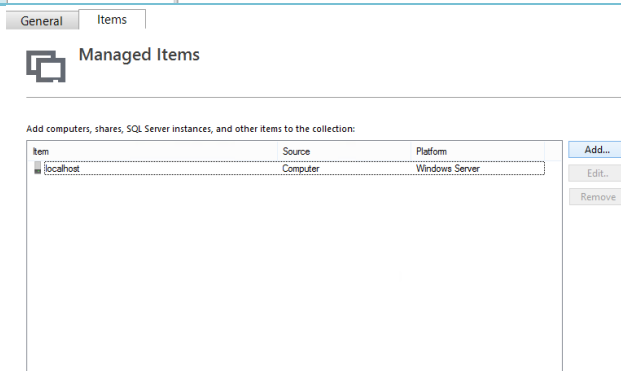
A partir de là il est possible de passer à la configuration de la surveillance vidéo des serveurs.

27



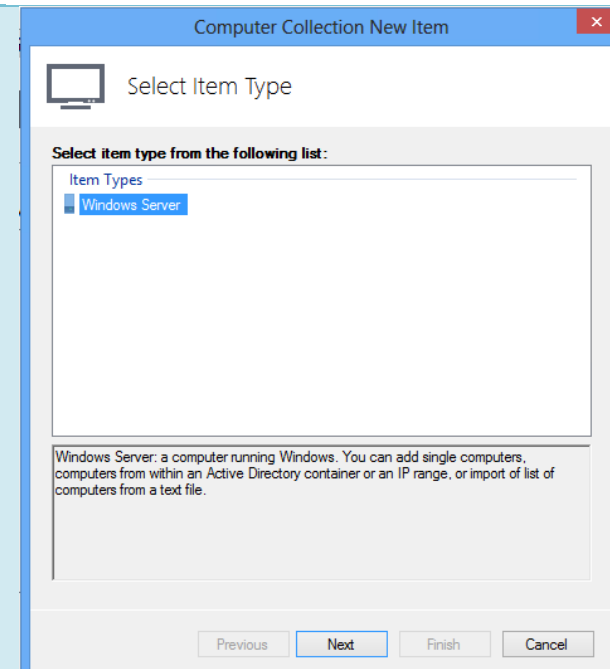
Au niveau de la rubrique **Netwrix Console Audit**, cliquez sur **Run**.

28



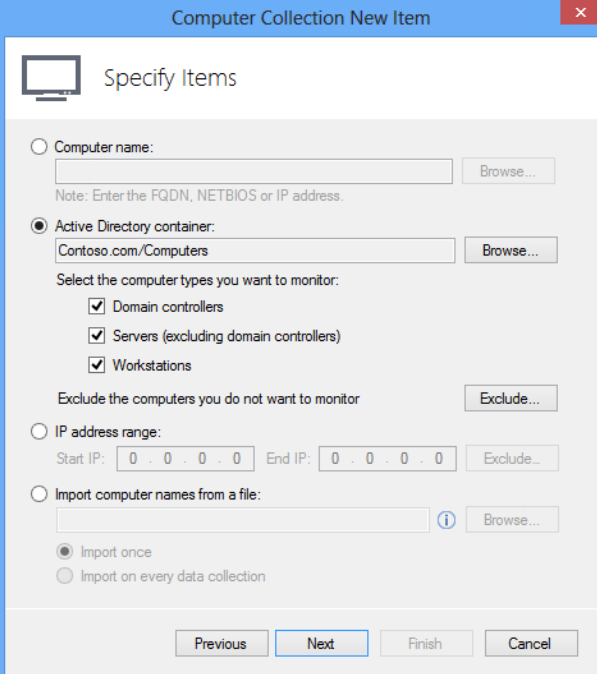
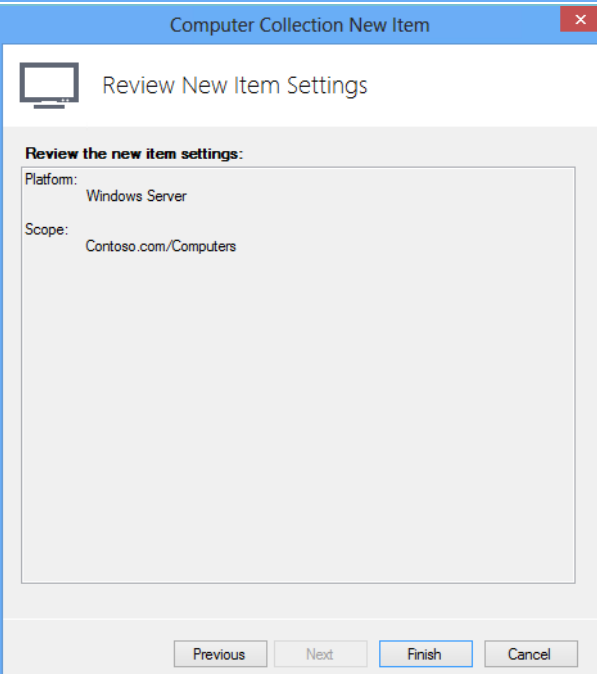
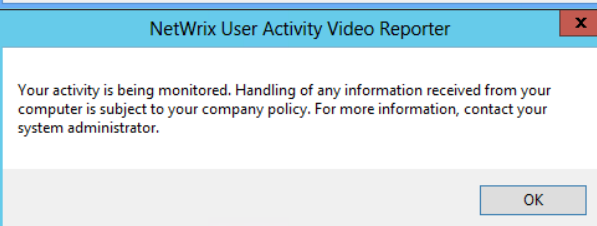
Ensuite, cliquer sur la rubriques **Items**, et pour ajouter des serveurs à surveiller, cliquez sur **Add**.

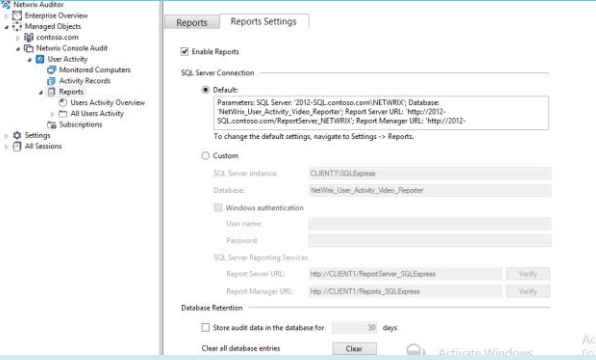
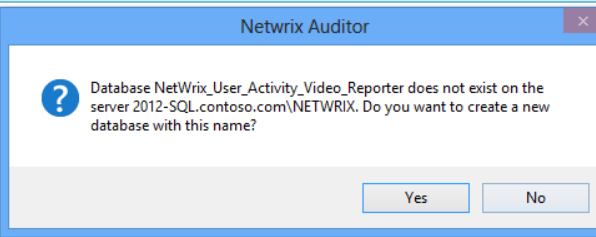
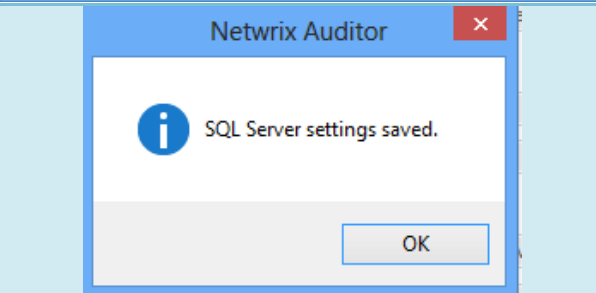
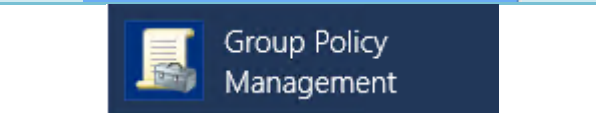
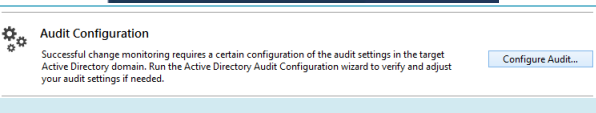

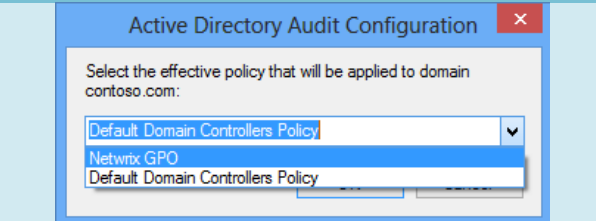
29



Choisissez, **Windows Server** puis **Next**.

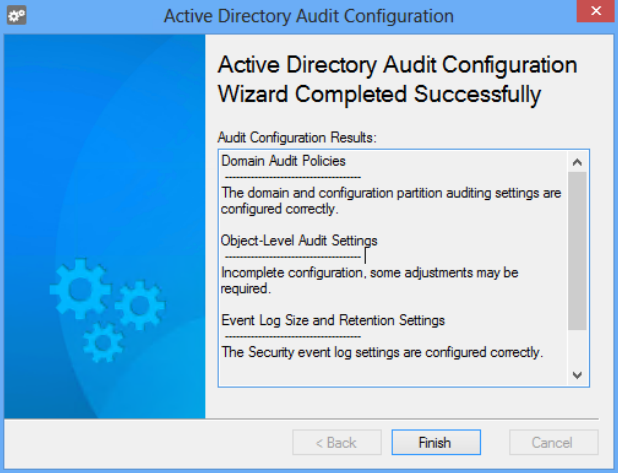
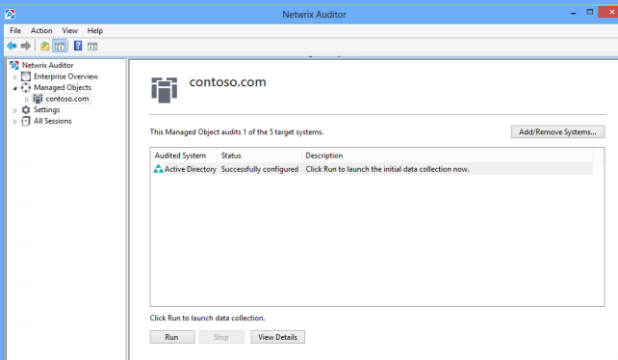
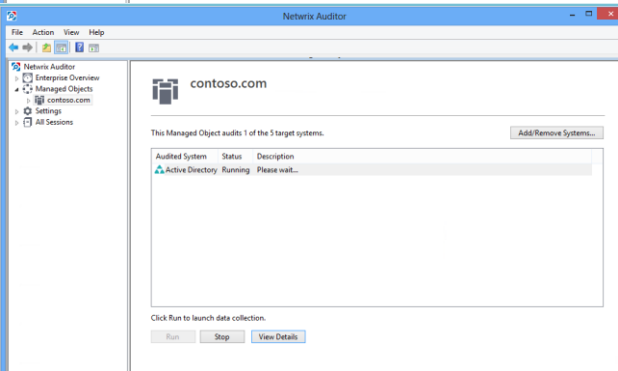
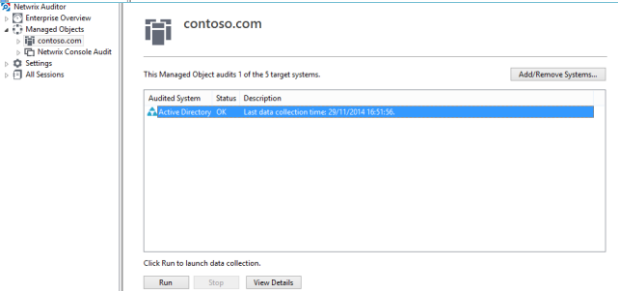


30		<p>Vous avez plusieurs possibilités de recherche des serveurs, soit par le nom, soit par le centenaire Active Directory, soit par une plage d'adresses IP, ou encore par l'import d'un fichier avec la liste des noms des serveurs.</p>
31		<p>Ensuite cliquez sur <b>Finish</b>.</p>
32		<p>Sur les serveurs, un agent s'installe, puis un message d'avertissement indiquera à chaque utilisateur se connectant sur le serveur que celui-ci est surveillé.</p>

33		<p>Une autre action nécessaire est la configuration des rapports.</p> <p>Pour cela, allez dans la rubrique, <b>Netwrix Console Audit, User Activity, Reports.</b></p> <p>Ensuite dans l'onglet, <b>Reports Settings</b>, cocher <b>Enable Reports</b> et indiquer votre serveur de reporting. Dans mon cas il est positionné sur la même instance que les bases de données.</p>
34		<p>Cliquez sur <b>Yes.</b></p>
35		<p>Et si tout s'est correctement déroulé, sur <b>OK.</b></p>
36		<p>Ensuite, pour appliquer les prérequis d'audit, veuillez créer une GPO de domaine dédié à Netwrix</p>
37		<p>Ensuite, allez au niveau de <b>Audit Configuration</b> et cliquer sur <b>Configure Audit..</b></p>
38		<p>Un assistant de configuration s'ouvre.</p> <p>Suivre les différentes étapes de configuration.</p> <p>Cliquer sur <b>Next.</b></p>
39		<p>Sélectionné la GPO préalablement crée</p>

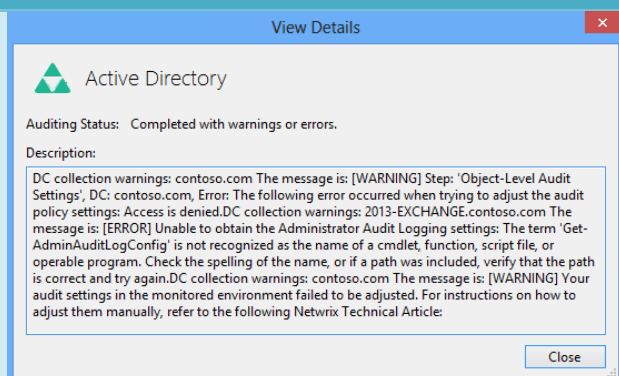
40		<p>Indiquer le compte de service de collecte des données. Ensuite cliquer sur <b>Detect</b> pour vérifier si le domaine est configuré correctement pour l'audit. Si ce n'est pas le cas cliquer sur <b>Adjust</b>.</p>
41		<p>Un message d'information vous indiquera si oui ou non la partition de domaine et de configuration a été correctement paramétrée.</p>
42		<p>L'assistant vérifiera l'état des permissions de l'Object-Level Audit et positionnera les valeurs adéquates.</p>
43		<p>Un message d'information vous permettra de valider l'état de votre plateforme.</p>

44		<p>Les paramètres de rétention et de tailles des logs seront également vérifiés et configurés en fonction des besoins du produit.</p>
45		<p>Un message d'information vous permettra de valider l'état de votre plateforme.</p>
46		<p>Si un serveur Exchange a été détecté dans votre environnement, il vous propose également de réaliser la configuration adéquate afin de positionner les bons paramètres à l'audit du serveur de messagerie.</p>
47		<p>Un message d'information vous permettra de valider l'état de votre plateforme</p>

48		<p>Un récapitulatif des actions est réalisé à la fin, cliquer ensuite sur <b>Finish</b>.</p>
49		<p>Pour terminer, retourner au niveau de la rubrique <b>Managed Objects</b>, puis sur votre domaine.</p> <p>Cliquer ensuite sur <b>Run</b> afin de débuter la première collecte des données.</p>
50		<p>La première collecte peut prendre plusieurs minutes..</p>
51		<p>Si tout se passe bien, le statut devrait passer à « OK » et votre Netwrix Auditor pour Active Directory est correctement configuré.</p> <p>Dans le cas contraire, je vous laisse lire la partie « <b>CONSEILS EN CAS D'UNE ANALYSE EN ECHEC</b> »</p>

## 4. CONSEILS EN CAS D'UNE ANALYSE EN ECHEC

1



Pas d'inquiétude, nous pouvons remarquer un « Object-Level Audit Settings ... Access is denied ».

Cela veut dire que les prérequis pour auditer la plateforme n'a pas été encore positionné.

Pour cela, deux possibilités, le faire manuellement ou à l'aide du setup de configuration de Netwrix. Les deux méthodes vont être détaillées pour plus de clarté.

Ensuite, nous avons une autre erreur concernant le serveur Exchange avec la commande « Get-AdminAuditLogConfig » non reconnue.

2

### 4.4.1. Configure Exchange Server Administrator Audit Logging Settings

If the audited AD domain has an Exchange organization running Exchange Server 2010 or 2013, you must configure the Exchange Server Administrator Audit Logging (AAL) settings. To do this, perform the following procedure on any of the audited Exchange Servers (these settings will then be replicated to all Exchange Servers in the domain).

#### To configure Exchange Server Administrator Audit Logging settings

1. On the computer where the audited Exchange Server is installed, navigate to Start → Programs → Exchange Management Shell.
2. Execute the following command depending on your Exchange Server version:
  - Exchange Server 2010  

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -  
AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets *
```
  - Exchange Server 2013  

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -  
AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets * -LogLevel Verbose
```
3. On the computer where Netwrix Auditor is installed, browse to the %Netwrix Auditor installation folder%\Active Directory Auditing folder, locate the SetAALExcludedCmdlets.ps1 file and copy it to the Exchange Server.
4. In Exchange Management Shell, in the command line, execute this file by specifying the path to it:

48/104

Netwrix Auditor Installation and Configuration Guide

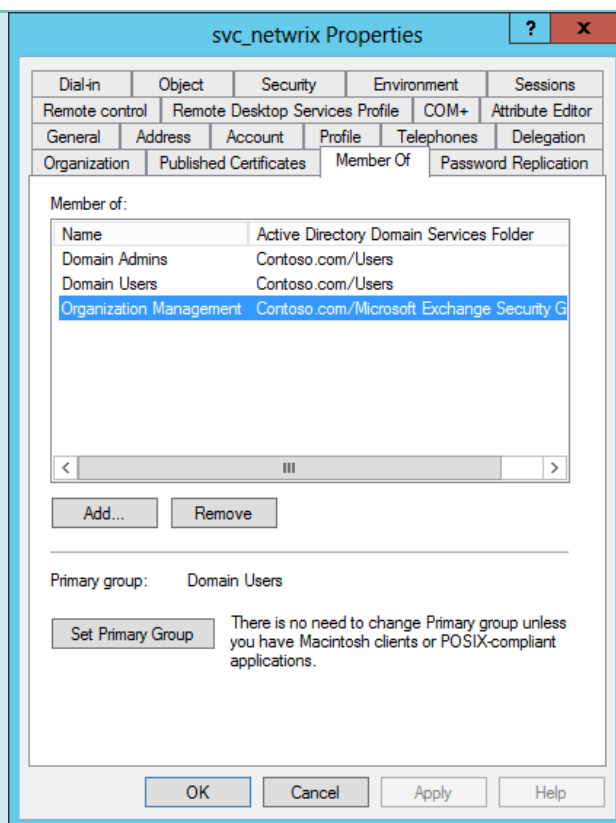
4. Configure IT Infrastructure for Audit

```
<Path_To_SetAALExcludedCmdlets_File>\SetAALExcludedCmdlets.ps1
```

This file contains a list of cmdlets that must be excluded from Exchange Server logging to reduce server load.

A l'aide de la documentation officielle, nous pouvons retrouver comment configurer l'audit d'un serveur Exchange.

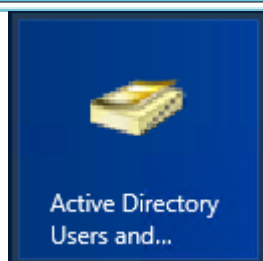
3



Ensuite il est demandé d'ajouter le groupe de sécurité universelle Organization Management au compte de service dédié à la collecte des informations sous peine d'avoir une nouvelle erreur sur la collecte des données.

Avec ces deux changements il ne devrait plus avoir de problème lié au serveur Exchange lors de la première analyse.

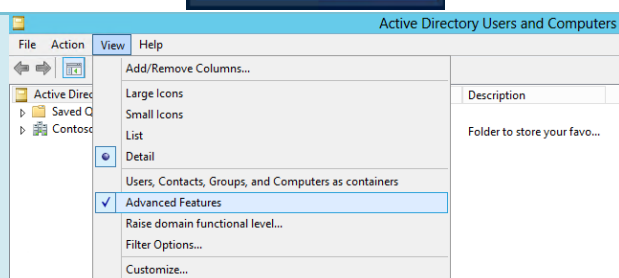
4



Ensuite pour ce qui est d'un problème d'accès refusés, voici la procédure à suivre.

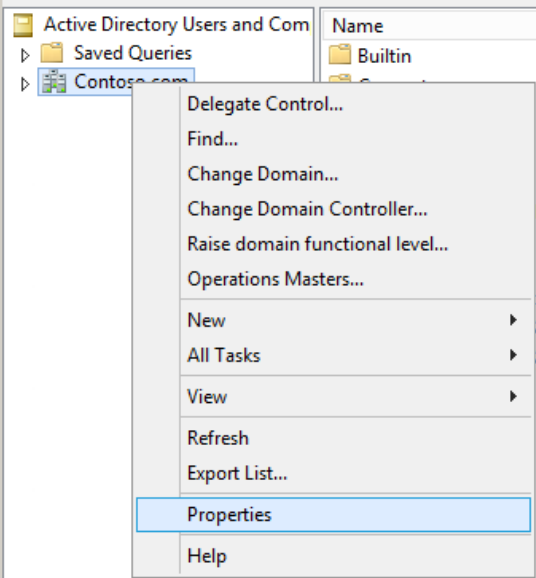
Cliquez sur l'utilitaire Utilisateurs et Ordinateurs Active Directory.

5



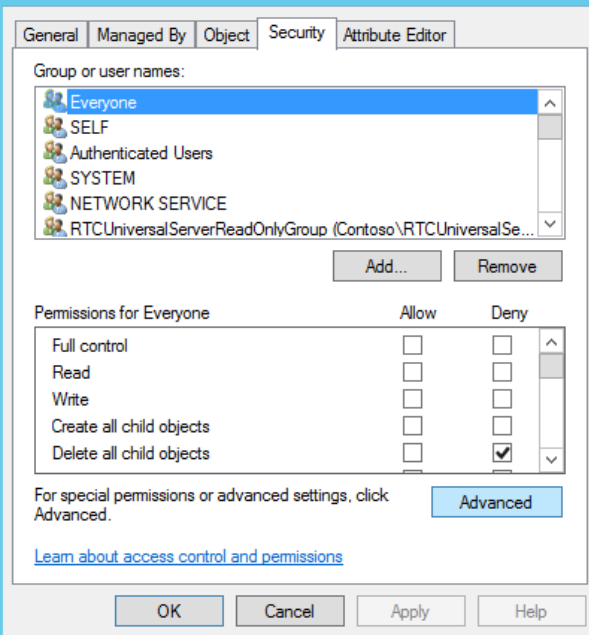
Ensuite, **View**, et cocher **Advanced Features**.

6



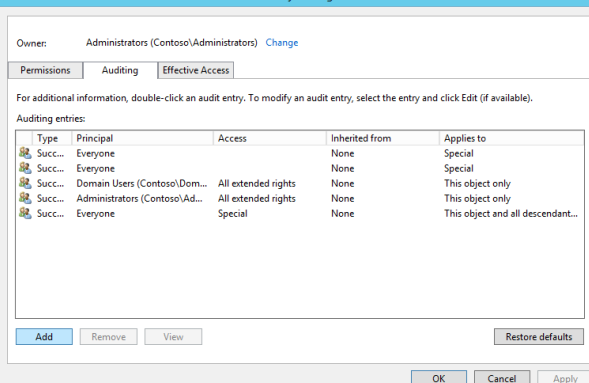
Puis au niveau du conteneur de votre domaine, clique droit, **Properties**.

7



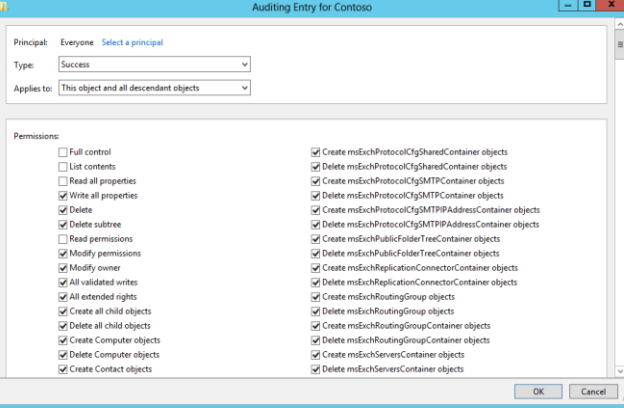
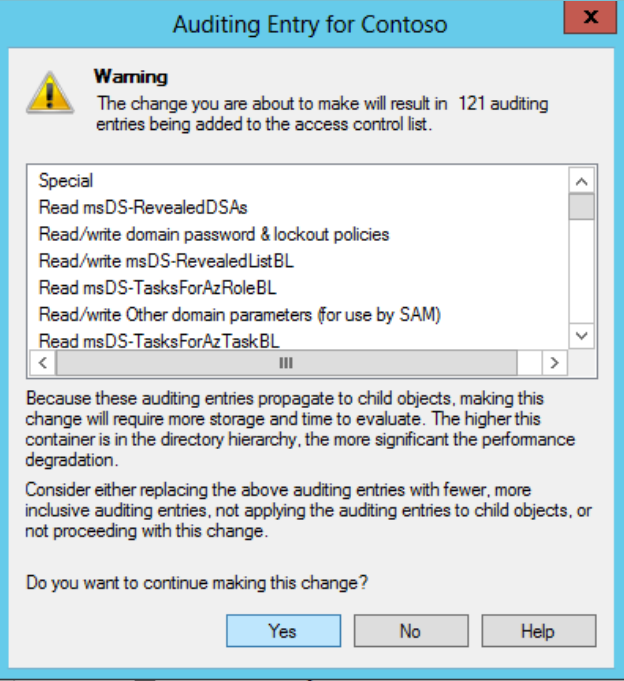
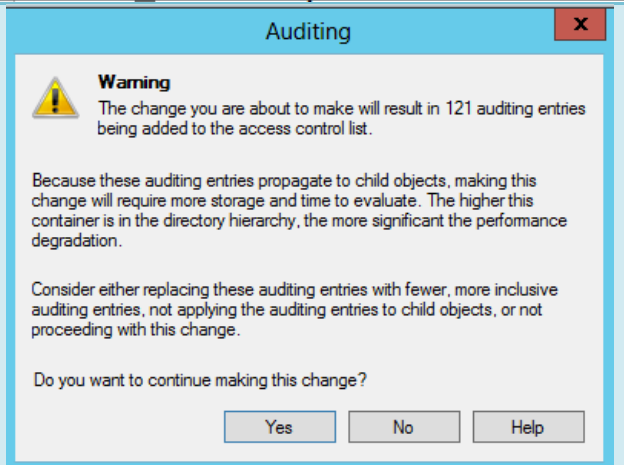
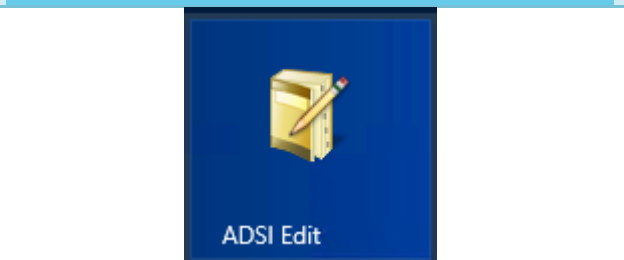
Allez au niveau de l'onglet **Security**, **Advanced**.

8

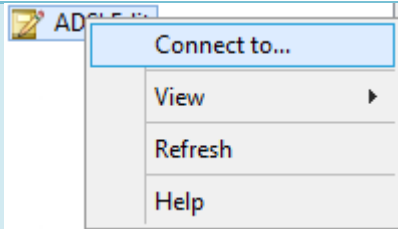


Au niveau de la rubrique **Audit** cliquer sur **Add**.

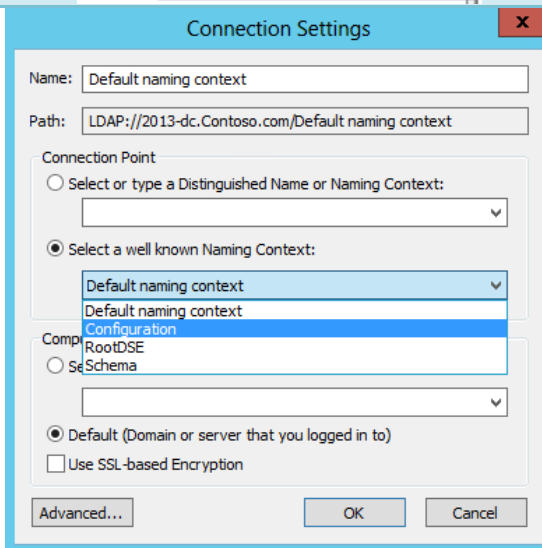


<p>9</p>		<p>Sélectionner le groupe <b>Everyone</b>. Positionner <b>Success</b> au niveau de Type. Cliquer au niveau de la liste déroulante sur <b>This object and all descendant objects</b>.</p> <p>Enfin cochez l'ensemble des permissions sauf :</p> <ul style="list-style-type: none"> <li>• <b>Full Control</b></li> <li>• <b>List contents</b></li> <li>• <b>Read all properties</b></li> <li>• <b>Et Read permissions</b></li> </ul>
<p>10</p>		<p>Un message d'alerte vous informe sur l'état des modifications de la nouvelle access control list.</p> <p>Cliquez sur <b>Yes</b>.</p>
<p>11</p>		<p>Une nouvelle fois, cliquez sur <b>Yes</b>.</p>
<p>12</p>		<p>Ensuite faire la même chose pour la partition de Configuration.</p> <p>Pour cela, exécuter ADSI Edit.</p>

13

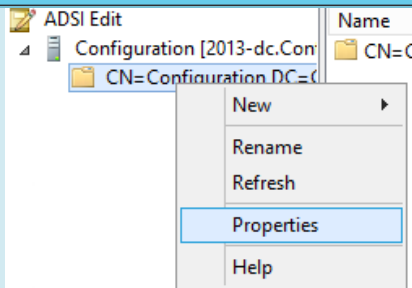
Clique droit, **Connect to..**

14



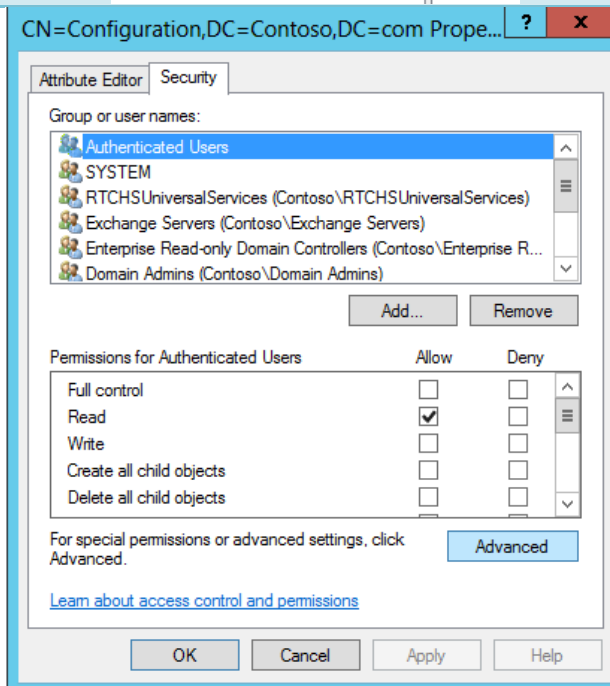
Au niveau de **Select a well known Naming Context**, choisissez : **Configuration**.

15



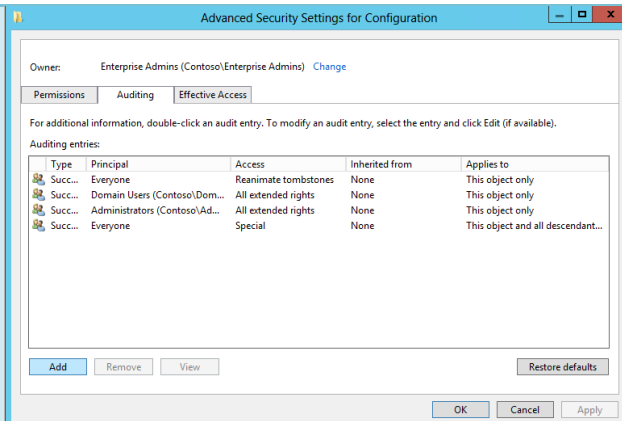
Au niveau du conteneur de Configuration, clique droit, **Properties**.

16



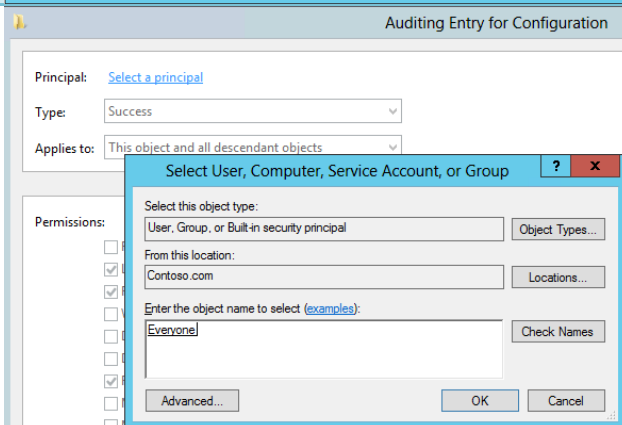
Allez au niveau de l'onglet **Security, Advanced**.

17



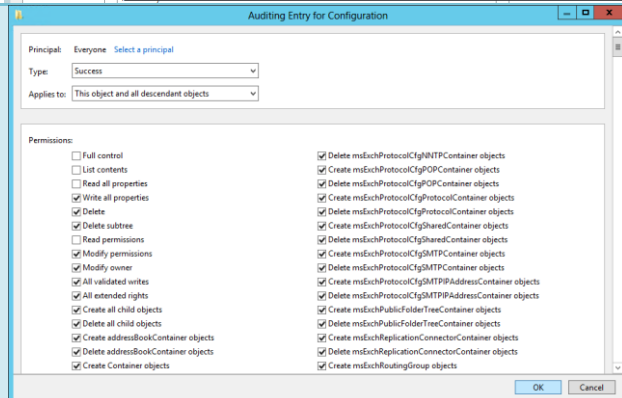
Au niveau de la rubrique **Audit** cliquer sur **Add**.

18



Sélectionner le groupe **Everyone**.

19

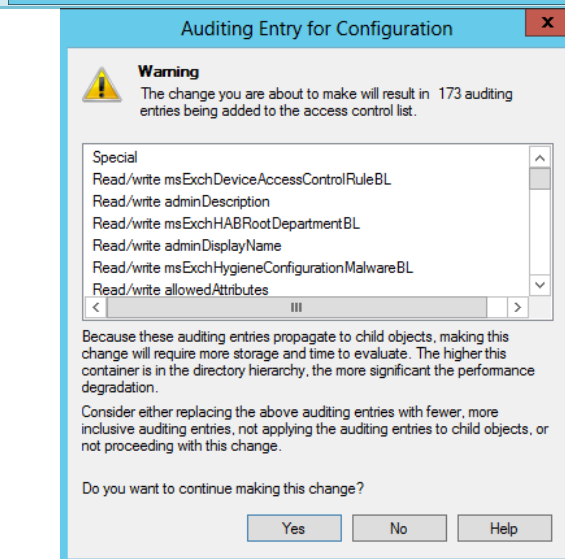


Positionner **Success** au niveau de Type. Cliquer au niveau de la liste déroulante sur **This object and all descendant objects**.

Enfin cochez l'ensemble des permissions sauf :

- **Full Control**
- **List contents**
- **Read all properties**
- **Et Read permissions**

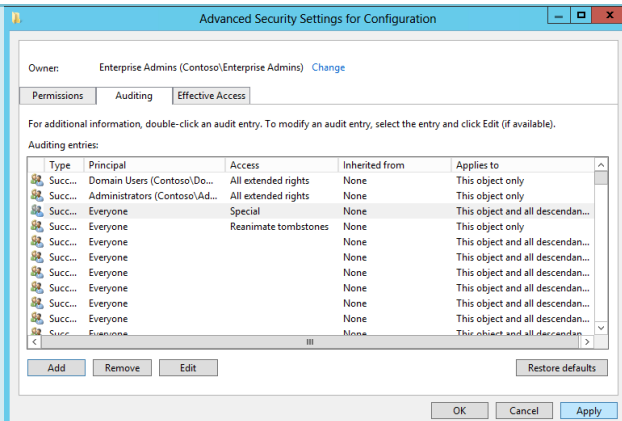
20



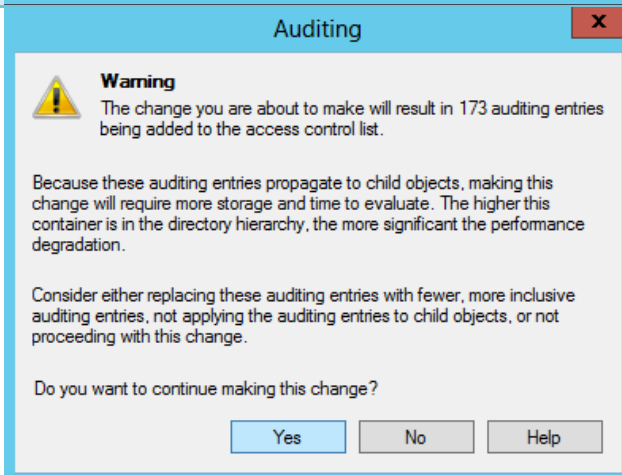
Un message d'alerte vous informe sur l'état des modifications de la nouvelle access control list.

Cliquez sur **Yes**.

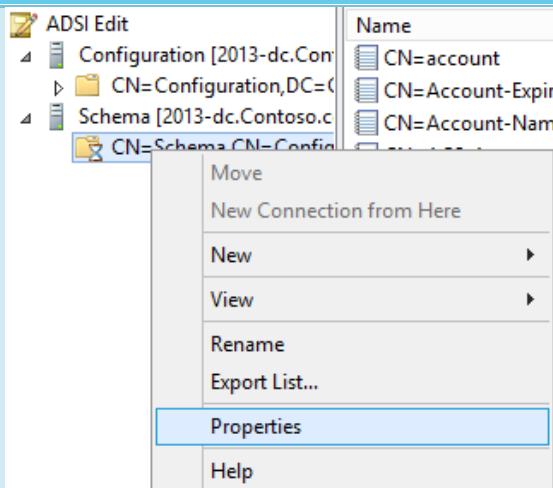
21

Cliquez sur **Apply**.

22

Cliquez sur **Yes**.

23

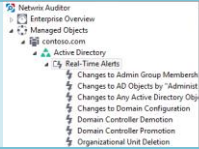


Même chose pour la partition du Schéma.

Ceci est important pour auditer l'ensemble de l'annuaire d'entreprise.

## 5. SCENARIO 1 : PRESENTATION DU REPORTING LORS DE LA CREATION D'OBJETS ACTIVE DIRECTORY

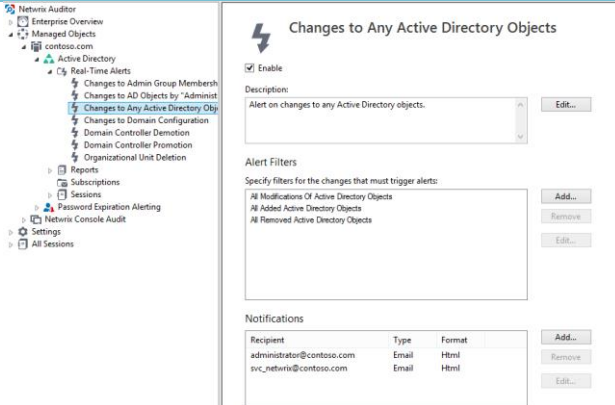
**1**



Name	Description
Changes to Admin Group Memberships	Alert on changes to the Domain Admins, and Enterprise Admins groups.
Changes to AD Objects by "Administrator"	Alert on any changes to Active Directory objects made under the "administrator"
Changes to Any Active Directory Objects	Alert on changes to any Active Directory objects.
Changes to Domain Configuration	Alert on changes to objects in the Configuration partition, such as sites, replicat
Domain Controller Demotion	Alert on a domain controller demotion.
Domain Controller Promotion	Alert on a domain controller promotion.
Organizational Unit Deletion	Alert on an Organizational Unit deletion.

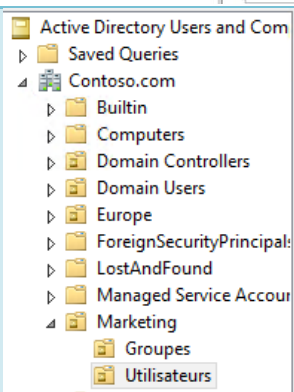
Dans la console Netwrix Auditor, vérifier que les alertes de changements en temps réels sont activées.

**2**



Pour cela double cliquer sur une règle et vérifier que la case **Enable** soit cochée.

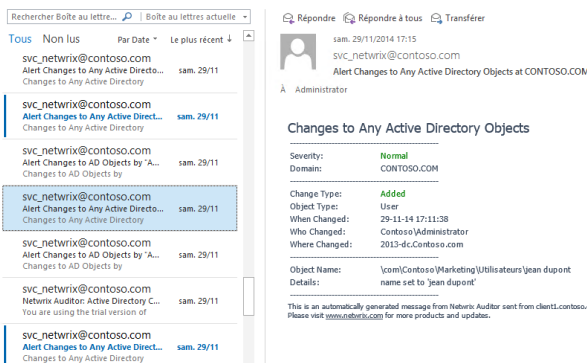
**3**



Name	Type
jean.dupont	User

Ensuite, à l'aide de l'outil Utilisateurs et Ordinateurs Active Directory, créer l'arborescence comme ci-contre.

**4**



5 minutes plus tard, une notification par messagerie électronique devrait apparaître permettant de donner une alerte rapide sur la création de l'arborescence.

Dans le corps du mail, nous pouvons constater les différents critères de ce changement :

- Change Type
- Object Type
- When Changed
- Who Changed
- Where Changed
- Object Name
- Details

Ce courriel permet de donner un état synthétique quasiment en temps réel des changements réalisés sur la plateforme Active Directory.



## 6. SCENARIO 2 : INVESTIGATION SUR LA SUPPRESSION D'OBJETS ACTIVE DIRECTORY PUIS RESTAURATION

1



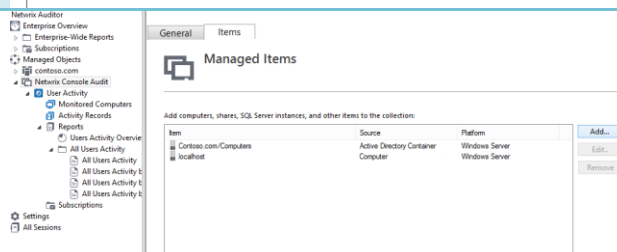
### Netwrix Console Audit

This Managed Object audits 1 of the 5 target systems.

Audited System	Status	Description
User Activity	Running	NetWrix User Activity Video Reporter Service running

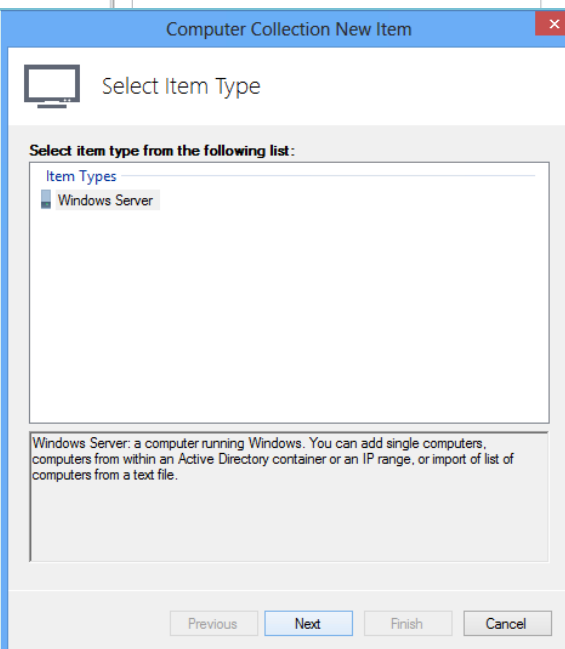
Dans la console Netwrix Auditor vérifier que le service **Netwrix User Activity Video Reporter** soit en cours d'exécution.

2



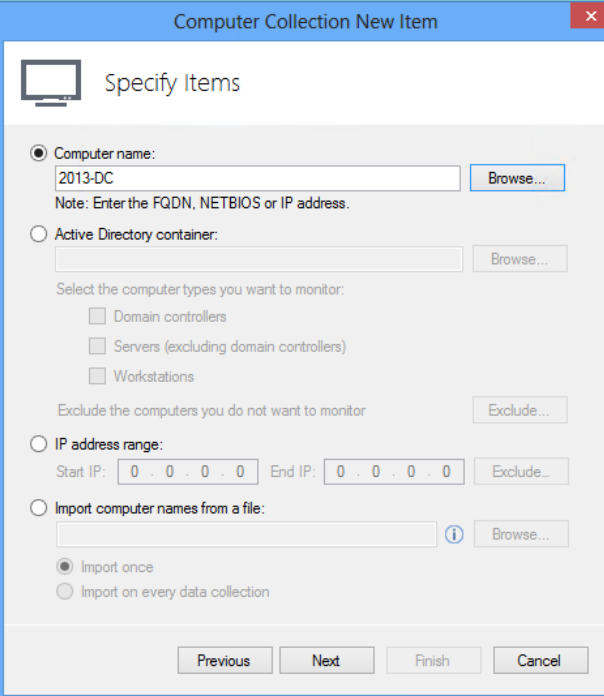
Allez dans l'onglet **Items**, puis cliquer sur **Add** pour ajouter le serveur à surveiller.

3



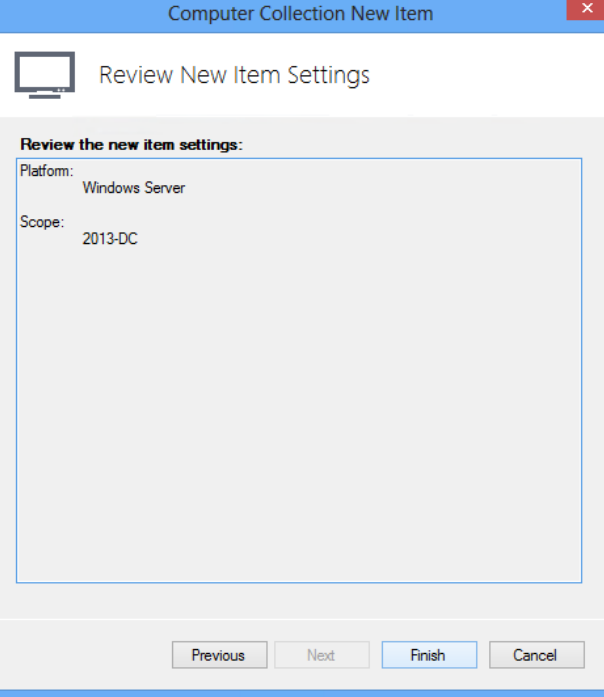
Sélectionner **Windows Server**, puis **Next**.

**4**



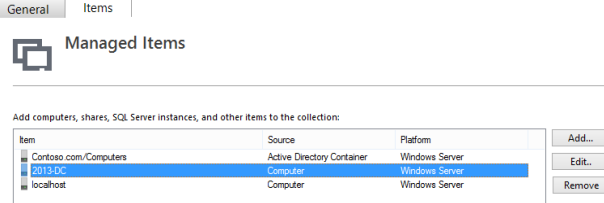
Nous souhaitons enregistrer l'activité sur le contrôleur de domaine : 2013-DC. Cliquez ensuite sur **Next**.

**5**



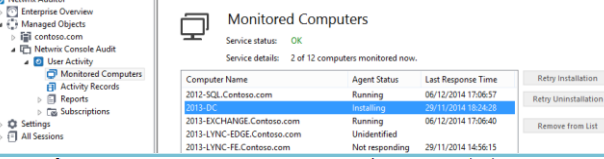
Un résumé est présent pour valider la configuration. Cliquez sur **Finish**.

**6**



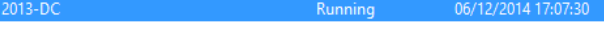
Le serveur apparaît dans la liste des équipements gérés.

**7**



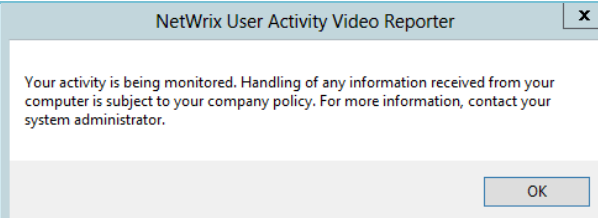
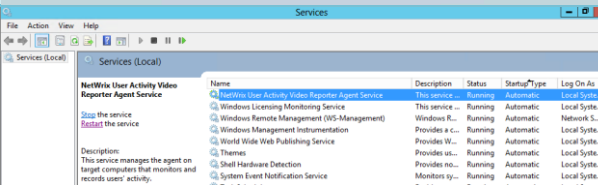
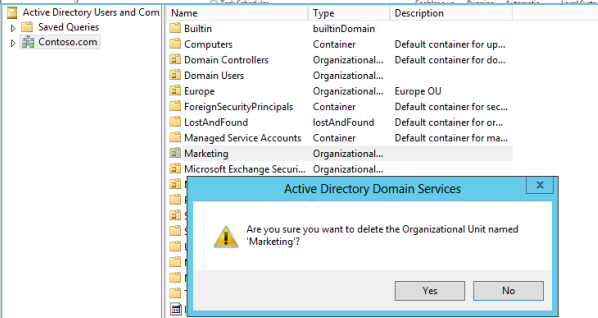
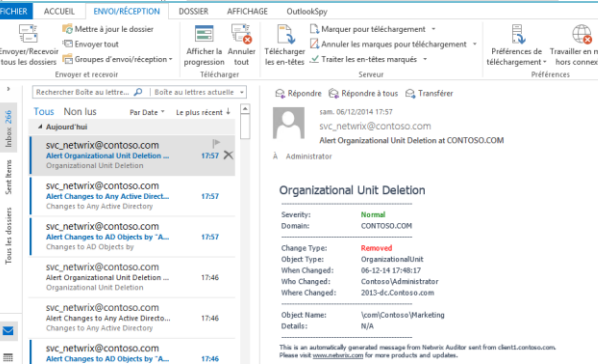
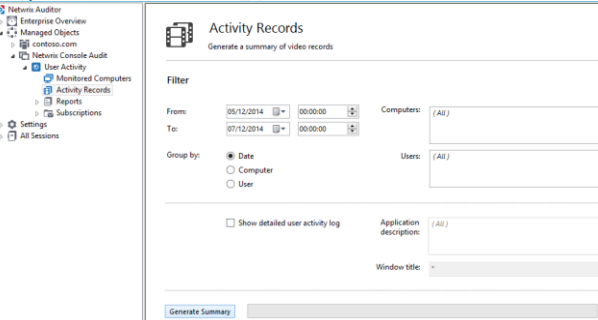
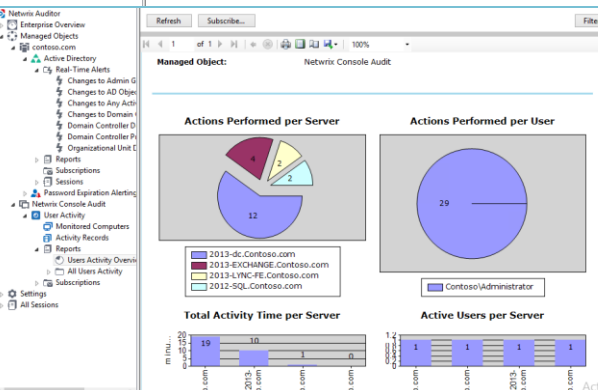
Dans la rubrique **Monitored Computers**, nous pouvons constater que l'agent est en cours d'installation sur le contrôleur de domaine.

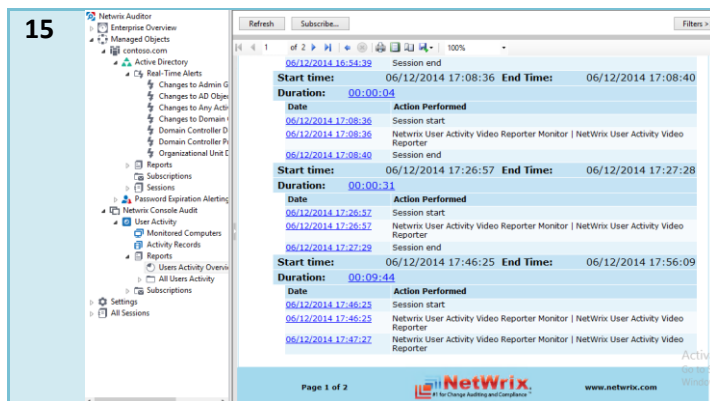
**8**



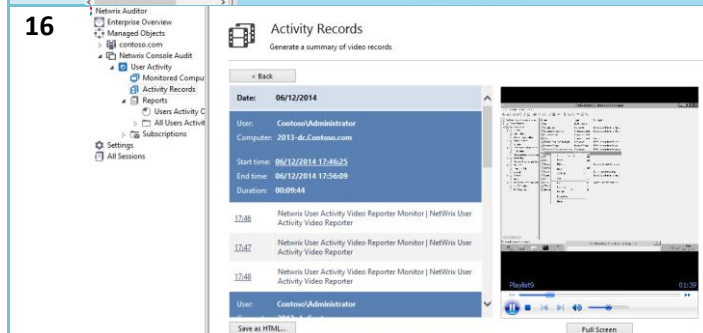
L'installation dure quelques minutes. Puis le statut de l'agent passe à



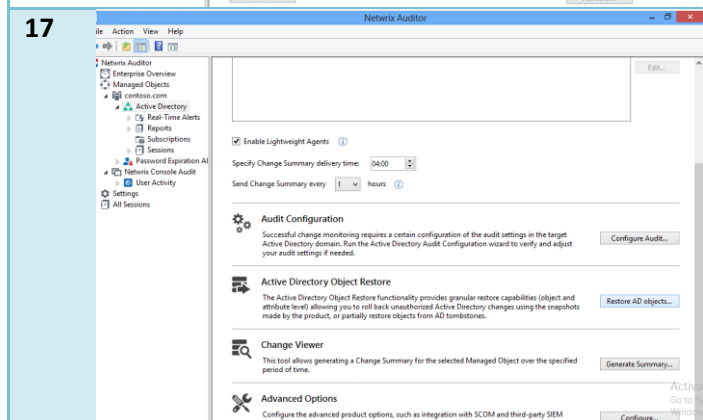
<p>9</p> 	<p><b>Running.</b></p> <p>Sur le contrôleur de domaine, un message apparaît à l'écran pour informer l'utilisateur de l'enregistrement de son activité sur le serveur.</p>
<p>10</p> 	<p>Nous pouvons également constater sur le serveur que le service <b>Netwrix User Activity Video Reporter Agent</b> est en cours d'exécution.</p>
<p>11</p> 	<p>Prenons le cas d'une suppression d'une OU.</p>
<p>12</p> 	<p>Dans les 5 minutes après la suppression le courriel d'alerte en temps réel parvient à l'administrateur.</p> <p>Cela donne un bilan rapide de la suppression.</p>
<p>13</p> 	<p>Ensuite, l'investigation continue à l'aide de la console Netwrix Auditor au niveau de la rubrique <b>Activity Records</b>.</p> <p>Il est possible de faire un filtrage sur la période désiré, l'ordinateur ou l'utilisateur.</p> <p>Enfin cliquer sur <b>Generate Summary</b>.</p>
<p>14</p> 	<p>Plusieurs graphes sont disponibles permettant une analyse complète par serveur, par utilisateur ou encore par temps d'activité sur chaque serveur.</p> <p>Cliquez sur un camembert pour avoir le détail des informations.</p>



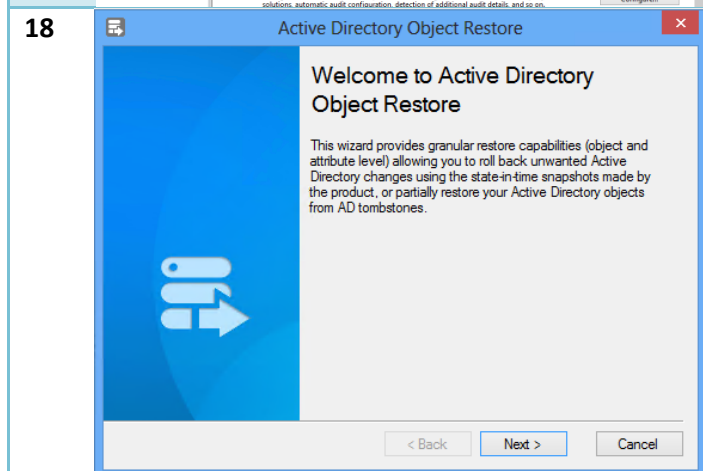
Ensuite sélectionner l'enregistrement où la date de la suppression a été constatée.



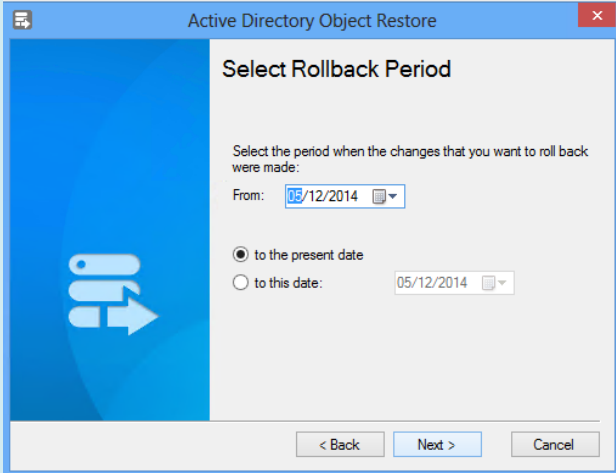
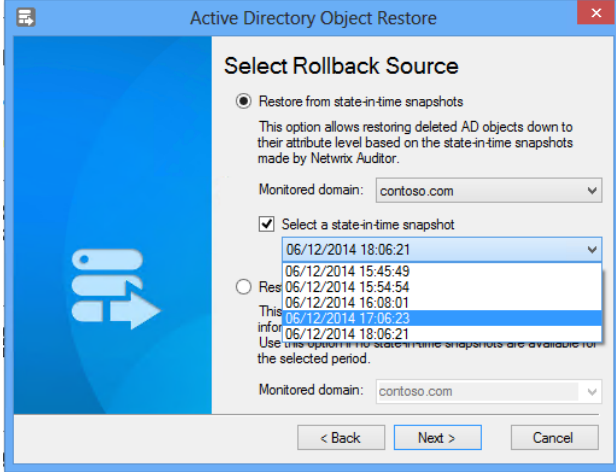
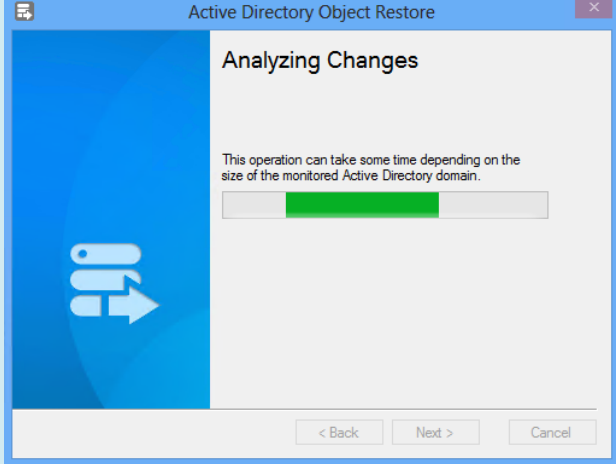
Visionner l'enregistrement de l'activité de l'utilisateur et vérifier ses actions.

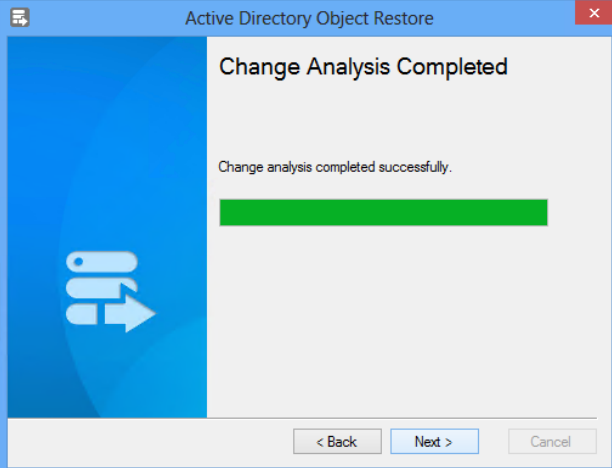
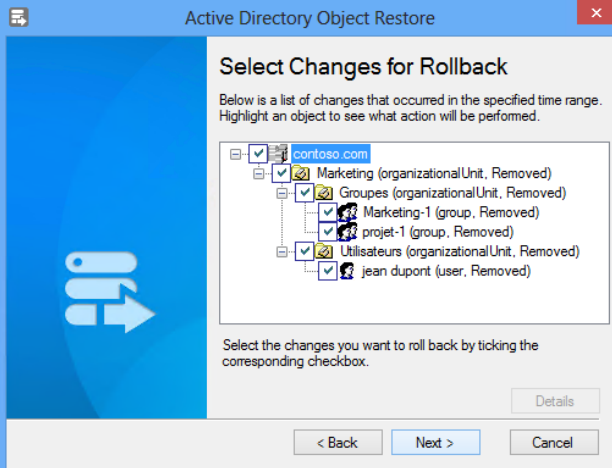
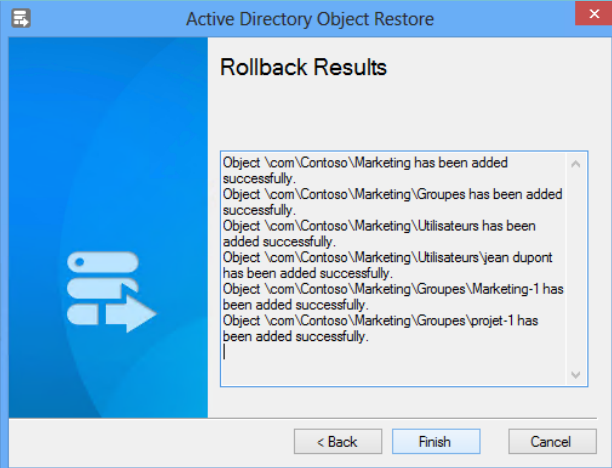


A partir de là il est possible de restaurer l'ensemble des objets Active Directory ayant été supprimés en retournant dans la rubrique **Active Directory** puis sur **Restore AD objects..**



Un assistant s'ouvre, cliquez sur **Next**.

19		Sélectionner la période de restauration.
20		Indiquez le Snapshot de l'Active directory à restaurer puis <b>Next</b> .
21		L'analyse des modifications dure plusieurs minutes.

22		Cliquez ensuite sur Next.
23		Sélectionner les objets Active Dircetory que vous souhaitez restaurer et cliquez sur <b>Next</b> .
24		<p>Un résumé de l'opération de restauration est disponible puis cliquez sur <b>Finish</b>.</p> <p>Il sera ensuite possible de vérifier à l'aide de l'outil Utilisateurs et Ordinateurs Active Directory que les objets sont à nouveaux disponibles.</p>

## 7. ETENDUES DES POSSIBILITES AVEC LA SOLUTION NETWRIX AUDITOR

PLATFORM	TYPICAL AUDIT QUESTIONS
<b>Active Directory</b>	Who added user to security group? Who delegated management rights to OU?
<b>VMware</b>	Who created a new virtual machine? Who changed resource pool parameters?
<b>MS Exchange</b>	Who deleted a mailbox? Who accessed another user's mailbox? Who reconfigured information store?
<b>SQL Server</b>	Who changed table structure schema in a production SQL database? Who deleted production SQL database? Who added new database login?
<b>File Server</b>	Who changed file permissions on file server? Who accessed sensitive files on file servers? Who deleted files from file server?
<b>NetApp Filer</b>	Who changed file permissions on NetApp Filers? Who attempted to access folders with sensitive data on NetApp Filers? Who failed to change files on NetApp Filers?
<b>EMC VNX/VNXe/Celerra</b>	Who changed file permissions on EMC VNX/VNXe/Celerra device? Who accessed sensitive files on EMC VNX/VNXe/Celerra device? Who deleted folders from EMC VNX/VNXe/Celerra device?
<b>Group Policy</b>	Who deactivated strong password policy? Who unlinked GPO from organization unit? Who configured new software installation policy?
<b>Windows Server</b>	Who installed what software? Who changed computer configuration settings? Who made changes to registry? Who added members to local Administrators group? What changes were made to DNS zones and records? What patches and hotfixes were installed recently? Who modified startup programs (AutoRun)? Who changed file sharing settings and open shares?
<b>SharePoint</b>	Which web applications were created/changed/deleted? What servers were added to / removed from a farm? What changes occurred to the incoming/outgoing e-mail settings?

Source : [https://www.netwrix.com/change\\_auditing\\_solution.html](https://www.netwrix.com/change_auditing_solution.html)

## 8. BILAN

AVANTAGES	INCONVENIENTS
Installation et configuration simple de mise en œuvre	Aucune granularité dans les droits d'administration de Netwrix Auditor
Solution modulaire et évolutive	Pas d'interface WEB de la console d'administration
Solution clé en main	Absence d'une version française
Prise en main rapide de l'outil : Interface intuitive et esthétique	Incompatible avec les serveurs Linux
Gestion complètes des événements : Rapports détaillés	Pas d'application mobile
Surveillance et alerte : Rapports temps réels, Dashboard synthétique, Enregistrement vidéo de l'activité utilisateur	
Supporte les dernières versions de Windows (2012, 2012 R2), Exchange 2013 et SQL Server 2014.	
Base de connaissance : Documentations officielles complètes ; blog officiel régulièrement alimentés en articles.	
Solution mature (> 8 ans), avec un support officiel	
Intégration avec la solution System Center : Package SCOM	