

# SOPHOS

## Sophos NAC Advanced Guide d'extraction des rapports

Version du produit : 3.2

Date du document : mars 2011



## Table des matières

1	À propos de ce document.....	3
2	Vues SQL.....	4
3	Schéma relationnel entre les Vues SQL.....	27
4	Annexe A : exemples de Vues SQL.....	28
5	Support technique.....	42
6	Mentions légales.....	43

# 1 À propos de ce document

Sophos NAC Advanced rassemble des données pour la création de rapports disponibles à la consultation à l'aide du Sophos Compliance Manager. Ce document contient une série documentée de Vues SQL écrites pour le Sophos Compliance Manager. Une Vue SQL est une table virtuelle ou temporaire qui vous permet de récupérer des données des bases de données SQL et de les stocker dans une vue. Les vues SQL vous permettent de manipuler des données de rapports en dehors des limites des bases de données de conformité Sophos, améliorant ainsi la flexibilité des rapports et leur interopérabilité avec les produits de création de rapports tiers. En plus des bases de données SQL, les Vues SQL disposent d'une interface plus logique et plus précise. Elles permettent, en outre, d'accéder à des données non contenues dans les rapports Sophos NAC Advanced. Vous recevez les données dans leur forme brute car elles n'ont pas été calculées, rassemblées ou récapitulées de quelque façon que ce soit. Plus important, alors que les structures des données sous-jacentes pourront changer dans les versions futures, les Vues SQL continueront d'être prises en charge afin que les requêtes écrites pour elles n'exigent aucune modification entre les versions.

Sophos a défini 18 Vues SQL contenant des données de rapports d'application, de conformité et d'agent. Les données récupérées à l'aide des Vues SQL proviennent du Report Warehouse de Sophos NAC Advanced, une base de données contenant uniquement des données de rapports archivées. Par défaut, les données sont archivées dans le Report Warehouse toutes les 24 heures à 2h30 du matin. Mais vous pouvez configurer la fréquence et l'heure d'archivage de ces données. Pour plus d'informations sur les paramètres du rapport, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

## 1.1 À qui s'adresse ce document ?

Ce document s'adresse aux généralistes en informatique travaillant au sein de petites et moyennes entreprises. Ce document peut également intéresser les spécialistes de l'informatique travaillant au sein d'entreprises disposant de plus de 25 000 ordinateurs d'extrémité. Si vous avez plus de 1000 ordinateurs d'extrémité, nous vous recommandons d'utiliser les Sophos Professional Services. Nos consultants Professional Services travaillent conjointement avec votre équipe de sécurité informatique pour mettre au point et mettre en place un plan de déploiement de vos logiciels.

## 2 Vues SQL

Sophos a défini 18 Vues SQL. Les sections suivantes contiennent les informations suivantes pour chaque Vue SQL :

- Définition de la Vue SQL
- Objectif de la Vue SQL
- Données renvoyées de la Vue SQL
- Définition du champ de données
- Relations entre les Vues SQL

Certaines Vues SQL ont une clé principale (PK, Primary Key) définie. La PK d'un tableau relationnel identifie de manière unique chaque enregistrement du tableau. La PK constitue un moyen de joindre les Vues SQL. Certaines Vues SQL ont une clé étrangère (FK, Foreign Key). La FK est un champ dans un tableau relationnel qui correspond à la colonne PK d'un autre tableau. La FK sert à croiser des références de tableaux.

### 2.1 Considérations et recommandations

Lors de l'utilisation de Vues SQL, nous vous conseillons de prendre en considération les éléments suivants :

- Les Vues SQL sont sécurisées à l'aide d'un nouveau rôle SQL nommé **nac\_public**. Cette fonctionnalité vous permet de contrôler l'accès aux Vues SQL lorsque vous le jugez nécessaire. Par défaut, le seul utilisateur avec un accès aux Vues SQL est l'administrateur de la base de données.
- N'exécutez **jamais** de requêtes sur toutes les Vues SQL lorsque le Report Warehouse archive des données de rapports. Les données sont archivées dans le Report Warehouse toutes les 24 heures à 2h30 du matin. Mais vous pouvez configurer la fréquence et l'heure d'archivage de ces données.
- Si vous exécutez des requêtes face aux Vues SQL lorsque d'autres exécutent des rapports à l'aide du Compliance Manager, ces tâches auront un impact les unes sur les autres et pourront ralentir à la fois la requête et les processus des rapports.

### 2.2 Agent Enforcer

La Vue SQL Agent Enforcer renvoie toutes les données de rapports fournies par l'agent de quarantaine lorsque l'état de quarantaine change sur l'ordinateur d'extrémité.

**Nom de la Vue SQL pour les requêtes = NACVP\_AgentEnforcer**

Nom colonne	Taille colonne	Définition et relation entre les vues
agentKey	bigint	PK
statusChangeDateTime	datetime	Date et heure de changement de l'état d'application de l'Agent Enforcer. La date et l'heure sont au temps moyen de Greenwich (GMT).

Nom colonne	Taille colonne	Définition et relation entre les vues
username	nvarchar(128)	Nom de l'utilisateur connecté à l'agent. Le nom utilisateur peut ne pas avoir de valeur si l'état d'application de l'ordinateur d'extrémité a changé et si ce dernier n'exécute pas une session d'agent active.
agentID	nvarchar(36)	Identifiant de l'installation de l'agent ou de l'ordinateur d'extrémité sur lequel le changement de l'état d'application a été signalé. L'identifiant de l'agent est un GUID généré par logiciel qui identifie de manière unique chaque installation d'agent.
agentVersion	nvarchar(20)	Version de l'agent installé sur l'ordinateur d'extrémité.
hostname	nvarchar(128)	Nom de l'ordinateur d'extrémité sur lequel l'agent est installé.
complianceState	nvarchar(128)	<p>État de conformité de l'ordinateur d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>compliant</b> : l'évaluation a déterminé que l'ordinateur d'extrémité est conforme à la stratégie. Le modèle d'accès Agent Enforcer conforme associé à la stratégie détermine l'accès réseau.</li> <li>■ <b>partial</b> : l'évaluation a déterminé que l'ordinateur d'extrémité est partiellement conforme à la stratégie. Le modèle d'accès Agent Enforcer partiellement conforme associé à la stratégie détermine l'accès réseau.</li> <li>■ <b>nonCompliant</b> : l'évaluation a déterminé que l'ordinateur d'extrémité n'est pas conforme à la stratégie. Le modèle d'accès Agent Enforcer non conforme associé à la stratégie détermine l'accès réseau.</li> </ul> <p><b>Important</b> : l'état de conformité de l'ordinateur d'extrémité est déterminé par l'évaluation des conditions du profil sur l'ordinateur d'extrémité et par le comportement de la stratégie affectée pour ce type de profil. L'état de conformité de chaque condition est remonté jusqu'au niveau des profils et de nombreux profils sont remontés jusqu'au niveau des stratégies pour déterminer l'état de conformité global. L'état le moins conforme détermine l'état de conformité global. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.</p>

Nom colonne	Taille colonne	Définition et relation entre les vues
reason	nvarchar(20)	<p>Raison pour laquelle un modèle d'accès particulier est affecté par l'Agent Enforcer. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>Assessment</b> : l'évaluation effectuée par l'agent a déterminé l'état de conformité. Le modèle d'accès Agent Enforcer associé à l'état de conformité de stratégie détermine l'accès réseau.</li> <li>■ <b>No Agent Tray</b> : l'agent n'est pas exécuté sur l'ordinateur d'extrémité. Cet état peut être signalé par l'Agent Enforcer si l'utilisateur n'a pas de session ouverte sur Windows ou si l'application Agent de la zone de notification ne fonctionne plus. Le modèle d'accès Agent Enforcer de la stratégie associé à l'état No Agent Tray de l'agent sert à déterminer l'accès réseau.</li> <li>■ <b>Policy Retrieval Error</b> : une stratégie n'a pas pu être récupérée pour l'utilisateur. Cet état peut résulter de l'impossibilité pour l'agent de récupérer la stratégie depuis le serveur d'applications de conformité, de la non-affectation d'une stratégie au groupe de l'utilisateur ou de l'obsolescence de l'état de conformité de l'utilisateur par rapport au champ Agent Policy Update Threshold configuré dans la zone Configure System &gt; Enforcer Settings. Le modèle d'accès Agent Enforcer de la stratégie associé à l'état Policy Retrieval Error Agent de l'agent détermine l'accès réseau.</li> <li>■ <b>Remediate</b> : la stratégie est en mode Remediate. Le modèle d'accès Agent Enforcer associé au mode de stratégie Remediate sert à déterminer l'accès réseau.</li> <li>■ <b>Report Only</b> : la stratégie est en mode Report Only. Le modèle d'accès Agent Enforcer associé au mode de stratégie Report Only sert à déterminer l'accès réseau.</li> <li>■ <b>User Override</b> : l'utilisateur a remplacé la quarantaine de l'agent sur l'ordinateur d'extrémité. Le modèle d'accès Agent Enforcer de la stratégie associé à l'état User Override Agent sert à déterminer l'accès réseau.</li> </ul>
templateName	nvarchar(128)	Nom et version du modèle d'accès qui détermine l'action prise par l'Agent Enforcer. Le modèle d'accès utilisé est basé sur la raison.
agentOffset	bigint	Décalage en date et en heure pouvant être utilisé pour calculer la date et l'heure signalées par l'agent plutôt que la date et l'heure qui étaient réglées sur celles du serveur.

Nom colonne	Taille colonne	Définition et relation entre les vues
sessionKey	bigint	Identifie la session d'agent auquel se rapporte cet enregistrement de l'agent de quarantaine. FK vers NACVP_Session

## 2.3 Application

La Vue SQL Application renvoie des données d'applications des stratégies définies dans le Compliance Manager. Cette Vue SQL contient une liste de toutes les applications et types d'applications signalés des agents.

**Nom de la Vue SQL pour les requêtes = NACVP\_Application**

Nom colonne	Taille colonne	Définition et relation entre les vues
applicationKey	bigint	PK
name	nvarchar(128)	Nom du système d'exploitation, du service pack, du correctif ou de l'application inclus dans la stratégie que l'agent a détectée sur l'ordinateur d'extrémité.
type	nvarchar(128)	Système d'exploitation, service pack, correctif ou type d'application inclus dans la stratégie que l'agent a détectée sur l'ordinateur d'extrémité.
versionNbr	int	Version de l'application que l'agent a détectée sur l'ordinateur d'extrémité.
applicationID	uniqueidentifier	Identifiant représentant une application. Les ID des applications sont des identifiants uniques générés de manière aléatoire. Un nouvel identifiant est affecté chaque fois qu'une application est mise à jour à l'aide de la fonctionnalité Save As New.

## 2.4 Action d'évaluation

La Vue SQL Assessment Action contient une liste consolidée d'actions d'évaluation. Les actions d'évaluation indiquent les actions exécutées sur chaque ordinateur d'extrémité par l'agent.

**Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentAction**

Nom colonne	Taille colonne	Définition et relation entre les vues
ruleKey	bigint	FK vers NACVP_AssessmentRule
resultKey	bigint	FK vers NACVP_AssessmentRule
type	nvarchar(128)	Type d'action d'actualisation qui était effectuée sur l'ordinateur d'extrémité. Des actions sont affichées ou

Nom colonne	Taille colonne	Définition et relation entre les vues
		<p>effectuées sur l'ordinateur d'extrémité seulement si la condition à laquelle l'action est associée est remplie. Les types d'actions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>Message</b> : affiche un message sur l'ordinateur d'extrémité. Cette action est disponible pour toutes les fonctionnalités.</li> <li>■ <b>Enable</b> : sur l'ordinateur d'extrémité, active la protection en temps réel pour les applications antivirus ou antispywares, active le pare-feu pour les applications pare-feu ou active les mises à jour automatiques pour les applications du gestionnaire de correctifs. Cette action est disponible pour la fonctionnalité d'application Real-Time Protection ou Enabled.</li> <li>■ <b>Update</b> : met à jour le fichier signature sur l'ordinateur d'extrémité. Cette action est disponible pour la fonctionnalité d'application Signature Date ou Signature Grace Period.</li> <li>■ <b>Scan</b> : lance un contrôle de moteur sur l'ordinateur d'extrémité. Cette action est disponible pour la fonctionnalité d'application Scan Date ou Scan Grace Period.</li> </ul>
paramValue	nvarchar(128)	Si le type est message, ce champ contient le texte du message qui était affiché sur l'ordinateur d'extrémité. Si le type est différent de message, ce champ est vide.

## 2.5 Profil d'évaluation

La Vue SQL Assessment Profile contient des informations sur les profils qui ont été signalés depuis les agents.

Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentProfile

Nom colonne	Taille colonne	Définition et relation entre les vues
profileKey	bigint	PK
resultKey	bigint	PK
name	nvarchar(128)	Nom du profil que l'agent a tenté de détecter sur l'ordinateur d'extrémité.
versionNbr	int	Version du profil qui a été évaluée par l'agent. Chaque fois que le profil est mis à jour, le numéro de version est mis à jour par incrémentation de un.

Nom colonne	Taille colonne	Définition et relation entre les vues
complianceState	nvarchar(128)	<p>État de conformité de profil. Cet état de conformité est composé des conditions de profil évaluées sur l'ordinateur d'extrémité. Toutes les conditions de profil sont évaluées pour déterminer l'état de conformité des profils. Les états de conformité disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>compliant</b> : l'évaluation a déterminé que le profil est conforme.</li> <li>■ <b>partial</b> : l'évaluation a déterminé que le profil est partiellement conforme.</li> <li>■ <b>nonCompliant</b> : l'évaluation a déterminé que le profil n'est pas conforme.</li> </ul>
installed :	bit	<p>Indique si l'élément de profil (système d'exploitation, correctif ou application) a été détecté sur l'ordinateur d'extrémité. Si la valeur est True, l'élément de profil a été détecté. Si la valeur est False, l'élément de profil n'a pas été détecté.</p>
selected	bit	<p>Spécifie si le profil a été utilisé pour déterminer l'état de conformité du type de profil. Si la valeur est True, ce profil a été utilisé. Si la valeur est False, ce profil n'a pas été utilisé ; à la place, un autre profil a été utilisé pour déterminer l'état de conformité.</p>
reason	nvarchar(128)	<p>Indique pourquoi le profil a été utilisé ou non pour déterminer l'état de conformité du type de profil. Ceci dépend du comportement de stratégie qui détermine comment les profils sont évalués par rapport aux profils du même type sur l'ordinateur d'extrémité. Les valeurs disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>Required</b> : indique si le profil de système d'exploitation requis est trouvé sur l'ordinateur d'extrémité. Le profil du système d'exploitation est requis et est évalué comme meilleur profil.</li> <li>■ <b>Best</b> : indique si le meilleur profil est trouvé sur l'ordinateur d'extrémité. Chaque profil d'un type particulier dans une stratégie est évalué sur l'ordinateur d'extrémité, la meilleure correspondance est déterminée, et seules les actions garanties associées au profil correspondant le mieux sont prises. Le comportement Best utilise le profil le plus conforme sur l'ordinateur d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Sauf indication contraire, les profils d'application sont évalués de cette manière.</li> <li>■ <b>Default</b> : indique si aucun profil dans une évaluation Best n'est trouvé sur l'ordinateur d'extrémité. Si aucun des profils évalués n'est installé sur l'ordinateur d'extrémité, alors l'état de</li> </ul>

Nom colonne	Taille colonne	Définition et relation entre les vues
		<p>conformité de la condition Else du profil ayant la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil dans la stratégie. Si l'un des systèmes d'exploitation n'est pas installé sur l'ordinateur d'extrémité, alors l'état de conformité de la condition Else du profil du système d'exploitation à la priorité la plus élevée est utilisé pour déterminer l'état de conformité et les actions du type de profil du système d'exploitation, et aucun profil supplémentaire n'est évalué pour cette stratégie.</p> <p>■ <b>All</b> : indique si tous les profils sont évalués sur l'ordinateur d'extrémité. Tous les profils d'un type particulier dans une stratégie sont évalués sur l'ordinateur d'extrémité, et les actions garanties associées à tous les profils sont prises. Le comportement All utilise le profil le moins conforme sur l'ordinateur d'extrémité pour déterminer l'état de conformité du type de profil dans la stratégie. Les profils de correctifs sont évalués de cette manière. Les profils d'applications que vous voulez empêcher sur l'ordinateur d'extrémité peuvent être évalués de cette manière.</p>
priority	int	Spécifie la priorité du profil dans le groupe de profils pour cette évaluation.
profileID	uniqueidentifier	Identifiant représentant un profil. Les ID des profils sont des identifiants uniques générés de manière aléatoire. Une nouvel identifiant est affecté chaque fois qu'un profil est mis à jour à l'aide de la fonctionnalité Save As New.
profileGroupKey	bigint	FK vers NACVP_AssessmentProfileGroup

## 2.6 Groupe de profils d'évaluation

La Vue SQL Assessment Profile Group contient des informations sur les groupes de profils qui ont été signalés depuis les agents.

**Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentProfileGroup**

Nom colonne	Taille colonne	Définition et relation entre les vues
profileGroupKey	bigint	PK
resultKey	bigint	PK

Nom colonne	Taille colonne	Définition et relation entre les vues
type	nvarchar(128)	Type de profil que l'agent a tenté de détecter sur l'ordinateur d'extrémité. Les types de profils incluent : Agent App, AntiSpyware, AVApp, IDS App, OS, Patch, PFW App et tous les profils d'applications personnalisés.
complianceState	nvarchar(128)	État de conformité du type de profil. Cet état de conformité est composé des profils évalués sur l'ordinateur d'extrémité conjointement au comportement de stratégie qui est Required, Best ou All. Les états de conformité disponibles sont : <ul style="list-style-type: none"> <li>■ <b>compliant</b> : l'évaluation a déterminé que le type de profil est conforme.</li> <li>■ <b>partial</b> : l'évaluation a déterminé que le type de profil est partiellement conforme.</li> <li>■ <b>nonCompliant</b> : l'évaluation a déterminé que le type de profil n'est pas conforme.</li> </ul>
assessmentKey	bigint	FK vers NACVP_AssessmentReport

## 2.7 Rapport d'évaluation

La Vue SQL Assessment Report contient des informations d'évaluation. Les informations d'évaluation indiquent les dates et les heures de début et de fin ainsi qu'une comptabilisation d'évaluation.

**Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentReport**

Nom colonne	Taille colonne	Définition et relation entre les vues
assessmentKey	bigint	PK
resultKey	bigint	PK
startDateTime	datetime	Date et heure de la première instance du résultat de l'évaluation de conformité dans l'intervalle temporel utilisé dans le rapport. L'évaluation inclut les opérations qui évaluent et appliquent la stratégie sur l'ordinateur d'extrémité. La fréquence de l'évaluation est basée sur l'intervalle d'évaluation et d'application défini dans la stratégie. La date et l'heure sont au temps moyen de Greenwich (GMT).
endDateTime	datetime	Date et heure de la dernière instance du résultat de l'évaluation de conformité dans l'intervalle temporel utilisé dans le rapport. L'évaluation inclut les opérations qui évaluent et appliquent la stratégie sur

Nom colonne	Taille colonne	Définition et relation entre les vues
		l'ordinateur d'extrémité. La date et l'heure sont au temps moyen de Greenwich (GMT).
complianceState	nvarchar(128)	<p>État de conformité de l'ordinateur d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>compliant</b> : l'évaluation a déterminé que l'ordinateur d'extrémité est conforme à la stratégie.</li> <li>■ <b>partial</b> : l'évaluation a déterminé que l'ordinateur d'extrémité est partiellement conforme à la stratégie.</li> <li>■ <b>nonCompliant</b> : l'évaluation a déterminé que l'ordinateur d'extrémité n'est pas conforme à la stratégie.</li> </ul> <p><b>Important</b> : l'état de conformité de l'ordinateur d'extrémité est déterminé par l'évaluation des conditions du profil sur l'ordinateur d'extrémité et par le comportement de la stratégie affectée pour ce type de profil. L'état de conformité de chaque condition est remonté jusqu'au niveau des profils et de nombreux profils sont remontés jusqu'au niveau des stratégies pour déterminer l'état de conformité global. L'état le moins conforme détermine l'état de conformité global. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.</p>
userGroup	nvarchar(128)	Groupe de l'utilisateur initialisant la session.
policyKey	bigint	FK vers NACVP_Policy
assessmentCount	int	Nombre d'évaluations de conformité qui ont eu lieu sans changement dans les résultats d'évaluation. Ce nombre correspond au nombre de fois que l'agent a effectué l'évaluation de conformité, d'après l'intervalle d'évaluation et d'application défini dans la stratégie.
lastAssessmentType	nvarchar(20)	Indique si la dernière évaluation a été initialisée par l'agent ou si elle a été manuellement initialisée par l'utilisateur.
lastFetchDateTime	datetime	Les dernières dates et heures auxquelles l'agent a vérifié l'existence d'une stratégie mise à jour sur le serveur d'applications de conformité. La date et l'heure proviennent du serveur d'applications de conformité et sont basés sur le fuseau horaire du serveur.
agentStartOffset	bigint	Décalage en date et en heure pouvant être utilisé pour calculer la date et l'heure véritables signalées par l'agent pour la première instance du résultat d'évaluation de

Nom colonne	Taille colonne	Définition et relation entre les vues
		conformité dans l'intervalle temporel utilisé dans le rapport. Cette date et cette heure peuvent être utilisées à la place de la date et de l'heure qui étaient réglées sur l'heure du serveur.
agentEndOffset	bigint	Décalage en date et en heure pouvant être utilisé pour calculer la date et l'heure de la dernière instance du résultat d'évaluation de conformité dans l'intervalle temporel utilisé sur le rapport. Cette date et cette heure peuvent être utilisées à la place de la date et de l'heure qui étaient réglées sur l'heure du serveur.
sessionKey	bigint	FK vers NACVP_Session

## 2.8 Règle d'évaluation

La Vue SQL Assessment Rule contient des informations sur les conditions qui ont été signalées depuis les agents.

Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentRule

Nom colonne	Taille colonne	Définition et relation entre les vues
ruleKey	bigint	PK
resultKey	bigint	PK
type	nvarchar(20)	Type de condition dans un système d'exploitation, correctif ou profil d'application. Les types de conditions incluent : default et nonDefault. La condition par défaut est une condition autre.
priority	int	Indique l'ordre dans lequel les conditions de profils sont évaluées. La condition autre est toujours avec la priorité la plus faible.
complianceState	nvarchar(128)	L'état de conformité de l'ordinateur d'extrémité est déterminé par l'évaluation des conditions du profil sur l'ordinateur d'extrémité et par le comportement de la stratégie affectée pour ce type de profil. L'état de conformité de chaque condition est remonté jusqu'au niveau des profils et de nombreux profils sont remontés jusqu'au niveau des stratégies pour déterminer l'état de conformité global. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.  <ul style="list-style-type: none"> <li>■ <b>compliant</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est conforme.</li> </ul>

Nom colonne	Taille colonne	Définition et relation entre les vues
		<ul style="list-style-type: none"> <li>■ <b>partial</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est partiellement conforme.</li> <li>■ <b>nonCompliant</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est non conforme.</li> </ul>
conditionResult	bit	Résultat de l'évaluation de la condition. Si le résultat est True, la condition définie dans le profil a été remplie sur l'ordinateur d'extrémité. Si le résultat est False, la condition définie dans le profil n'a pas été remplie sur l'ordinateur d'extrémité.
policyValue	nvarchar(128)	Valeur de la condition qui a été configurée dans le profil.
policyOperator	nvarchar(20)	Opérateur de la condition qui a été configurée dans le profil.
outputValue	nvarchar(128)	Affiche le résultat qui a été détecté sur l'ordinateur d'extrémité lors d'une comparaison qui a été configurée dans le profil. Le résultat peut être une version, un nombre ou une date, ou tout autre élément qui délimite la condition sur l'ordinateur d'extrémité.
servicePackKey	bigint	FK vers NACVP_ServicePack
ruleGroupKey	bigint	FK vers NACVP_AssessmentRuleGroup

## 2.9 Groupe de règles d'évaluation

La Vue SQL Assessment Rule Group contient des informations sur les groupes de règles qui ont été signalés depuis les agents.

**Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentRuleGroup**

Nom colonne	Taille colonne	Définition et relation entre les vues
ruleGroupKey	bigint	PK
resultKey	bigint	PK
type	nvarchar(128)	Identifie le type de groupe de conditions évaluées. Les états disponibles sont : <ul style="list-style-type: none"> <li>■ <b>Exists</b> : type de groupe de conditions qui vérifie les conditions installées.</li> <li>■ <b>Capability</b> : type de groupe de conditions qui vérifie les fonctionnalités.</li> </ul>

Nom colonne	Taille colonne	Définition et relation entre les vues
complianceState	nvarchar(128)	Identifie l'état de conformité des conditions. Les états de conformité disponibles sont : <ul style="list-style-type: none"> <li>■ <b>compliant</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est conforme.</li> <li>■ <b>partial</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est partiellement conforme.</li> <li>■ <b>nonCompliant</b> : la condition a été remplie lors de l'évaluation, et l'état de conformité associé est non conforme.</li> </ul>
applicationKey	bigint	FK vers NACVP_Application
osKey	bigint	FK vers NACVP_OS
profileKey	bigint	FK vers NACVP_Profile

## 2.10 Séquence d'évaluation

La Vue SQL Assessment Sequence contient des clés pour joindre la Vue SQL Assessment Report et générer un rapport semblable au rapport des changements de conformité du Compliance Manager. Cette Vue SQL permet d'identifier les relations précédentes et suivantes des entrées du rapport d'évaluation à l'aide du même nom utilisateur/AgentID.

**Nom de la Vue SQL pour les requêtes = NACVP\_AssessmentSequence**

Nom colonne	Taille colonne	Définition et relation entre les vues
assessmentKey	bigint	FK vers NACVP_AssessmentReport
prevAssessmentKey	bigint	FK vers NACVP_AssessmentReport

## 2.11 DHCP Enforcer

La Vue SQL DHCP Enforcer renvoie les données de rapports capturées par le RADIUS Enforcer pour les requêtes DHCP.

**Nom de la Vue SQL pour les requêtes = NACVP\_DHCPEnforcer**

Nom de colonne	Taille de colonne	Définition et relation entre les vues
dhcpKey	bigint	PK
accessDateTime	datetime	Date et heure de la tentative d'accès réseau. La date et l'heure sont au temps moyen de Greenwich (GMT).

Nom de colonne	Taille de colonne	Définition et relation entre les vues
macAddress	nvarchar(128)	Adresse MAC du périphérique tentant de se connecter au réseau. L'adresse MAC qui apparaît est affectée au NIC associé à la requête DHCP du client.
username	nvarchar(128)	Nom de l'utilisateur initialisant la tentative d'accès réseau.
agentID	nvarchar(36)	Identifiant de l'installation de l'agent ou de l'ordinateur d'extrémité auquel l'utilisateur est connecté.
hostname	nvarchar(128)	Nom du périphérique tentant de se connecter au réseau. Le nom d'hôte est dérivé de la demande du client.
complianceState	nvarchar(128)	<p>État de conformité de l'ordinateur d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>compliant:</b> l'évaluation a déterminé que l'ordinateur d'extrémité est conforme à la stratégie. Les modèles d'accès DHCP Enforcer conformes associés à la stratégie déterminent l'accès réseau.</li> <li>■ <b>partial:</b> l'évaluation a déterminé que l'ordinateur d'extrémité est partiellement conforme à la stratégie. Les modèles d'accès DHCP Enforcer partiellement conformes associés à la stratégie déterminent l'accès réseau.</li> <li>■ <b>nonCompliant:</b> l'évaluation a déterminé que l'ordinateur d'extrémité n'est pas conforme à la stratégie. Les modèles d'accès DHCP Enforcer non conformes associés à la stratégie déterminent l'accès réseau.</li> </ul> <p><b>Important :</b> l'état de conformité de l'ordinateur d'extrémité est déterminé par l'évaluation des conditions du profil sur l'ordinateur d'extrémité et par le comportement de la stratégie affectée pour ce type de profil. L'état de conformité de chaque condition est remonté jusqu'au niveau des profils et de nombreux profils sont remontés jusqu'au niveau des stratégies pour déterminer l'état de conformité global. L'état le moins conforme détermine l'état de conformité global. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.</p>
returnedUserClass	nvarchar(128)	Classe d'utilisateur DHCP renvoyée au serveur DHCP par le DHCP Enforcer pour application.
sourceUserClass	nvarchar(128)	Classe utilisateur DHCP qui, si elle existe, est envoyée au serveur DHCP depuis le client DHCP.

Nom de colonne	Taille de colonne	Définition et relation entre les vues
vendorClass	nvarchar(128)	Classe du fournisseur du client DHCP.
templateName	nvarchar(128)	Nom et version du modèle d'accès qui détermine l'action prise par le DHCP Enforcer. Le modèle d'accès utilisé est basé sur la raison.
reason	nvarchar(20)	<p>Raison pour laquelle un modèle d'accès particulier a été affecté par le DHCP Enforcer. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>Assessment:</b> l'évaluation effectuée par l'agent a déterminé l'état de conformité. Les modèles d'accès DHCP Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau.</li> <li>■ <b>Default Template:</b> l'ordinateur d'extrémité peut avoir une stratégie associée ou être une exemption désignée, mais aucun modèle d'accès associé n'a été trouvé. Les modèles d'accès Default désignés dans la zone Configure System &gt; Enforcer Settings sont utilisés pour déterminer l'accès réseau.</li> <li>■ <b>Enforcer Override:</b> la mise en application n'a pas été vérifiée. Si la case à cocher Override Enforcers est sélectionnée dans la zone Configure System &gt; Enforcer Settings, les modèles d'accès Maintenance Mode/Enforcer Override aussi désignés dans cette zone servent à déterminer l'accès réseau.</li> <li>■ <b>Exempted:</b> l'ordinateur d'extrémité est exempté selon les critères d'exemption définis dans la zone Enforce &gt; Exemptions. Les modèles d'accès associés aux critères d'exemption servent à déterminer l'accès réseau.</li> <li>■ <b>Maintenance Mode:</b> le logiciel est en mode de maintenance. Les modèles d'accès Maintenance Mode/Enforcer Override désignés dans la zone Configure System &gt; Enforcer Settings déterminent l'accès réseau.</li> <li>■ <b>Policy Retrieval Error:</b> l'état de conformité de l'ordinateur d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone Configure System &gt; Enforcer Settings. Les modèles d'accès DHCP Enforcer de la stratégie associés à l'état Policy Retrieval Error déterminent l'accès réseau.</li> <li>■ <b>Reserved:</b> l'adresse MAC du périphérique demandant l'accès réseau est réservé pour un périphérique particulier sur le serveur DHCP.</li> <li>■ <b>System Error:</b> Enforcer a rencontré une erreur qui a empêché le succès de l'opération. Le paramètre du registre SystemErrors sur le serveur</li> </ul>

Nom de colonne	Taille de colonne	Définition et relation entre les vues
		<p>d'applications de conformité est défini par défaut pour refuser l'accès réseau.</p> <ul style="list-style-type: none"> <li>■ <b>Template Error:</b> un modèle d'accès associé était introuvable et les modèles d'accès Default désignés dans la zone Configure System &gt; Enforcer Settings ne pouvaient pas être utilisés. Si cette erreur est reçue, l'accès réseau est déterminé par le serveur DHCP, lequel renvoie une réponse de rejet RADIUS sans classe d'utilisateurs définie et refuse l'accès à l'utilisateur.</li> <li>■ <b>Unknown Endpoint:</b> aucun enregistrement de conformité n'existe. Les modèles d'accès Unknown Endpoint désignés dans la zone Configure System &gt; Enforcer Settings déterminent l'accès réseau.</li> </ul>
exemptionReason	nvarchar(20)	<p>Spécifie le motif d'exemption. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>User Class:</b> la classe d'utilisateur a été spécifiée comme une exemption.</li> <li>■ <b>Vendor Class:</b> la classe du fournisseur a été spécifiée comme une exemption.</li> <li>■ <b>MAC Address:</b> l'adresse MAC a été spécifiée comme une exemption.</li> <li>■ <b>IP Scope:</b> l'étendue IP a été spécifiée comme une exemption.</li> </ul>
clientAction	nvarchar(128)	<p>Action prise par l'ordinateur d'extrémité. L'ordinateur d'extrémité initialise la publication et le renouvellement des adresses IP d'après l'action d'application d'agents spécifiée dans la stratégie. L'agent obtient de nouvelles adresses IP lorsqu'il lance et initialise une évaluation de conformité, lorsque l'état de conformité de l'ordinateur d'extrémité change et lorsque les modèles d'accès DHCP Enforcer définis dans la stratégie de l'ordinateur d'extrémité changent. Les valeurs disponibles incluent :</p> <ul style="list-style-type: none"> <li>■ <b>None:</b> les adresses IP de l'ordinateur d'extrémité ne sont ni publiées ni renouvelées.</li> <li>■ <b>ReleaseRenew:</b> les adresses IP de l'ordinateur d'extrémité sont publiées, puis renouvelées à l'aide du serveur DHCP. Les adresses IP courantes sont laissées de côté avant l'obtention de nouvelles.</li> <li>■ <b>NULL Value:</b> l'agent n'a pas signalé d'action.</li> </ul>

Nom de colonne	Taille de colonne	Définition et relation entre les vues
nasIPAddress	nvarchar(15)	Adresse IP du serveur DHCP demandant l'accès réseau depuis le DHCP Enforcer. Il s'agit du serveur DHCP sur lequel le logiciel DHCP Enforcer est installé.
selectionIPAddress	nvarchar(15)	Adresse IP du relais DHCP (s'il est présent dans la requête DHCP originale) utilisé par le DHCP Enforcer pour sélectionner un modèle d'accès DHCP Enforcer.
exemptionCondition	nvarchar(128)	Nom de l'exemption et critères d'exemption.
transactionID	nvarchar(128)	Identifiant de transaction renvoyé depuis le serveur DHCP. L'identifiant de transaction associe les messages du client DHCP avec les réponses du serveur.
count	int	Spécifie le nombre de demandes DHCP uniques qui ont été traitées pour cet enregistrement.
assessmentKey	bigint	Identifie la session d'agent et l'évaluation auxquelles se rapporte cet enregistrement DHCP Enforcer. FK vers NACVP_AssessmentReport

## 2.12 Système d'exploitation

La Vue OS SQL renvoie des informations relatives au système d'exploitation telles qu'elles sont définies à l'aide du Compliance Manager. Cette Vue SQL contient une liste de tous les types de systèmes d'exploitation signalés des agents.

**Nom de la Vue SQL pour les requêtes = NACVP\_OS**

Nom colonne	Taille colonne	Définition et relation entre les vues
osKey	bigint	PK
name	nvarchar(128)	Nom du système d'exploitation inclus dans la stratégie que l'agent a détectée sur l'ordinateur d'extrémité.

## 2.13 Correctif

La Vue SQL Patch renvoie des informations relatives au correctif telles qu'elles sont définies dans le Compliance Manager. Cette Vue SQL contient une liste de tous les correctifs qui ont été signalés depuis les agents.

**Nom de la Vue SQL pour les requêtes = NACVP\_Patch**

Nom colonne	Taille colonne	Définition et relation entre les vues
patchKey	bigint	PK

Nom colonne	Taille colonne	Définition et relation entre les vues
name	nvarchar(128)	Nom du correctif inclus dans la stratégie que l'agent a détectée sur l'ordinateur d'extrémité.

## 2.14 Résultat de correctif

La Vue SQL Patch Result contient des informations sur les résultats des correctifs qui ont été signalées depuis les agents.

Nom de la Vue SQL pour les requêtes = NACVP\_PatchResult

Nom colonne	Taille colonne	Définition et relation entre les vues
patchKey	bigint	FK vers NACVP_Patch
ruleKey	bigint	FK vers NACVP_AssessmentRule
resultKey	bigint	FK vers NACVP_AssessmentRule
conditionResult	bit	Résultat de la condition du correctif. Si le résultat est True, la condition a été remplie. Si le résultat est False, la condition n'a pas été remplie.
outputValue	nvarchar(128)	Valeur du correctif depuis la stratégie que l'agent a détectée sur l'ordinateur d'extrémité lors de l'évaluation. La outputValue est True si l'agent a déterminé que le correctif a été installé ou n'était pas requis et False si l'agent a déterminé que le correctif n'a pas été installé. La outputValue est la chaîne de caractères {null} si l'agent n'a pas évalué si oui ou non le correctif était installé.  <b>Remarque :</b> l'agent temporaire n'évalue pas les correctifs si l'utilisateur est connecté en tant qu'utilisateur avec restrictions.

## 2.15 Stratégie

La Vue SQL Policy contient des informations sur toutes les stratégies qui ont été signalées depuis les agents.

Nom de la Vue SQL pour les requêtes = NACVP\_Policy

Nom colonne	Taille colonne	Définition et relation entre les vues
policyKey	bigint	PK
name	nvarchar(128)	Nom de la stratégie qui a été évaluée par l'agent.

Nom colonne	Taille colonne	Définition et relation entre les vues
versionNbr	int	Version de la stratégie qui a été évaluée par l'agent. Chaque fois que la stratégie est mise à jour, le numéro de version est mis à jour par incrémentation de un.
mode	nvarchar(128)	Mode de la stratégie qui a été évaluée par l'agent. Les modes de stratégie sont : enforce, remediate et report.
policyID	uniqueidentifier	Les ID des stratégies sont des identifiants uniques générés de manière aléatoire. Un nouvel identifiant est affecté chaque fois qu'une stratégie est mise à jour à l'aide de la fonctionnalité Save As New.

## 2.16 RADIUS Enforcer

La Vue SQL RADIUS Enforcer renvoie les données de rapports capturées par le RADIUS Enforcer pour les requêtes avec authentification normale.

Nom de la Vue SQL pour les requêtes = NACVP\_RADIUSEnforcer

Nom de colonne	Taille de colonne	Définition et relation entre les vues
RADIUSKey	bigint	PK
accessDateTime	datetime	Date et heure de la tentative d'accès réseau. La date et l'heure sont au temps moyen de Greenwich (GMT).
username	nvarchar(128)	Nom de l'utilisateur initialisant la tentative d'accès réseau.
userGroup	nvarchar(128)	Groupe de l'utilisateur initialisant la tentative d'accès réseau.
complianceState	nvarchar(128)	État de conformité de l'ordinateur d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont : <ul style="list-style-type: none"> <li>■ <b>compliant:</b> l'évaluation a déterminé que l'ordinateur d'extrémité est conforme à la stratégie. Les modèles d'accès RADIUS Enforcer conformes associés à la stratégie déterminent l'accès réseau.</li> <li>■ <b>partial:</b> l'évaluation a déterminé que l'ordinateur d'extrémité est partiellement conforme à la stratégie. Les modèles d'accès RADIUS Enforcer partiellement conformes associés à la stratégie déterminent l'accès réseau.</li> <li>■ <b>nonCompliant:</b> l'évaluation a déterminé que l'ordinateur d'extrémité n'est pas conforme à la stratégie. Les modèles d'accès RADIUS Enforcer non conformes associés à la stratégie déterminent l'accès réseau.</li> </ul>

Nom de colonne	Taille de colonne	Définition et relation entre les vues
		<p><b>Important :</b> l'état de conformité de l'ordinateur d'extrémité est déterminé par l'évaluation des conditions du profil sur l'ordinateur d'extrémité et par le comportement de la stratégie affectée pour ce type de profil. L'état de conformité de chaque condition est remonté jusqu'au niveau des profils et de nombreux profils sont remontés jusqu'au niveau des stratégies pour déterminer l'état de conformité global. L'état le moins conforme détermine l'état de conformité global. Une fois qu'un état de conformité est déterminé, l'accès réseau basé sur cet état de conformité peut être appliqué à l'aide des modèles d'accès affectés dans la stratégie.</p>
reason	nvarchar(20)	<p>Raison pour laquelle un modèle d'accès particulier a été affecté par le RADIUS Enforcer. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>Assessment:</b> l'évaluation effectuée par l'agent a déterminé l'état de conformité. Les modèles d'accès RADIUS Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau.</li> <li>■ <b>Default Template:</b> l'ordinateur d'extrémité peut avoir une stratégie associée ou être une exemption désignée, mais aucun modèle d'accès associé n'a été trouvé. Les modèles d'accès Default désignés dans la zone Configure System &gt; Enforcer Settings sont utilisés pour déterminer l'accès réseau.</li> <li>■ <b>Enforcer Override:</b> la mise en application n'a pas été vérifiée. Si la case à cocher Disable Enforcer est sélectionnée dans la zone Configure System &gt; Enforcer Settings, les modèles d'accès Maintenance Mode/Enforcer Override aussi désignés dans cette zone servent à déterminer l'accès réseau.</li> <li>■ <b>Exempted:</b> l'ordinateur d'extrémité est exempté selon les critères d'exemption définis dans la zone Enforce &gt; Exemptions. Les modèles d'accès associés aux critères d'exemption servent à déterminer l'accès réseau.</li> <li>■ <b>Maintenance Mode:</b> le logiciel est en mode de maintenance. Les modèles d'accès Maintenance Mode/Enforcer Override désignés dans la zone Configure System &gt; Enforcer Settings déterminent l'accès réseau.</li> <li>■ <b>Policy Retrieval Error:</b> l'état de conformité de l'ordinateur d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone Configure System &gt; Enforcer Settings. Les modèles d'accès RADIUS Enforcer de la</li> </ul>

Nom de colonne	Taille de colonne	Définition et relation entre les vues
		<p>stratégie associés à l'état Policy Retrieval Error déterminent l'accès réseau.</p> <ul style="list-style-type: none"> <li>■ <b>System Error:</b> Enforcer a rencontré une erreur qui a empêché le succès de l'opération. Le paramètre du registre SystemErrors sur le serveur d'applications de conformité est défini par défaut pour refuser l'accès réseau.</li> <li>■ <b>Template Error:</b> un modèle d'accès associé était introuvable et les modèles d'accès Default désignés dans la zone Configure System &gt; Enforcer Settings ne pouvaient pas être utilisés. Si cette erreur est reçue, l'accès réseau est déterminé par le serveur DHCP, lequel renvoie une réponse de rejet RADIUS sans classe d'utilisateurs définie et refuse l'accès à l'utilisateur.</li> <li>■ <b>Unknown Endpoint:</b> aucun enregistrement de conformité n'existe. Les modèles d'accès Unknown Endpoint désignés dans la zone Configure System &gt; Enforcer Settings déterminent l'accès réseau.</li> </ul>
exemptionReason	nvarchar(20)	<p>Spécifie le motif d'exemption. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> <li>■ <b>User Name:</b> le nom utilisateur a été spécifié comme une exemption.</li> <li>■ <b>User Group:</b> le groupe d'utilisateurs a été spécifié comme une exemption.</li> </ul>
templateName	nvarchar(128)	<p>Nom et version du modèle d'accès qui a déterminé l'action prise par le RADIUS Enforcer. Le modèle d'accès utilisé est basé sur la raison.</p>
nasIPAddress	nvarchar(15)	<p>Adresse IP du dispositif demandant l'authentification de l'accès réseau depuis RADIUS Enforcer. Le dispositif peut être un RAC (Remote Access Concentrator), un routeur, un commutateur ou tout autre dispositif de réseau.</p>
clientIdentifier	nvarchar(50)	<p>Identifiant du périphérique tentant de se connecter au réseau. L'identifiant est une chaîne de caractères qui identifie le dispositif, comme une adresse MAC, et qui est dérivé de la demande client RADIUS.</p>
exemptionCondition	nvarchar(128)	<p>Nom de l'exemption et critères d'exemption.</p>
assessmentKey	bigint	<p>Identifie la session d'agent et l'évaluation auxquelles se rapporte cet enregistrement RADIUS Enforcer.</p> <p>FK vers NACVP_AssessmentReport</p>

Nom de colonne	Taille de colonne	Définition et relation entre les vues
clientAction	nvarchar(20)	<p>Action prise par l'ordinateur d'extrémité lorsqu'il est affecté à un réseau local virtuel de quarantaine. L'ordinateur d'extrémité initialise la nouvelle authentification en fonction de l'action d'application d'agents spécifiée dans la stratégie. L'agent authentifie de nouveau l'ordinateur d'extrémité lorsqu'il lance et initialise une évaluation de conformité, lorsque l'état de conformité de l'ordinateur d'extrémité change, lorsque le mode de stratégie change et lorsque les modèles d'accès RADIUS Enforcer définis dans la stratégie de l'ordinateur d'extrémité changent. Les valeurs disponibles incluent :</p> <ul style="list-style-type: none"> <li>■ <b>None:</b> l'ordinateur d'extrémité n'est pas automatiquement authentifié de nouveau lorsqu'il est affecté à un réseau local virtuel de quarantaine. L'utilisateur de l'ordinateur d'extrémité doit exécuter un script spécialisé pour réauthentifier l'ordinateur d'extrémité.</li> <li>■ <b>Toggle:</b> l'ordinateur d'extrémité n'est pas automatiquement authentifié de nouveau lorsqu'il est affecté à un réseau local virtuel de quarantaine. Si l'ordinateur d'extrémité est conforme à la stratégie, il est affecté à un réseau local virtuel conforme au moment de la nouvelle authentification, comme le désignent les modèles d'accès RADIUS Enforcer.</li> <li>■ <b>NULL:</b> l'agent n'a pas signalé d'action.</li> </ul>

## 2.17 Service Pack

La Vue SQL Service Pack contient des informations sur les résultats des service packs qui ont été signalés depuis les agents.

Nom de la Vue SQL pour les requêtes = NACVP\_ServicePack

Nom colonne	Taille colonne	Définition et relation entre les vues
servicePackKey	bigint	PK
name	nvarchar(128)	Nom du service pack inclus dans la stratégie que l'agent a détectée sur l'ordinateur d'extrémité.

## 2.18 Session

La Vue SQL Session est une vue des données des rapports de l'agent contenant des informations sur chaque session de l'agent ainsi que des informations détaillées concernant l'ordinateur

d'extrémité sur lequel l'agent est installé. Une session commence lorsque l'utilisateur se connecte à l'agent et se termine lorsqu'il se déconnecte de l'agent.

**Nom de la Vue SQL pour les requêtes = NACVP\_Session**

Nom de colonne	Taille de colonne	Définition et relation entre les vues
sessionKey	bigint	PK
startDateTime	datetime	Date et heure auxquelles le premier utilisateur sur un ordinateur d'extrémité s'est connecté à l'agent. La date et l'heure sont au temps moyen de Greenwich (GMT).
endDateTime	datetime	Date et heure de fin de session du dernier agent fonctionnant sur un ordinateur d'extrémité. Une valeur NULL signifie que la session d'agent n'est pas terminée. La date et l'heure du temps moyen de Greenwich (GMT).
username	nvarchar(128)	Nom de l'utilisateur ouvrant la session.
agentID	nvarchar(36)	Identifiant de l'installation de l'agent ou de l'ordinateur d'extrémité à partir duquel la session est lancée. L'identifiant de l'agent est un GUID généré par logiciel qui identifie de manière unique chaque installation d'agent.
agentVersion	nvarchar(20)	Version de l'agent installé sur l'ordinateur d'extrémité.
hostname	nvarchar(128)	Nom de l'ordinateur d'extrémité sur lequel l'agent est installé.
osPlatformName	nvarchar(128)	Système d'exploitation installé sur l'ordinateur d'extrémité.
servicePackName	nvarchar(128)	Nom du service pack du système d'exploitation Microsoft installé sur l'ordinateur d'extrémité.
designation	nvarchar(128)	Affiche différentes variantes du même système d'exploitation. Par exemple, Edition familiale, Professionnel et Small Business.
sessionType	nvarchar(50)	Type d'agent initialisant la session. Les types de sessions incluent l'agent permanent ou l'agent temporaire. Le type de session Continu inclut l'agent de quarantaine.
wanIPAddress	nvarchar(15)	Adresse source de la communication entre l'agent et le serveur d'applications de conformité.

## 2.19 Session NIC

La Vue SQL Session NIC contient les adresses MAC et les adresses IP de toutes les cartes réseau (NIC, Network Interface Cards) trouvées sur un ordinateur d'extrémité lors d'une session. Généralement, un ordinateur d'extrémité a plus d'une adresse MAC et IP par session.

**Nom de la Vue SQL pour les requêtes = NACVP\_SessionNIC**

Nom colonne	Taille colonne	Définition et relation entre les vues
sessionKey	bigint	FK vers NACVP_Session
ipAddress	nvarchar(15)	Adresses IP de l'ordinateur d'extrémité sur lequel l'agent est installé. Dans le rapport, chaque adresse IP est affectée au même NIC que l'adresse MAC située à côté. Si le NIC n'a pas d'adresse IP, cette valeur est laissée vierge.
macAddress	nvarchar(128)	Adresses MAC de l'ordinateur d'extrémité sur lequel l'agent est installé. Dans le rapport, chaque adresse MAC est affectée au même NIC que l'adresse IP située à côté.



## 4 Annexe A : exemples de Vues SQL

Cette section contient des exemples d'utilisation et de jonction des Vues SQL pour produire les informations requises du rapport Sophos NAC Advanced.

### 4.1 Exemple de session d'agent

Le rapport Agent Session du Compliance Manager est semblable à cet exemple.

```
SELECT s.sessionKey, s.startDateTime, s.endDateTime,
       s.username, s.agentID, s.hostname, s.osPlatformName
FROM NACVP_Session s
ORDER BY s.startDateTime DESC

SELECT s.sessionKey, sn.macAddress, sn.ipAddress
FROM NACVP_SessionNIC sn
INNER JOIN NACVP_Session s ON s.sessionKey = sn.sessionKey
ORDER BY s.startDateTime DESC

SELECT ar.sessionKey, ar.assessmentKey, ar.startDateTime,
       ar.endDateTime, ar.assessmentCount, ar.complianceState,
       p.name, p.versionNbr, ar.userGroup
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
ORDER BY s.startDateTime DESC, ar.startDateTime

SELECT ar.assessmentKey,
       CASE WHEN COUNT(ae.sessionKey) > 0 THEN 'true'
       ELSE 'false'
       END AS agentEnforcerLink,
       CASE WHEN COUNT(re.assessmentKey) > 0 THEN 'true'
       ELSE 'false'
       END AS radiusEnforcerLink,
       CASE WHEN COUNT(de.assessmentKey) > 0 THEN 'true'
       ELSE 'false'
       END AS dhcpEnforcerLink
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
LEFT OUTER JOIN NACVP_RADIUSEnforcer re
  ON re.assessmentKey = ar.assessmentKey
LEFT OUTER JOIN NACVP_AgentEnforcer ae
  ON ae.sessionKey = ar.sessionKey
LEFT OUTER JOIN NACVP_DHCPEnforcer de
  ON de.assessmentKey = ar.assessmentKey
GROUP BY ar.assessmentKey, s.startDateTime, ar.startDateTime
ORDER BY s.startDateTime DESC, ar.startDateTime
```

## 4.2 Exemple de version d'agent

Le Compliance Manager ne dispose pas de rapport semblable à cet exemple.

```
SELECT s.agentVersion, ar.userGroup, s.username,
       s.agentID, ar.startDateTime
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
WHERE ar.startDateTime = (SELECT MAX(ar2.startDateTime)
                          FROM NACVP_AssessmentReport ar2
                          INNER JOIN NACVP_Session s2
                          ON s2.sessionKey = ar2.sessionKey
                          WHERE s2.username = s.username
                          AND s2.agentID = s.agentID
                          GROUP BY s2.username, s2.agentID)
ORDER BY s.agentVersion, ar.userGroup, s.username, s.agentID,
         ar.startDateTime
```

## 4.3 Exemple de récapitulatif de version d'agent

Le Compliance Manager ne dispose pas de rapport semblable à cet exemple.

```
CREATE TABLE #summary
(
  agentVersion nvarchar(20),
  agentVersionCount int,
  userGroup nvarchar(128),
  userGroupCount int
)

INSERT INTO #summary
SELECT s.agentVersion, 0, ar.userGroup, COUNT(ar.userGroup)
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
WHERE ar.startDateTime = (SELECT MAX(ar2.startDateTime)
                          FROM NACVP_AssessmentReport ar2
                          INNER JOIN NACVP_Session s2
                          ON s2.sessionKey = ar2.sessionKey
                          WHERE s2.username = s.username
                          AND s2.agentID = s.agentID
                          GROUP BY s2.username, s2.agentID)
GROUP BY s.agentVersion, ar.userGroup

UPDATE #summary
SET agentVersionCount = (
  SELECT SUM(s.userGroupCount)
  FROM #summary s
  WHERE #summary.agentVersion = s.agentVersion
  GROUP BY s.agentVersion
)
```

```
SELECT * FROM #summary
ORDER BY agentVersion, userGroup

DROP TABLE #summary
```

## 4.4 Exemple de détail d'agent

Le rapport Application Detail du Compliance Manager est semblable à cet exemple.

```
CREATE TABLE #lastAssessment
(
  assessmentKey bigint,
  username nvarchar(128),
  agentID nvarchar(128),
  endDateTime datetime,
  osPlatformName nvarchar(128),
  userGroup nvarchar(128)
)

INSERT INTO #lastAssessment
SELECT ar.assessmentKey, s.username, s.agentID, ar.endDateTime,
       s.osPlatformName, ar.userGroup
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
WHERE ar.endDateTime = (
  SELECT MAX(ar2.endDateTime)
  FROM NACVP_AssessmentReport ar2
  INNER JOIN NACVP_Session s2 ON s2.sessionKey = ar2.sessionKey
  WHERE s2.username = s.username
  AND s2.agentID = s.agentID
  GROUP BY s2.username, s2.agentID
)

CREATE TABLE #results
(
  type nvarchar(128),
  name nvarchar(128),
  version nvarchar(128),
  operatingSystem nvarchar(128),
  groupName nvarchar(128),
  username nvarchar(128),
  agentID uniqueidentifier,
  assessmentDateTime datetime
)

-- This is for Apps
INSERT INTO #results
(type, name, version, operatingSystem, groupName, username,
 agentID, assessmentDateTime)
SELECT a.type, a.name, aru.outputValue, ar.osPlatformName,
       ar.userGroup, ar.username, ar.agentID, ar.endDateTime
```

```
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey AND arg.type = 'installed'
INNER JOIN NACVP_Application a
  ON a.applicationKey = arg.applicationKey
LEFT OUTER JOIN NACVP_AssessmentRuleGroup arg2
  ON arg2.profileKey = ap.profileKey
  AND arg2.resultKey = ap.resultKey AND arg2.type = 'version'
LEFT OUTER JOIN NACVP_AssessmentRule aru
  ON aru.ruleGroupKey = arg2.ruleGroupKey
  AND aru.resultKey = arg2.resultKey
WHERE ap.installed = 1

-- This is for OSes
INSERT INTO #results
(type, name, version, operatingSystem, groupName, username,
agentID, assessmentDateTime)
SELECT 'OS' AS type, o.name, aru.outputValue, ar.osPlatformName,

  ar.userGroup, ar.username, ar.agentID, ar.endDateTime
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey AND arg.type = 'installed'
INNER JOIN NACVP_OS o ON o.osKey = arg.osKey
LEFT OUTER JOIN NACVP_AssessmentRuleGroup arg2
  ON arg2.profileKey = ap.profileKey
  AND arg2.resultKey = ap.resultKey AND arg.type = 'version'
LEFT OUTER JOIN NACVP_AssessmentRule aru
  ON aru.ruleGroupKey = arg2.ruleGroupKey
  AND aru.resultKey = arg2.resultKey
WHERE ap.installed = 1

-- This is for service packs
INSERT INTO #results
(type, name, version, operatingSystem, groupName, username,
agentID, assessmentDateTime)
SELECT 'servicePack' AS type, sp.name, NULL AS outputValue,
  ar.osPlatformName, ar.userGroup, ar.username, ar.agentID,
  ar.endDateTime
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
INNER JOIN NACVP_AssessmentProfile ap
```

```

    ON ap.profileGroupKey = apg.profileGroupKey
    AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
    ON arg.profileKey = ap.profileKey
    AND arg.resultKey = ap.resultKey AND arg.type = 'servicePack'
INNER JOIN NACVP_AssessmentRule aru
    ON aru.ruleGroupKey = arg.ruleGroupKey
    AND aru.resultKey = arg.resultKey
INNER JOIN NACVP_ServicePack sp
    ON sp.servicePackKey = aru.servicePackKey
WHERE aru.conditionResult = 1

-- This is for patches
INSERT INTO #results
(type, name, version, operatingSystem, groupName, username,
agentID, assessmentDateTime)
SELECT 'patch' AS type, p.name, NULL AS outputValue,
    ar.osPlatformName, ar.userGroup, ar.username, ar.agentID,
    ar.endDateTime
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
    ON apg.assessmentKey = ar.assessmentKey
INNER JOIN NACVP_AssessmentProfile ap
    ON ap.profileGroupKey = apg.profileGroupKey
    AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
    ON arg.profileKey = ap.profileKey
    AND arg.resultKey = ap.resultKey
INNER JOIN NACVP_AssessmentRule aru
    ON aru.ruleGroupKey = arg.ruleGroupKey
    AND aru.resultKey = arg.resultKey
INNER JOIN NACVP_PatchResult pr
    ON pr.ruleKey = aru.ruleKey
    AND pr.resultKey = aru.resultKey
INNER JOIN NACVP_Patch p ON p.patchKey = pr.patchKey
WHERE pr.conditionResult = 1
SELECT * from #results
ORDER BY type, name, operatingSystem, version, groupName,
    username, agentID

DROP TABLE #results
DROP TABLE #lastAssessment

```

## 4.5 Exemple de récapitulatif d'application

Le rapport Application Summary du Compliance Manager est semblable à cet exemple.

```

CREATE TABLE #lastAssessment
(
assessmentKey bigint,
resultKey bigint,
userGroup nvarchar(128)
)

```

```
INSERT INTO #lastAssessment
(assessmentKey, resultKey, userGroup)
SELECT ar.assessmentKey, ar.resultKey, ar.userGroup
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
WHERE ar.endDateTime = (
    SELECT MAX(ar2.endDateTime)
    FROM NACVP_AssessmentReport ar2
    INNER JOIN NACVP_Session s2 ON s2.sessionKey = ar2.sessionKey

    WHERE s2.username = s.username
    AND s2.agentID = s.agentID
    GROUP BY s2.username, s2.agentID
)

CREATE TABLE #summary
(
    appType nvarchar(128),
    appTypeCount int,
    appName nvarchar(128),
    appNameCount int,
    appVer nvarchar(128),
    appVerCount int,
    groupName nvarchar(128),
    groupNameCount int
)

-- This is for Apps
INSERT into #summary
SELECT a.type, 0, a.name, 0, aru.outputValue, 0,
    ar.userGroup, COUNT(ar.userGroup)
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
    ON apg.assessmentKey = ar.assessmentKey
    AND apg.resultKey = ar.resultKey
INNER JOIN NACVP_AssessmentProfile ap
    ON ap.profileGroupKey = apg.profileGroupKey
    AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
    ON arg.profileKey = ap.profileKey
    AND arg.resultKey = ap.resultKey AND arg.type = 'installed'
INNER JOIN NACVP_Application a
    ON a.applicationKey = arg.applicationKey
LEFT OUTER JOIN NACVP_AssessmentRuleGroup arg2
    ON arg2.profileKey = ap.profileKey
    AND arg2.resultKey = ap.resultKey AND arg2.type = 'version'
LEFT OUTER JOIN NACVP_AssessmentRule aru
    ON aru.ruleGroupKey = arg2.ruleGroupKey
    AND aru.resultKey = arg2.resultKey
WHERE ap.installed = 1
GROUP BY a.type, a.name, aru.outputValue, ar.userGroup

-- This is for Apps
INSERT into #summary
```

```
SELECT 'OS', 0, o.name, 0, NULL, 0,
      ar.userGroup, COUNT(ar.userGroup)
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
  AND apg.resultKey = ar.resultKey
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey AND arg.type = 'installed'
INNER JOIN NACVP_OS o ON o.osKey = arg.osKey
WHERE ap.installed = 1
GROUP BY o.name, ar.userGroup

-- This is for Service Packs
INSERT into #summary
SELECT 'Service Pack', 0, sp.name, 0, NULL, 0,
      ar.userGroup, COUNT(ar.userGroup)
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
  AND apg.resultKey = ar.resultKey
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey AND arg.type = 'servicePack'
INNER JOIN NACVP_AssessmentRule aru
  ON aru.ruleGroupKey = arg.ruleGroupKey
  AND aru.resultKey = arg.resultKey
INNER JOIN NACVP_ServicePack sp
  ON sp.servicePackKey = aru.servicePackKey
WHERE aru.conditionResult = 1
GROUP BY sp.name, ar.userGroup

-- This is for patches
INSERT into #summary
SELECT 'Patch', 0, p.name, 0, NULL, 0,
      ar.userGroup, COUNT(ar.userGroup)
FROM #lastAssessment ar
INNER JOIN NACVP_AssessmentProfileGroup apg
  ON apg.assessmentKey = ar.assessmentKey
  AND apg.resultKey = ar.resultKey
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey
INNER JOIN NACVP_AssessmentRule aru
  ON aru.ruleGroupKey = arg.ruleGroupKey
  AND aru.resultKey = arg.resultKey
```

```
INNER JOIN NACVP_PatchResult pr
  ON pr.ruleKey = aru.ruleKey AND pr.resultKey = aru.resultKey
INNER JOIN NACVP_Patch p ON p.patchKey = pr.patchKey
WHERE pr.conditionResult = 1
GROUP BY p.name, ar.userGroup

UPDATE #summary
SET appTypeCount = (
  SELECT SUM(s.groupNameCount)
  FROM #summary s
  WHERE #summary.appType = s.appType
  GROUP BY s.appType
)

UPDATE #summary
SET appNameCount = (
  SELECT SUM(s.groupNameCount)
  FROM #summary s
  WHERE #summary.appType = s.appType
  AND #summary.appName = s.appName
  GROUP BY s.appType, s.appName
)

UPDATE #summary
SET appVerCount = (
  SELECT SUM(s.groupNameCount)
  FROM #summary s
  WHERE #summary.appType = s.appType
  AND #summary.appName = s.appName
  AND #summary.appVer = s.appVer
  GROUP BY s.appType, s.appName, s.appVer
)

SELECT * FROM #summary
ORDER BY appType, appName, appVer, groupName

DROP TABLE #summary
DROP TABLE #lastAssessment
```

## 4.6 Exemple RADIUS Enforcer

Le rapport RADIUS Enforcer du Compliance Manager est semblable à cet exemple.

```
SELECT re.accessDateTime, re.username, re.userGroup,
  re.complianceState, re.reason, re.exemptionReason,
  re.templateName, re.nasIPAddress, re.clientIdentifier,
  re.exemptionCondition, re.assessmentKey, re.clientAction
FROM EFVP_RADIUSEnforcer re
ORDER BY accessDateTime DESC
```

## 4.7 Exemple de changement de conformité

Le rapport Compliance Change du Compliance Manager est semblable à cet exemple.

```

SELECT s.username, s.agentID, ar.endDateTime,
       ar.complianceState, p.name, p.versionNbr, ar.userGroup,
       ar.assessmentKey
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
INNER JOIN NACVP_AssessmentSequence asq
         ON asq.assessmentKey = ar.assessmentKey
WHERE NOT EXISTS (
         SELECT ar2.assessmentKey
         FROM NACVP_AssessmentReport ar2
         WHERE ar2.assessmentKey = asq.prevAssessmentKey
        )
UNION
SELECT s.username, s.agentID, ar.endDateTime,
       ar.complianceState, p.name, p.versionNbr, ar.userGroup,
       ar.assessmentKey
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
INNER JOIN NACVP_AssessmentSequence asq
         ON asq.assessmentKey = ar.assessmentKey
INNER JOIN NACVP_AssessmentReport ar2
         ON ar2.assessmentKey = asq.prevAssessmentKey
INNER JOIN NACVP_Policy p2 ON p2.policyKey = ar2.policyKey
AND (ar2.complianceState <> ar.complianceState
     OR p2.name <> p.name
     OR p2.versionNbr <> p.versionNbr
     OR ar2.userGroup <> ar.userGroup)
ORDER BY s.username, s.agentid, ar.endDateTime DESC,
         ar.complianceState, p.name, p.versionNbr

```

## 4.8 Exemple de détail de conformité

Le rapport Compliance Detail du Compliance Manager est semblable à cet exemple.

```

SELECT ar.complianceState, p.name, p.versionNbr,
       ar.userGroup, s.username, s.agentID, ar.endDateTime,
       ar.assessmentKey
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
WHERE NOT EXISTS (
         SELECT asq.prevAssessmentKey
         FROM NACVP_AssessmentSequence asq
         WHERE asq.prevAssessmentKey = ar.assessmentKey
        )

```

```
)
ORDER BY ar.complianceState, p.name, p.versionNbr
```

## 4.9 Exemple de récapitulatif de conformité

Le rapport Compliance Summary du Compliance Manager est semblable à cet exemple.

```
CREATE TABLE #summary
(
    complianceState nvarchar(20),
    complianceStateCount int,
    policyName nvarchar(128),
    policyNameCount int,
    policyVersionNbr int,
    policyVersionNbrCount int,
    userGroup nvarchar(128),
    userGroupCount int
)

INSERT INTO #summary
SELECT ar.complianceState, 0, p.name, 0,
       p.versionNbr, 0, ar.userGroup, COUNT(ar.userGroup)
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
WHERE ar.startDateTime = (SELECT MAX(ar2.startDateTime)
                          FROM NACVP_AssessmentReport ar2
                          INNER JOIN NACVP_Session s2
                          ON s2.sessionKey = ar2.sessionKey
                          WHERE s2.username = s.username
                          AND s2.agentID = s.agentID
                          GROUP BY s2.username, s2.agentID)
GROUP BY ar.complianceState, p.name, p.versionNbr, ar.userGroup

UPDATE #summary
SET complianceStateCount = (
    SELECT COUNT(s.complianceState)
    FROM #summary s
    WHERE #summary.complianceState = s.complianceState
    GROUP BY s.complianceState
)

UPDATE #summary
SET policyNameCount = (
    SELECT COUNT(s.policyName)
    FROM #summary s
    WHERE #summary.complianceState = s.complianceState
    AND #summary.policyName = s.policyName
    GROUP BY s.complianceState, s.policyName
)

UPDATE #summary
SET policyVersionNbrCount = (
```

```
SELECT COUNT(s.policyVersionNbr)
FROM #summary s
WHERE #summary.complianceState = s.complianceState
AND #summary.policyName = s.policyName
AND #summary.policyVersionNbr = s.policyVersionNbr
GROUP BY s.complianceState, s.policyName, s.policyVersionNbr
)

SELECT * FROM #summary
ORDER BY complianceState, policyName, policyVersionNbr DESC,
userGroup

DROP TABLE #summary
```

## 4.10 Exemple DHCP Enforcer

Le rapport DHCP Enforcer du Compliance Manager est semblable à cet exemple.

```
SELECT de.accessDateTime, de.macAddress, de.hostname,
de.complianceState, de.reason, de.exemptionReason,
de.templateName, de.clientAction, de.username,
de.agentID, de.returnedUserClass, de.sourceUserClass,
de.vendorClass, de.nasIPAddress, de.selectionIPAddress,
de.exemptionCondition, de.transactionID, de.assessmentKey
FROM NACVP_DHCPEnforcer de
ORDER BY accessDateTime DESC
```

## 4.11 Exemple de détail de stratégie

Le rapport Policy Detail du Compliance Manager est semblable à cet exemple.

```
SELECT p.name, p.versionNbr, ar.userGroup, s.username,
s.agentID, ar.endDateTime, ar.lastFetchDateTime
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
WHERE ar.startDateTime = (SELECT MAX(ar2.startDateTime)
FROM NACVP_AssessmentReport ar2
INNER JOIN NACVP_Session s2
ON s2.sessionKey = ar2.sessionKey
WHERE s2.username = s.username
AND s2.agentID = s.agentID
GROUP BY s2.username, s2.agentID)
ORDER BY p.name, p.versionNbr, ar.userGroup, s.username,
s.agentID, ar.endDateTime
```

## 4.12 Exemple de récapitulatif de stratégie

Le rapport Policy Summary du Compliance Manager est semblable à cet exemple.

```

CREATE TABLE #summary
(
    policyName nvarchar(128),
    policyNameCount int,
    policyVersion int,
    policyVersionCount int,
    groupName nvarchar(128),
    groupNameCount int
)

INSERT INTO #summary
SELECT p.name, 0, p.versionNbr, 0, ar.userGroup,
    COUNT(ar.userGroup)
FROM NACVP_AssessmentReport ar
INNER JOIN NACVP_Session s ON s.sessionKey = ar.sessionKey
INNER JOIN NACVP_Policy p ON p.policyKey = ar.policyKey
WHERE ar.startDateTime = (SELECT MAX(ar2.startDateTime)
    FROM NACVP_AssessmentReport ar2
    INNER JOIN NACVP_Session s2
    ON s2.sessionKey = ar2.sessionKey
    WHERE s2.username = s.username
    AND s2.agentID = s.agentID
    GROUP BY s2.username, s2.agentID)
GROUP BY p.name, p.versionNbr, ar.userGroup

UPDATE #summary
SET policyNameCount = (
    SELECT SUM(s.groupNameCount)
    FROM #summary s
    WHERE #summary.policyName = s.policyName
    GROUP BY s.policyName
)

UPDATE #summary
SET policyVersionCount = (
    SELECT SUM(s.groupNameCount)
    FROM #summary s
    WHERE #summary.policyName = s.policyName
    AND #summary.policyVersion = s.policyVersion
    GROUP BY s.policyName, s.policyVersion
)

SELECT * FROM #summary
ORDER BY policyName, policyVersion, groupName

DROP TABLE #summary

```

## 4.13 Exemple Agent Enforcer

Le rapport Agent Enforcer du Compliance Manager est semblable à cet exemple.

```
SELECT qa.statusChangeDateTime, qa.username,
       qa.agentID, qa.hostname, qa.complianceState, qa.templateName,
       qa.reason, qa.sessionKey
FROM NACVP_AgentEnforcer qa
ORDER BY statusChangeDateTime DESC
```

## 4.14 Exemple de session

La page Assessment Details du Compliance Manager est semblable à cet exemple.

```
SELECT ar.startDateTime, ar.endDateTime
FROM NACVP_AssessmentReport ar
WHERE ar.assessmentKey = 3

SELECT apg.profileGroupKey, apg.type, apg.complianceState
FROM NACVP_AssessmentProfileGroup apg
WHERE apg.assessmentKey = 3
ORDER BY apg.complianceState, apg.type

SELECT apg.profileGroupKey, ap.profileKey, ap.name, ap.selected,
       ap.reason, ap.installed, ap.complianceState
FROM NACVP_AssessmentProfileGroup apg
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
WHERE apg.assessmentKey = 3
ORDER BY apg.complianceState, apg.type, ap.complianceState,
       ap.priority, ap.name

SELECT apg.profileGroupKey, ap.profileKey, arg.ruleGroupKey,
       arg.type, arg.complianceState
FROM NACVP_AssessmentProfileGroup apg
INNER JOIN NACVP_AssessmentProfile ap
  ON ap.profileGroupKey = apg.profileGroupKey
  AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
  ON arg.profileKey = ap.profileKey
  AND arg.resultKey = ap.resultKey
WHERE apg.assessmentKey = 3
ORDER BY apg.complianceState, apg.type, ap.complianceState,
       ap.priority, ap.name, arg.type

SELECT apg.profileGroupKey, ap.profileKey, arg.ruleGroupKey,
       CASE
         WHEN ar.type = 'default' THEN 'Else'
         WHEN ar.servicePackKey = 0 THEN arg.type
```

```
        ELSE sp.name
    END AS conditionName, ar.outputValue, ar.policyOperator,
    ar.policyValue, ar.conditionResult, ar.complianceState,
    aa.type, aa.paramValue
FROM NACVP_AssessmentProfileGroup apg
INNER JOIN NACVP_AssessmentProfile ap
    ON ap.profileGroupKey = apg.profileGroupKey
    AND ap.resultKey = apg.resultKey
INNER JOIN NACVP_AssessmentRuleGroup arg
    ON arg.profileKey = ap.profileKey
    AND arg.resultKey = ap.resultKey
INNER JOIN NACVP_AssessmentRule ar
    ON ar.ruleGroupKey = arg.ruleGroupKey
    AND ar.resultKey = arg.resultKey
LEFT OUTER JOIN NACVP_AssessmentAction aa
    ON aa.ruleKey = ar.ruleKey
    AND aa.resultKey = ar.resultKey
LEFT OUTER JOIN NACVP_ServicePack sp
    ON sp.servicePackKey = ar.servicePackKey
WHERE apg.assessmentKey = 3
ORDER BY apg.complianceState, apg.type, ap.complianceState,
    ap.priority, ap.name, arg.type, ar.priority
```

## 5 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à [support@sophos.fr](mailto:support@sophos.fr), y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

## **6 Mentions légales**

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.