

Sophos NAC Advanced Anleitung zur Fehlersuche

Produktversion: 3.2
Stand: April 2011



Inhalt

1	Installationsprobleme.....	3
2	Probleme mit Compliance Manager.....	4
3	Protokollierungsprobleme.....	7
4	Datenübertragungsprobleme von Agent zu Server.....	8
5	Probleme mit dem VPN-Client.....	11
6	Richtlinienprobleme.....	12
7	Registrierungsprobleme.....	18
8	Report-Probleme.....	20
9	Probleme mit Alerts.....	23
10	Serverprobleme.....	24
11	Enforcer-Probleme.....	26
12	Probleme mit Anwendungen anderer Hersteller.....	34
13	Technischer Support.....	35
14	Rechtlicher Hinweis.....	36

1 Installationsprobleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Installationsproblemen mit Sophos NAC Advanced.

1.1 Installation der Compliance-Datenbanken

Die Installation der Compliance Datenbanken wird abgebrochen

Ursache: Sie sind nicht als Administrator an den Compliance Datenbanken angemeldet.

Lösung: Melden Sie sich als Administrator an.

Ursache: Bei der Installation wird ein Fenster mit der folgenden Meldung angezeigt: „Failed to load the test rule file“ mit einem XML-Dateinamen und der Meldung „Cursor operation conflict“. Diese Meldung wird angezeigt, weil das Attribut „No count“ für Verbindungen auf dem SQL-Server aktiviert ist.

Lösung:

1. Rufen Sie den Open Microsoft SQL Server Enterprise Manager auf und suchen Sie nach dem SQL-Server, auf dem die Installation fehlgeschlagen ist.
2. Rechtsklicken Sie auf den SQL-Server und wählen Sie **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Verbindungen**.
4. Suchen Sie in der Liste **Attribute** nach dem Attribut „No count“ und deaktivieren Sie das Kontrollkästchen.
5. Klicken Sie auf **OK**.

1.2 Installation des Agenten

Der Agent lässt sich nicht installieren

Ursache: Sie sind auf dem jeweiligen Endpoint nicht als Administrator angemeldet.

Lösung: Melden Sie sich auf dem jeweiligen Endpoint (also lokal) als Administrator an.

2 Probleme mit Compliance Manager

Dieser Abschnitt beschreibt die Fehlerbehebung bei Problemen mit Compliance Manager.

2.1 Verbindung oder Installation

Keine Verbindung zu Compliance Manager möglich.

Ursache: Administrator kann sich nicht an Compliance Manager anmelden.

Lösung:

1. Stellen Sie sicher, dass der Compliance Anwendungsserver erreichbar ist.
2. Wenn die Konten über Compliance Manager und einen externen Benutzerspeicher verwaltet werden, müssen Kontoname und Kennwort gültig sein.

Hinweis: Geben Sie **admin** und ein Kennwort Ihrer Wahl bei Ihrer ersten Anmeldung an Compliance Manager ein.

3. Wenn die Konten über einen externen Benutzerspeicher verwaltet werden, muss der für das Compliance Manager-Konto verwendete Benutzerspeicher mit dem für die Agentenauthentifizierung verwendeten Benutzerspeicher übereinstimmen. Ist dies nicht der Fall, müssen Sie zunächst eine Verbindungsanforderungsrichtlinie (Connection Request Policy) einrichten und ihr höchste Priorität zuordnen. Weitere Informationen finden Sie in der *Sophos NAC Advanced Installationsanleitung*.
4. In den Compliance Datenbanken sind die Berechtigungen für die Sophos Anwendungen möglicherweise nicht richtig eingerichtet. Nähere Informationen finden Sie unter „Die Compliance Anwendungsserver- oder RADIUS-Serverkomponenten können keine Verbindung zu den Compliance Datenbanken“ herstellen in folgendem Abschnitt: [SQL-Server](#) (Seite 25).

Ursache: Der ASP.NET-Dienst ist nicht aktiv.

Lösung: Setzen Sie den ASP.NET-Dienst auf „automatisch“ und starten Sie ihn.

2.2 Compliance Manager

In Compliance Manager werden bestimmte Fenster nicht angezeigt.

Ursache: Wenn der Popup-Blocker aktiviert ist, können einige Tasks in Compliance Manager nicht ausgeführt werden, z.B. das Drucken von Reports und das Abrufen der Online-Hilfe.

Lösung: Deaktivieren Sie den Popup-Blocker, wenn Sie mit Compliance Manager arbeiten.

Die Seiten werden in Compliance Manager nicht ordnungsgemäß angezeigt.

Ursache: In Internet Explorer 6.x wurde die Compliance Manager-Website nicht als „vertrauenswürdige Site“ eingerichtet.

Lösung: Fügen Sie Compliance Manager in Internet Explorer zu den vertrauenswürdigen Sites hinzu. Dieser Schritt trifft nicht für Internet Explorer 7.x zu.

In Compliance Manager lassen sich keine Funktionen erstellen, ändern oder konfigurieren.

Ursache: Die Compliance Datenbanken sind nicht verfügbar.

Lösung:

1. Sorgen Sie dafür, dass die Compliance Datenbanken einwandfrei funktionieren.
2. Der SQL-Serverdienst muss ordnungsgemäß gestartet worden sein. Außerdem muss das Kennwort für den Sophos NAC Advanced-Dienst, der diese SQL-Serverinstanz startet, mit dem Kennwort übereinstimmen, das vor der Installation von Sophos NAC Advanced erstellt wurde.

Ursache: Die Installation des Compliance Anwendungsservers wurde nicht erfolgreich abgeschlossen.

Lösung: Suchen Sie im Ereignisprotokoll von Compliance Anwendungsserver nach Installationsfehlern und beenden Sie die Installation des Compliance Anwendungsservers.

Es sind keine Patches erhältlich.

Ursache: Wenn in der Patchliste in Compliance Manager keine Patches aufgeführt sind, kann der Patch Loader keine Patches laden.

Lösung: Überprüfen Sie auf der Startseite von Compliance Manager im Bereich „Server Task Status“, ob der Patch Loader-Task abgebrochen wurde und aus welchem Grund dies passiert ist. Es ist sehr wahrscheinlich, dass entweder der Compliance Anwendungsserver über keinen ausgehenden Internetzugang verfügt (eine Voraussetzung für Patch Loader) oder dass der Proxyserver nicht bzw. nicht richtig konfiguriert wurde. Starten Sie den Task „Patch Loader“ auf dem Compliance Anwendungsserver manuell, damit die Patchdaten heruntergeladen und aktualisiert werden können. Konfigurieren Sie Ihren Proxyserver. Weitere Informationen finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

Das Datum der Signaturdateien für Viren-/Spywareschutz-Anwendungen scheint veraltet zu sein.

Ursache: Die neueste Signaturdatei wurde nicht vom Current Definition Loader-Task abgerufen.

Lösung: Überprüfen Sie auf der Startseite von Compliance Manager im Bereich „Server Task Status“, ob der Current Definition Loader abgebrochen wurde und aus welchem Grund dies passiert ist. Es ist sehr wahrscheinlich, dass entweder der Compliance Anwendungsserver über keinen ausgehenden Internetzugang verfügt (eine Voraussetzung für Current Definition Loader) oder dass der Proxyserver nicht bzw. nicht richtig konfiguriert wurde. Starten Sie den Task „Current Definition Loader“ auf dem Compliance Anwendungsserver manuell, damit die Signaturdaten heruntergeladen und aktualisiert werden können. Konfigurieren Sie Sophos NAC Advanced als RADIUS-Proxyserver. Weitere Informationen finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

Anwendungsnamen werden in Sophos NAC Advanced nicht richtig angezeigt.

Ursache: Die Unterstützung für ostasiatische Sprachen wurde nicht installiert.

Lösung: Überprüfen Sie auf dem Computer, auf dem Sie Compliance Manager aufrufen, ob die zur Unterstützung ostasiatischer Sprachen erforderlichen Dateien installiert wurden (über Systemsteuerung > Regions- und Sprachoptionen).

Das Klicken auf die Browser-Schaltflächen verursacht einen Fehler.

Ursache: Sie bedienen die Software über die Schaltflächen des Webbrowsers.

Lösung: Compliance Manager bietet keine Webbrowser-Schaltflächen. Bedienen Sie das Programm über die jeweils vorhandenen Menübefehle, Links und Schaltflächen.

Es werden nicht alle Anwendungsfähigkeiten oder Korrekturmaßnahmen einer Anwendung angezeigt.

Ursache: Fähigkeiten oder Korrekturmaßnahmen werden von dieser Anwendungsversion auf allen Betriebssystemen nicht unterstützt.

Lösung: Die verfügbaren Anwendungsfähigkeiten und Korrekturmaßnahmen hängen vom Softwaredesign der Anwendung ab. Einige Fähigkeiten und Korrekturmaßnahmen stehen für bestimmte Betriebssysteme, auf denen die Anwendung unterstützt wird, oder für alle Versionen einer Anwendung nicht zur Verfügung. Nicht verfügbare Fähigkeiten werden nicht angezeigt. Wenn eine Fähigkeit nur auf bestimmten Betriebssystemen verfügbar ist, werden nur diese Betriebssysteme angezeigt. Wenn eine Korrekturmaßnahme nur auf bestimmten Betriebssystemen unterstützt wird, werden die Betriebssysteme, auf denen die Maßnahme nicht zur Verfügung steht, mit einem x angezeigt.

Es empfiehlt sich, die Richtlinien vor der Installation zu testen, um sicherzustellen, dass Sie über die richtige Anwendung, die richtigen Anwendungserkennungsregeln, Profileinstellungen und Richtlinienereinstellungen verfügen.

Es werden nicht alle Fähigkeiten eines Profils angezeigt.

Ursache: Es passen nicht alle Fähigkeiten auf die Seite von Compliance Manager.

Lösung: Reduzieren Sie die Struktur neben der Überschrift, um die Fähigkeiten auf der Webseite anzuzeigen.

3 Protokollierungsprobleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Problemen mit der Protokollierung.

3.1 Agentenprotokoll

Für den Quarantine Agent sind keine Protokolldateien vorhanden

Ursache: Die Protokollierung ist nicht aktiviert.

Lösung: Aktivieren Sie die Protokollierung für den Agenten über das Kontrollkästchen **Protokollierung aktivieren** in der Versionsinfo. Wenn nicht in der Agent Configuration Template der Richtlinie des Endpoints angegeben, wird die Protokollierung automatisch auf Stufe 1 (Fehler- und Warnmeldungen) gesetzt.

Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Protokolldateien für Windows 2000 und Windows XP befinden sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Sophos NAC\Logs. Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdaten\Sophos\Sophos NAC\Logs.

3.2 Dissolvable Agent-Protokoll

Für den Dissolvable Agent sind keine Protokolldateien vorhanden

Ursache: Die Protokollierung ist nicht aktiviert.

Lösung: Aktivieren Sie die Protokollierung für den Dissolvable Agent. Aktivieren Sie die Protokollierung für den Agenten über das Kontrollkästchen **Protokollierung aktivieren** in der Versionsinfo. Weitere Informationen finden Sie in der *Sophos NAC Advanced Agent Konfigurationsanleitung*.

Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Die Protokolldateien befinden sich im Verzeichnis <Laufwerk>:\Sophos\SDA<Zufallszahl>\Logs:

4 Datenübertragungsprobleme von Agent zu Server

Dieser Abschnitt beschreibt die Fehlerbehebung bei Problemen mit der Datenübertragung von Agent zu Server.

4.1 Richtlinienabruf, Registrierung, Reporting

Das Abrufen von Richtlinien, die Registrierung und/oder das Reporting funktioniert nicht.

Wichtig: Weitere Probleme mit Richtlinien, Registrierung oder Reporting finden Sie unter [Richtlinienprobleme](#) (Seite 12), [Registrierungsprobleme](#) (Seite 18) oder [Report-Probleme](#) (Seite 20).

Ursache: Bei der Installation des Agenten war die Adresse des Compliance Anwendungsservers falsch oder die Serveradresse wurde nach der Installation des Agenten geändert. Die Serveradresse zur Verbindung mit dem Compliance Anwendungsserver wird im Fehlerprotokoll aufgeführt.

Sollte die IP-Adresse oder der DNS-Name **nicht** korrekt oder der Compliance Anwendungsserver nicht verfügbar sein, wird folgender Fehler im Ergebnisfenster angezeigt: „Der Agent war nicht in der Lage <> abzurufen. Sollte dieses Problem fortbestehen, wenden Sie sich an Ihren Administrator, um das Problem zu melden. (Grund: Server nicht gefunden. Code: 700)“.

Wenn die IP-Adresse bzw. der DNS-Name korrekt ist, aber **nicht** der URL-Pfad, wird folgender Fehler im Ergebnisfenster angezeigt: „Der Agent war nicht in der Lage <> abzurufen. Sollte dieses Problem fortbestehen, wenden Sie sich an Ihren Administrator, um das Problem zu melden. (Grund: URL ist ungültig. Code: 404)“.

Lösung:

1. Vergewissern Sie sich über eine vom Benutzer eingeleitete Konformitätsprüfung, dass der Compliance Anwendungsserver tatsächlich nicht ansprechbar ist. Rechtsklicken Sie dazu auf das Symbol des Quarantine Agent im Statusbereich der Taskleiste und wählen Sie die Option „Konformität überprüfen“.
2. Wählen Sie im Dialogfeld „Über...“ das Kontrollkästchen „Protokollierung aktivieren“, um die Protokollierung des Agenten zu aktivieren. Überprüfen Sie anschließend die Serveradresse (IP-Adresse oder DNS-Name) und den Servermodus (http/https) des Compliance Anwendungsservers. Öffnen Sie hierzu die Agent API-Protokolldatei <GUID>_trace.log. Für Compliance Agent wird diese Protokolldatei angezeigt, wenn die Einstellung „Logging Agent“ der Agent Configuration Template auf **Log All Messages and Brief Trace** gesetzt ist. Für den Dissolvable Agent wird diese Einstellung angegeben, wenn die Protokollierung aktiviert ist. Beim Compliance Agent befinden sich Protokolldateien für Windows 2000 und Windows XP im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Sophos NAC\Logs. Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdateien\Sophos\Sophos NAC\Logs. Bei Dissolvable Agent befinden sich die Protokolldateien im Verzeichnis <Laufwerk>:\Sophos\SDA<Zufallszahl>\Logs:
3. Installieren Sie den Agenten unter Angabe der korrekten Adresse des Compliance Anwendungsservers neu. Bei der Installation darf die Serveradresse (< Compliance

Anwendungsserver> mit den Webdiensten „Registration Interface“, „Policy Interface“ und „Reporting Interface“) nur als DNS-Name (z.B. „www.sophos.de“) oder als IP-Adresse (z.B. „10.0.0.160“) angegeben werden.

Wichtig: Wenn das Web-Zertifikat des Compliance Anwendungsservers eine IP-Adresse erfordert, muss bei der Installation des Agenten eine IP-Adresse angegeben werden. Wenn das Web-Zertifikat einen DNS-Namen erfordert, muss bei der Installation des Agenten der DNS-Name angegeben werden.

Ursache: Die Agentenregistrierung wurde gelöscht. Im Ergebnisfenster wird folgender Fehler angezeigt: „Der Agent war nicht in der Lage <> abzurufen. Sollte dieses Problem fortbestehen, wenden Sie sich an Ihren Administrator, um das Problem zu melden. (Grund: Der Server hat die Anforderung abgelehnt. Code: 500)“.

Lösung: Registrieren Sie den Agenten neu. Rechtsklicken Sie auf dem Endpoint auf das Agenten-Symbol im Statusbereich der Taskleiste und wählen Sie **Registrierung**.

Ursache: Der Endpoint verfügt nicht über Internetzugriff.

Lösung: Der Endpoint muss über Internetzugang verfügen.

Ursache: Auf dem Agenten oder auf Compliance Anwendungsserver ist kein SSL-Zertifikat installiert.

Lösung:

1. Das digitale Zertifikat der Zertifizierungsstelle muss im Speicher der vertrauenswürdigen Zertifizierungsstelle auf dem lokalen Rechner (nicht dem des Benutzers) installiert sein. Dies ist für https erforderlich.

Hinweis: Zur ordnungsgemäßen Validierung von Zertifikaten auf Endpoints, die unter älteren Windows -Systemen betrieben werden (darunter auch Windows 2000), installieren Sie das entsprechende „Stammzertifikat-Update“ von der Microsoft-Website.

2. Stellen Sie sicher, dass auf dem Compliance Anwendungsserver ein digitales Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (wie VeriSign) installiert ist. Dies ist für https erforderlich.

Hinweis: Wenn Sie die Tests über HTTP durchführen, verwenden die URLs ebenfalls HTTP.

Ursache: Der Compliance Anwendungsserver ist nicht ansprechbar.

Lösung:

1. Die Firewall-Software auf dem Endpoint darf keinen Datenverkehr zum Compliance Anwendungsserver blockieren. Stellen Sie sicher, dass der Datenverkehr zum Endpoint nicht durch eine Firewall blockiert wird. Wenn Datenverkehr durch eine Firewall gesperrt wird, rufen Sie die Firewall auf und lassen Sie den Datenfluss zu.
2. Stellen Sie sicher, dass die Adresse des Compliance Anwendungsservers korrekt ist, indem Sie die Compliance Anwendungsserver-URL in einem Internetbrowser testen. Wenn ein Fehler mit den Webdiensten angezeigt wird, ist die Serveradresse korrekt. Sie können eine der folgenden URLs testen:

[http\(s\)://< Compliance Anwendungsserver>/RegistrationInterface/RegistrationInterface310.asmx](http(s)://< Compliance Anwendungsserver>/RegistrationInterface/RegistrationInterface310.asmx)

[http\(s\)://< Compliance Anwendungsserver>/ServerStatusInterface/ServerStatusInterface310.aspx](http(s)://< Compliance Anwendungsserver>/ServerStatusInterface/ServerStatusInterface310.aspx)

3. Stellen Sie sicher, dass der Compliance Anwendungsserver den entsprechenden Access Templates von Compliance Manager als erlaubte Netzwerkressource zugewiesen wurde.
4. Sollte sich der Endpoint außerhalb des Netzwerks befinden, muss sich dieser am VPN anmelden und über den Agent eine vom Benutzer eingeleitete Konformitätsprüfung des Endpoints durchführen.

Ursache: Der Agent stellt die Verbindung zum Compliance Anwendungsserver über einen Web-Proxyserver mit den falschen Einstellungen her.

Lösung: Öffnen Sie die Web-Proxyeinstellungen im Internet Explorer und sorgen Sie dafür, dass sie korrekt sind:

1. Klicken Sie auf **Extras > Internetoptionen**.
2. Klicken Sie auf die Registerkarte **Verbindungen**.
3. Klicken Sie auf **Einstellungen und/oder LAN-Einstellungen** und geben Sie die entsprechenden Proxyeinstellungen ein.

Stellen Sie sicher, dass die Adresse des Compliance Anwendungsservers korrekt ist, indem Sie die Compliance Anwendungsserver-URL in einem Internetbrowser testen. Wenn ein Fehler mit den Webdiensten angezeigt wird, ist die Serveradresse korrekt. Sie können eine der folgenden URLs testen:

[http\(s\)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.aspx](http(s)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.aspx)

[http\(s\)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.aspx](http(s)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.aspx)

Ursache: Der Agent stellt die Verbindung zum Compliance Anwendungsserver über einen Web-Proxyserver her, dessen Einstellungen jedoch nicht für den aktuellen Benutzer zutreffen.

Lösung: Die Web-Proxyeinstellungen im Internet Explorer müssen für den aktuellen Benutzer eingestellt sein, da die Einstellungen für jeden Benutzer getrennt konfiguriert werden. Weitere Informationen sind unter dem vorigen Problem aufgeführt.

Ursache: Ein DNS-Eintrag wurde geändert und der Endpoint wurde nicht neu gestartet oder der Prozess „AgentAPI.exe“ wurde nicht gestoppt und wieder gestartet.

Lösung: Starten Sie jeden Endpoint neu oder verlassen Sie den Agenten und stoppen und starten Sie den Prozess „AgentAPI.exe“ auf jedem Endpoint neu. Auf diese Weise werden die veralteten DNS-Einträge gelöscht.

Ursache: Die Serverschlüssel stimmen nicht überein. Im Ergebnisfenster wird folgender Fehler angezeigt: „Server-Überprüfung fehlgeschlagen. Code: 701“ (wenn ausführliche Fehlermeldungen aktiviert sind).

Lösung: Wenn in Compliance Manager ein neuer Serverschlüssel generiert wird, muss derselbe Schlüssel auf alle Compliance Anwendungsserver importiert werden, damit sie übereinstimmen.

Stellen Sie sicher, dass Sie die richtige XML-Datei „ServerKey.xml“ verwenden, und dass auf allen Compliance Anwendungsserver derselbe Serverschlüssel verwendet wird (falls mehrere Server eingesetzt werden).

5 Probleme mit dem VPN-Client

Dieser Abschnitt beschreibt die Fehlerbehebung bei Problemen mit dem VPN-Client.

5.1 VPN

Das VPN, oder eine andere Anwendung eines Fremdherstellers, ruft den Agenten nicht auf

Ursache: Der Quarantine Agent wird nicht vom VPN oder anderer Fremdsoftware gerufen.

Lösung: Anwendungen von Fremdherstellern müssen den Compliance Checker (Cmpchk.exe) aufrufen können, um eine vollständige Konformitätsprüfung über den Agenten einzuleiten . Weitere Informationen finden Sie in der *Sophos NAC Advanced Agent Konfigurationsanleitung* .

Ursache: Agent läuft nicht.

Lösung: Überprüfen Sie, ob der Agent bereits vor dem Aufruf durch die Anwendung eines Fremdherstellers ausgeführt wurde.

Keine Verbindung zum VPN

Ursache: Dem Agent Policy Update Threshold zufolge ist der letzte Richtlinienabruf des Endpoints veraltet.

Lösung: Der letzte Richtlinienabruf des Endpoints muss in dem im Feld „Agent Policy Update Threshold“ in Compliance Manager ((**Configure System** > **Enforcer Settings**)) angegebenen Zeitraum stattgefunden haben.

Ursache: Die beim Aufruf des Compliance Checkers (Cmpchk.exe) ausgegebenen Fehlercodes sind nicht korrekt.

Lösung: Stellen Sie sicher, dass die ausgegebenen Fehlercodes korrekt sind und ordnungsgemäß verarbeitet werden. Weitere Informationen finden Sie in der *Sophos NAC Advanced Agent Konfigurationsanleitung* .

VPN-Authentifizierung abgebrochen

Ursache: Der Benutzername für die RADIUS-Authentifizierung stimmt nicht mit dem Benutzernamen für die VPN-Authentifizierung überein.

Lösung: Stellen Sie sicher, dass die Zeichen des Benutzernamens genau mit den Zeichen des Agenten für die RADIUS-Authentifizierung und die VPN-Client-Anwendung übereinstimmen (es wird dabei nicht zwischen Groß- und Kleinschreibung unterschieden).

Ursache: Dem Endpoint wird eine RADIUS Enforcer Access Template zugewiesen, die irrtümlicherweise den Zugriff verweigert.

Lösung: Ermitteln Sie über den RADIUS Enforcer Report in Compliance Manager, welche Access Template aus welchem Grund dem Endpoint zugewiesen wird.

Die richtigen RADIUS Enforcer Access Templates müssen auf die entsprechenden Access und Compliance States in der Richtlinie und in den Enforcer-Einstellungen übertragen sein. Überprüfen Sie, ob die Access Templates über die richtigen Einstellungen und Netzwerkressourcen verfügen.

6 Richtlinienprobleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Richtlinienproblemen.

6.1 Abrufen von Richtlinien

Die Richtlinie konnte nicht abgerufen werden.

Wichtig: Weitere Informationen finden Sie unter [Datenübertragungsprobleme von Agent zu Server](#) (Seite 8).

Ursache: Die Registrierung des Benutzers am Agenten ist abgelaufen. Im Ergebnisfenster wird folgender Fehler angezeigt: „Das Abrufen der Richtlinie schlug aufgrund einer abgelaufenen Benutzerregistrierung fehl. Sie müssen den Agent neu registrieren.“

Lösung: Der Benutzer muss sich am Agenten über die Schaltfläche **Register** neu anmelden.

6.2 Prüfung und Durchsetzung von Richtlinien

Agent kann Richtlinie nicht prüfen/durchsetzen

Wichtig: Weitere Informationen finden Sie unter [Datenübertragungsprobleme von Agent zu Server](#) (Seite 8).

Ursache: Die Registrierung des Benutzers am Agenten ist abgelaufen. Im Ergebnisfenster wird folgender Fehler angezeigt: „Die Durchsetzung der Richtlinie schlug aufgrund einer abgelaufenen Benutzerregistrierung fehl. Sie müssen den Agent neu registrieren.“

Lösung: Der Benutzer muss sich am Agenten über die Schaltfläche **Register** neu anmelden.

Endpoint empfängt keine Richtlinien (bei Benutzerauthentifizierung)

Ursache: Es wurde keine Standardrichtlinie festgelegt, und der Benutzer ist Mitglied einer Gruppe, der keine Richtlinie in Compliance Manager zugewiesen wurde. Oder der Benutzer kann keiner Gruppe zugeordnet werden.

Lösung: Weisen Sie in Compliance Manager der Gruppe eine Richtlinie zu oder erstellen Sie eine Standardrichtlinie.

Ursache: Die Gruppe des Benutzers hat sich seit der letzten Agentenregistrierung des Benutzers und dem letzten Richtlinienabruf geändert.

Lösung: Lassen Sie die Benutzerregistrierung im Bereich **Manage > Endpoints** von Compliance Manager ablaufen, sodass der Agent den Benutzer neu registrieren und die richtige Richtlinie abrufen kann.

Ursache: Die Benutzergruppe wurde nicht in Compliance Manager erstellt.

Lösung: Erstellen Sie die Gruppe in Compliance Manager. Weitere Informationen finden Sie in der Compliance Manager zu Hilfe.

Ursache: Wenn Sie Quarantine Agent verwenden, wurde der Policy Refresh Interval noch nicht erreicht und deshalb hat der Agent die Richtlinie noch nicht abgerufen.

Lösung: Rufen Sie die Richtlinie über eine vom Benutzer eingeleitete Konformitätsprüfung über die Menüoption „Konformität überprüfen“ des Quarantine Agent-Symbols im Statusbereich der Taskleiste ab.

Endpoint empfängt die falsche Richtlinie

Ursache: Die Gruppe des Benutzers hat sich seit der letzten Agentenregistrierung des Benutzers und dem letzten Richtlinienabruf geändert.

Lösung: Lassen Sie die Benutzerregistrierung im Bereich **Manage > Endpoints** von Compliance Manager ablaufen, sodass der Agent den Benutzer neu registrieren und die richtige Richtlinie abrufen kann.

Ursache: Der Benutzer ist zwar Mitglied einer Gruppe, doch der Gruppe wurde in Compliance Manager nicht die korrekte Richtlinie zugewiesen.

Lösung: Der Gruppe muss in Compliance Manager die korrekte Richtlinie zugewiesen sein.

Ursache: Die Gruppen sind in Compliance Manager nicht richtig priorisiert.

Lösung: Stellen Sie sicher, dass den Gruppen in Compliance Manager jeweils die richtige Priorität zugeordnet wurde. Wenn einem Endpoint mehr als eine Gruppe zugeordnet wurde, wird die erste Gruppe gewählt. Wenn der Benutzer die Standardrichtlinie erhält, so müssen die Gruppennamen korrekt sein.

Ursache: Der Benutzer ist kein Mitglied der erwarteten Gruppe im Benutzerspeicher.

Lösung: Der Benutzer muss der richtigen Gruppe im Benutzerspeicher angehören. Überprüfen Sie außerdem die Richtigkeit des Gruppennamens. Zur fehlerfreien Authentifizierung des Gruppennamens muss dieser in Compliance Manager entweder mit dem Namen einer Sicherheitsgruppe im Benutzerspeicher (Active Directory oder Windows NT) oder mit einem vom RADIUS-Server (RADIUS-Proxy) ausgegebenen Wert übereinstimmen.

Ursache: Die Benutzergruppe wurde nicht in Compliance Manager erstellt.

Lösung: Erstellen Sie die Gruppe in Compliance Manager. Weitere Informationen finden Sie in der Compliance Manager zu Hilfe.

Ursache: Dem Endpoint wird statt der richtigen Richtlinie die Standardrichtlinie zugewiesen.

Lösung: Der Benutzer muss der korrekten Gruppe im Benutzerspeicher zugewiesen sein. Der Gruppename muss erstellt und akkurat im Compliance Manager sein. Der Gruppe muss in Compliance Manager die korrekte Richtlinie zugewiesen sein.

Wenn Sie die Registrierungseinstellung **Use Computer Logon** verwenden, muss die Anmeldung an Endpoints über Domänenzugangsdaten erfolgen; ansonsten wird ihnen die Standardrichtlinie überwiesen.

Überprüfung findet nicht über aktuelle Richtlinie statt

Wichtig: Weitere Informationen finden Sie unter [Datenübertragungsprobleme von Agent zu Server](#) (Seite 8).

Ursache: Wenn Sie Quarantine Agent verwenden, wurde das Policy Refresh Interval noch nicht erreicht und deshalb hat der Agent die aktualisierte Richtlinie noch nicht abgerufen.

Lösung: Rufen Sie die Richtlinie über eine vom Benutzer eingeleitete Konformitätsprüfung über die Menüoption „Konformität überprüfen“ des Quarantine Agent-Symbols im Statusbereich der Taskleiste ab.

Einstellungen oder Funktionen des Agenten wurden falsch auf den Endpoint übertragen.

Ursache: Dieses Problem kann neben dem Problem „Endpoint empfängt die falsche Richtlinie“ oder „Endpoint führt keine Überprüfung mit einer aktuellen Richtlinie durch“ als Begleiterscheinung auftreten.

Lösung: Überprüfen Sie anhand des Agent Session Reports, ob der Endpoint die richtige und aktuelle Richtlinie empfängt. Wenn dies nicht der Fall ist, befolgen Sie die Schritte zur Fehlerbehebung unter „Endpoint empfängt die falsche Richtlinie“ oder „Endpoint führt keine Überprüfung mit einer aktuellen Richtlinie durch“. Wenn der Agent die richtige und aktuelle Richtlinie empfängt, fahren Sie mit den anderen Schritten in diesem Abschnitt fort.

Ursache: Falsche Agent Configuration Template wurde der Richtlinie des Endpoints hinzugefügt oder die Einstellungen der Agent Configuration Template sind falsch.

Lösung: Prüfen Sie, ob die richtige Agent Configuration Template auf die Richtlinie des Endpoints übertragen wird und sie die richtigen Einstellungen enthält.

Ursache: Agent zeigt nicht das erwartete Gebietsschema der Maske an.

Lösung: Die Agentenmaske wird je nach dem Standard-Gebietsschema ungeachtet der Sprache des auf dem Endpoint installierten Betriebssystems dynamisch angezeigt.

Korrekturmaßnahmen lassen sich nicht für Windows-Update-Profil aktivieren.

Ursache: Gruppenrichtlinie ermöglicht keine Aktivierung von „Automatic Updates“.

Lösung: Wenn die Gruppenrichtlinie die Aktivierung von „Automatic Updates“ nicht zulässt, kann sie nicht mit der Compliance Richtlinie überschrieben werden. Sorgen Sie dafür, dass die Gruppenrichtlinie Ihren Ansprüchen entspricht und die Compliance Richtlinie mit der Gruppenrichtlinie synchron ist.

Anwendung wird auf dem Endpoint nicht erkannt oder Erkennung schlägt fehl

Ursache: Die erkannte Anwendung ist möglicherweise nicht korrekt.

Lösung: Überprüfen Sie, ob Sie den richtigen Anwendungsnamen in Verbindung mit dem Profil verwenden, das der Richtlinie zugewiesen wurde. Anwendungen werden in Compliance Manager unter dem Hauptproduktnamen aufgelistet. Unter Umständen wird die Anwendung unter einem anderen Namen vertrieben. Um den Hauptproduktnamen zu ermitteln, überprüfen Sie das installierte Produkt oder wenden Sie sich an den Hersteller.

Es empfiehlt sich, die Richtlinien vor der Installation zu testen, um sicherzustellen, dass Sie über die richtige Anwendung, die richtigen Anwendungserkennungsregeln, Profileinstellungen und Richtlinieneinstellungen verfügen.

Ursache: Die Erkennungsregeln der Installed-Fähigkeit für die individuelle Anwendung sind inkorrekt.

Lösung: Es empfiehlt sich, die Richtlinien vor der Installation auf eine Testgruppe zu übertragen, um sicherzustellen, dass Sie über die richtige Anwendung, die richtigen Anwendungserkennungsregeln, Profileinstellungen und Richtlinieneinstellungen verfügen.

Aktivieren Sie auf dem Agenten die Protokollierungsstufe „Brief Trace“. Aktivieren Sie das Kontrollkästchen „Protokollierung aktivieren“ im Fenster mit der Versionsinfo. Achten Sie darauf, dass in der Agent Configuration Template, die der Richtlinie des Endpoints zugewiesen wurde, die Protokollierung des Agenten auf Fehler- und Warnmeldungen, Informationen sowie die Erstellung kurzer Ablaufverfolgungsmeldungen eingestellt ist. Versuchen Sie, die Erkennungsprobleme anhand des API-Protokolls des Agenten (<GUID>_trace.log) zu beheben.

Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Protokolldateien für Windows 2000 und Windows XP befinden sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Sophos NAC\Log. Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdateien\Sophos\Sophos NAC\Log.

Ursache: Das Datum zur Registrierungserkennung einer Anwendung befindet sich nicht im richtigen Format.

Lösung: Wenn Sie bei der Registrierungserkennung ein Datum angeben, muss das Datumsformat mit dem des Endpoints übereinstimmen. Zur Auswahl stehen „English (U.S.)“ und „System Locale“. Letztere Option übernimmt das Datumsformat der jeweiligen Betriebssystemsprache. Zur Ermittlung des richtigen Formats empfiehlt es sich, zunächst die Anwendung auf den gewünschten internationalen Betriebssystemen zu installieren, die Herstelleranwendung zu starten und die verschiedenen Datumsformate zu beachten und zu notieren.

Ursache: Die in der Profild Fähigkeit oder Anwendungserkennungsregel definierte Versionsnummer enthält die falsche Anzahl von Kennwerten für die geplante Endpoint-Analyse.

Lösung: Die Version wird auf dem Endpoint anhand der in der Bedingung oder Erkennungsregel angegebenen Kennwerte analysiert. Wenn Sie also eine Versionsfähigkeit definieren oder eine Erkennungsregel mit einer Version erstellen, muss die Versionsnummer die richtige Anzahl von Kennwerten für die geplante Endpoint-Analyse enthalten.

Wenn Sie beispielsweise eine Bedingung mit == 8 anlegen und auf dem Endpoint Version 8.1 installiert wurde, vergleicht die Software Version 8.1 mit dem in der Bedingung festgelegten Kennwert (nämlich 8). Die Bedingung ist somit erfüllt. Wenn Sie jedoch eine Bedingung mit == 8.0 anlegen und die auf dem Endpoint installierte Version lautet 8.1, vergleicht die Software Version 8.1 mit den beiden Kennwerten (nämlich 8 und 0) in der Bedingung. In diesem Fall ist die Bedingung nicht erfüllt.

Ursache: Das in der Fähigkeit definierte Datumsformat stimmt nicht genau mit dem Format überein, das von der Konformitätsprüfung ausgegeben wird.

Lösung: Wenn Sie für eine Standardviren- oder Spywareschutzanwendung ein Profil definieren und eine Datumsfähigkeit („Last Scan Date“ und „Signature Date“) mit dem Operator == (gleich) angeben, muss das Datum vom Endpoint im Format MM/TT/JJJJ zurückgegeben werden. Wenn die Anwendung das Datum im Format MM/TT/JJJJ HH:MM:SS zurückgibt, kann die Erkennung fehlschlagen, auch wenn das Datum am Endpoint mit dem in der Bedingung angegebenen Wert identisch ist. Um dieses Problem zu vermeiden, können Sie den Operator >= (größer gleich) oder <= (kleiner gleich) anstelle von == bei der Definition von Daten verwenden, oder testen Sie eine Richtlinie, bevor Sie sie installieren, um sicherzustellen, dass die Erkennung durch den Operator == nicht fehlschlägt.

6.3 Meldungen und Korrekturmaßnahmen

Auf dem Endpoint werden keine Meldungen angezeigt und keine Korrekturmaßnahmen durchgeführt.

Ursache: Meldung wird für Benutzer nicht angezeigt.

Lösung:

1. Überprüfen Sie, ob sich die Richtlinie im Modus „Remediate“ bzw. „Enforce“ befindet. Im Modus „Report Only“ werden keine Meldungen angezeigt.
2. Überprüfen Sie, ob eine Meldung erstellt wird, ob sie mit der richtigen Profilbedingung verbunden ist und die Bedingung am Endpoint erfüllt wurde. Sehen Sie sich über Compliance Manager den Agent Session Report, den Assessment Details-Link für die Profildetails sowie die für Benutzer angezeigten Meldungen an.

Ursache: Meldung wird nur auf englischsprachigen Betriebssystemen angezeigt.

Lösung: Für alle Profile in der Richtlinie des Endpoints müssen zumindest Meldungen auf Englisch (die Standardsprache) eingerichtet sein. Daraufhin sollten die Meldungen auch in andere Sprachen übersetzt werden.

Ursache: Korrekturmaßnahme wird nicht am Endpoint ausgeführt.

Lösung:

1. Überprüfen Sie, ob sich die Richtlinie im Modus „Remediate“ bzw. „Enforce“ befindet. Im Modus „Report Only“ werden keine Korrekturmaßnahmen ausgeführt.
2. Überprüfen Sie, ob die Korrekturmaßnahme für die richtige Profilbedingung gewählt und die Bedingung am Endpoint erfüllt wurde. Sehen Sie sich über Compliance Manager den Agent Session Report, den Assessment Details-Link für die Profildetails sowie die Korrekturmaßnahmen an, die am Endpoint durchgeführt werden.
3. Bei einer Richtlinie, für die die Software eine Viren- oder Spywareschutz-Signaturdatei automatisch aktualisieren soll, muss überprüft werden, ob die entsprechende Access Template den Zugriff auf den Serverspeicherort der Signaturdatei zulässt, damit das Update implementiert werden kann.
4. Wenn Sie die Schritte 1 bis 3 geprüft haben und die Korrekturmaßnahme immer noch nicht ausgeführt wird, steht sie unter diesem Betriebssystem möglicherweise nicht zur Verfügung. Wenn eine Korrekturmaßnahme nur auf bestimmten Betriebssystemen unterstützt wird, werden die Betriebssysteme, auf denen die Maßnahme nicht zur Verfügung steht, mit einem x angezeigt. Sorgen Sie dafür, dass Benutzer die Anwendung auf andere Weise korrigieren können und dass eine Meldung für diese Anwendungsfähigkeit erstellt wird, die Benutzern Korrekturhinweise gibt.

6.4 Patches

Agent ruft nicht die neuesten Patches ab

Wichtig: Weitere Informationen finden Sie unter [Ereignisprotokoll](#) (Seite 25).

Ursache: Sophos NAC Advanced lädt nicht die neuesten Patches herunter.

Lösung: Überprüfen Sie auf der Startseite von Compliance Manager im Bereich „Server Task Status“, ob der Patch Loader abgebrochen wurde und aus welchem Grund dies passiert ist. Die wahrscheinlichste Fehlerursache liegt darin, dass der Compliance Anwendungsserver nicht auf das Internet zugreifen kann. Für CurrentDefsLoader ist Internetzugriff jedoch erforderlich. Starten Sie den Task „Patch Loader“ auf dem Compliance Application Server manuell, damit die Patchdaten heruntergeladen und aktualisiert werden können. Weitere Informationen finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

Ursache: Verwaltete Patches für ältere Agenten (3.0.x).

Lösung: Falls ein Compliance Anwendungsserver nicht über Internetzugang verfügt, stellen Sie sicher, dass die für die Patchererkennung verwendete CAB-Datei manuell auf dem Compliance Anwendungsserver gepostet wird. Weitere Informationen finden Sie unter „Patch Loader-Fehler werden im Ereignisprotokoll des Compliance Anwendungsservers angezeigt“. Weitere Informationen finden Sie unter [Ereignisprotokoll](#) (Seite 25).

Ursache: Der Benutzer verwendet den Dissolvable Agent, hat aber nur eingeschränkten Zugriff auf den Endpoint.

Lösung: Der Dissolvable Agent kann keine Patch-Analyse durchführen, wenn der Benutzer nicht über volle Zugriffsrechte verfügt. Geben Sie dem Benutzer Administratorrechte und starten Sie Dissolvable Agent erneut. Wenn dies nicht möglich ist, empfiehlt sich die Einrichtung einer separaten Richtlinie für Benutzer des Dissolvable Agent. Diese Benutzer verfügen meist über Gastzugang. Diese Richtlinie sollte keine Patches, jedoch das „Windows Update Profile“ enthalten. Durch dieses Profil werden der Windows-Update-Dienst installiert und automatische Updates aktiviert.

6.5 Datum der Signaturdateien

Die Datumsangaben der neuesten Signaturdateien für Viren- und Spywareschutzsoftware werden nicht vom Agenten abgerufen.

Wichtig: Weitere Informationen finden Sie unter [Ereignisprotokoll](#) (Seite 25).

Ursache: Sophos NAC Advanced lädt nicht die neuesten Signaturdateien herunter.

Lösung: Überprüfen Sie auf der Startseite von Compliance Manager im Bereich „Server Task Status“, ob der Current Definition Loader abgebrochen wurde und aus welchem Grund dies passiert ist. Die wahrscheinlichste Fehlerursache liegt darin, dass der Server nicht auf das Internet zugreifen kann. Für Current Definition Loader ist Internetzugriff jedoch erforderlich. Starten Sie den Task „Current Definition Loader“ auf dem Server manuell, damit die Signaturdaten heruntergeladen und aktualisiert werden können. Weitere Informationen finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

7 Registrierungprobleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Registrierungsproblemen des Endpoints.

7.1 Registrierung

Registrierung fehlgeschlagen

Wichtig: Weitere Informationen finden Sie unter [Datenübertragungsprobleme von Agent zu Server](#) (Seite 8).

Authentifizierung fehlgeschlagen

Ursache: Dem Agenten wurde der falsche Benutzername bzw. das falsche Kennwort übermittelt.

Lösung: Stellen Sie sicher, dass der Benutzername bzw. das Kennwort für den Agenten korrekt ist. Der Benutzername bzw. das Kennwort wird entweder direkt vom Benutzer in das Registrierungsfenster eingegeben oder über die Befehlszeile durch ein Skript oder eine andere Anwendung, z.B. einen Dialer, übermittelt.

Ursache: Der Benutzer wurde nicht im Benutzerspeicher des Kunden konfiguriert.

Lösung: Legen Sie den Benutzernamen bzw. das Kennwort im Benutzerspeicher des Kunden (z.B. unter Active Directory oder Windows NT) fest.

Ursache: Gemeinsamer geheimer Schlüssel des IAS stimmt nicht überein.

Hinweis: Weitere Informationen zur Fehlerdiagnose über das Authentication Test-Tool finden Sie in der *Sophos NAC Advanced Tools-Anleitung*.

Lösung: Zur Ermittlung eines nicht übereinstimmenden gemeinsamen geheimen IAS-Schlüssels rufen Sie den Wert des gemeinsamen geheimen Schlüssels über das Secret Encryption-Tool ab, und testen Sie ihn im Authentication Test-Tool. Ein nicht übereinstimmender gemeinsamer geheimer Schlüssel meldet eine „ungültige Antwort“, die in etwa wie folgt aussieht:

„Completed Attempt (1): To server 127.0.0.1:1812. Status: InvalidResponse In 2578.1085 mS. Radius request failed after all attempts. Last Reason: InvalidResponse“

Dieses Problem beheben Sie wie folgt:

Setzen Sie den gemeinsamen geheimen IAS-Schlüssel mit dem Secret Encryption-Tool im Policy Interface und den IAS shared secret auf dem RADIUS-Client.

Ursache: Authentifizierungstyp stimmt nicht überein.

Hinweis: Weitere Informationen zur Fehlerdiagnose über das Authentication Test-Tool finden Sie in der *Sophos NAC Advanced Tools-Anleitung*.

Lösung: Zur Ermittlung eines nicht übereinstimmenden Authentifizierungstyps rufen Sie den Wert des Authentifizierungstyps von der Datei „Registration Interface Web.config“ ab (der Standard nach Installation ist MS-CHAP v2) und testen Sie den Wert anhand des Authentication Test-Tools. Ein nicht übereinstimmender Authentifizierungstyp zeigt einen Zugriffsverweigerungsfehler an, der ungefähr wie folgt aussieht:

„Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS.“

Wenn Sie keine RADIUS-Server einsetzen, befindet sich im Systemereignis-Protokoll eine Meldung, die wie folgt aussieht:

„Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy.“

Dieses Problem beheben Sie wie folgt:

- Ändern Sie den Authentifizierungstyp in der Datei „Registration Interface Web.config“ (normalerweise im Unterverzeichnis Inetpub\wwwroot\RegistrationInterface auf dem Compliance Anwendungsserver) so, dass er einem der Authentifizierungstypen auf dem authentifizierenden RADIUS-Server entspricht.
- Wenn Sie einen RADIUS-Proxyserver einsetzen, überprüfen Sie das Protokoll oder die Konfiguration des authentifizierenden RADIUS-Servers, um die verwendeten Authentifizierungsmethoden zu ermitteln. Ändern Sie den Authentifizierungstyp in der Datei „Web.config“ der Richtlinienchnittstelle so, dass er einem der Authentifizierungstypen des authentifizierenden RADIUS-Servers entspricht.

Im Ereignisprotokoll des Compliance Anwendungsservers werden Fehler in Zusammenhang mit der Registrierungsschnittstelle (Registration Interface) angezeigt

Ursache: Die Registrierungsschnittstelle kann nicht mit dem RADIUS Enforcer kommunizieren.

Lösung: Suchen Sie im Ereignisprotokoll von Compliance Anwendungsserver nach Fehlern. Wenn ein Fehler besagt, dass alle Kontaktversuche zum RADIUS Enforcer fehlgeschlagen sind, überprüfen Sie mithilfe des Secret Encryption-Tools die IP-Adresse, Protokolle und den gemeinsamen geheimen Schlüssel des RADIUS Enforcers in der Registrierungsschnittstelle. Weitere Informationen finden Sie in der *Sophos NAC Advanced Tools-Anleitung*.

8 Report-Probleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Report-Problemen.

8.1 Agent

Agent kann keinen Report erstellen

Wichtig: Weitere Informationen finden Sie unter [Datenübertragungsprobleme von Agent zu Server](#) (Seite 8).

Ursache: Die Registrierung des Benutzers am Agenten ist abgelaufen. Im Ergebnisfenster wird folgender Fehler angezeigt: „Der Report-Vorgang schlug aufgrund einer abgelaufenen Benutzerregistrierung fehl. Sie müssen den Agent neu registrieren.“

Lösung: Der Benutzer muss sich am Agenten über die Schaltfläche Register neu anmelden.

8.2 Compliance Manager

Im Agent Session-Report fehlen Daten

Ursache: Wenn Sie den Quarantine Agent verwenden, wurde das Reporting-Intervall der Richtlinie noch nicht erreicht und deshalb hat der Agent die Report-Daten nicht aktualisiert.

Lösung: Aktualisieren Sie die Report-Daten über eine vom Benutzer eingeleitete Konformitätsprüfung über die Menüoption „Konformität überprüfen“ des Quarantine Agent-Symbols im Statusbereich der Taskleiste.

Reports sehen unvollständig aus oder es fehlen Daten

Ursache: Policy Transfer Service ist möglicherweise nicht aktiv.

Lösung: Starten Sie den Policy Transfer Service auf dem Compliance Anwendungsserver und stellen Sie ihn auf „Automatic“.

Die Erstellung eines Reports mit archivierten Daten liefert keine Ergebnisse

Ursache: Der Task „Report Warehouse Loader SQL“ wurde nicht gestartet.

Lösung: Wenn dies der Fall ist, wird im Report neben dem Reportnamen „No Data Available“ angezeigt. Überprüfen Sie im Bereich „Server Task Status“ auf der Startseite von Compliance Manager, wann der „Report Warehouse Loader“ ausgeführt wurde und ob Fehler aufgetreten sind. Überzeugen Sie sich davon, dass der SQL Server Agent auf der Instanz ausgeführt wird, die die Compliance Datenbanken hostet. Standardmäßig führt der SQL Server Agent jede Nacht um 2.30 Uhr (oder zu einem manuell festgelegten Zeitpunkt) den Task „Report Warehouse Loader“ aus, der Daten von der ReportStore-Datenbank in die ReportStoreWH-Datenbank verschiebt. Es empfiehlt sich, in den Eigenschaften des SQL Server Agent festzulegen, dass dieser nach einem unverhofften Abbruch automatisch neu gestartet wird. Außerdem muss der SQLAgent-Dienst (Instanzname) ausgeführt werden. Es empfiehlt sich, die Instanz „SQLAgent“ auf „Automatic“ zu setzen.

Weitere Informationen zum Task „Sophos NAC - Load WH“ finden Sie in der Sophos NAC Advanced installation guide.

Die Erstellung eines Reports mit archivierten Daten liefert Ergebnisse, die nicht mehr aktuell sind

Ursache: Der Task „Report Warehouse Loader SQL“ wurde längere Zeit nicht mehr ausgeführt.

Lösung: Wenn dies der Fall ist, wird im Report neben dem Reportnamen Folgendes angezeigt: „Use Data from the Last Archive (mm/dd/yyyy hh:mm:ss)“. Dabei liegt das Datum mehr als 24 Stunden hinter dem eigentlichen Datum zurück. Überprüfen Sie im Bereich „Server Task Status“ auf der Startseite von Compliance Manager, wann der „Report Warehouse Loader“ ausgeführt wurde und ob Fehler aufgetreten sind. Überzeugen Sie sich davon, dass der SQL Server Agent auf der Instanz ausgeführt wird, die die Compliance Databases hostet. Standardmäßig führt der SQL Server Agent jede Nacht um 2:30 Uhr den Task „Report Warehouse Loader SQL“ aus, der Daten von der ReportStore-Datenbank in die ReportStoreWH-Datenbank verschiebt. Es empfiehlt sich, in den Eigenschaften des SQL Server Agent festzulegen, dass dieser nach einem unverhofften Abbruch automatisch neu gestartet wird. Außerdem muss der SQLAgent-Dienst (Instanzname) ausgeführt werden. Es empfiehlt sich, die Instanz „SQLAgent“ auf „Automatic“ zu setzen.

Weitere Informationen zum Task „Sophos NAC - Load WH“ finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

Die Erstellung eines Reports mit aktuellen Daten liefert veraltete Ergebnisse

Ursache: Wenn Sie den Quarantine Agent verwenden, wurde das Reporting-Intervall der Richtlinie noch nicht erreicht und deshalb hat der Agent die Report-Daten nicht aktualisiert.

Lösung: Aktualisieren Sie die Report-Daten über eine vom Benutzer eingeleitete Konformitätsprüfung über die Menüoption „Konformität überprüfen“ des Quarantine Agent-Symbols im Statusbereich der Taskleiste.

Ursache: Der Agent Report Service ist möglicherweise nicht aktiv.

Lösung: Starten Sie den Agent Report Service auf dem Compliance Anwendungsserver und stellen Sie ihn auf „Automatic“.

Die Erstellung eines Reports mit archivierten Daten liefert unvollständige Ergebnisse

Ursache: Der Task „Sophos NAC - Load WH“ wurde längere Zeit nicht mehr ausgeführt oder lässt sich nicht ausführen.

Lösung: Wenn dies der Fall ist, wird im Report neben dem Reportnamen Folgendes angezeigt: „Use Data from the Last Archive (mm/dd/yyyy hh:mm:ss)“. Dabei liegt das Datum mehr als 24 Stunden hinter dem eigentlichen Datum zurück. Überprüfen Sie auf der Startseite von Compliance Manager im Bereich „Server Task Status“, ob der Task „Report Warehouse Loader“ nicht ausgeführt werden konnte und aus welchem Grund dies passiert ist. Überzeugen Sie sich davon, dass der SQL Server Agent auf der Instanz ausgeführt wird, die die Compliance Datenbanken hostet. Standardmäßig führt der SQL Server Agent jede Nacht um 2.30 Uhr (oder zu einem manuell festgelegten Zeitpunkt) den Task „Report Warehouse Loader“ aus, der Daten von der ReportStore-Datenbank in die ReportStoreWH-Datenbank verschiebt. Es empfiehlt sich, in den Eigenschaften des SQL Server Agent festzulegen, dass dieser nach einem unverhofften Abbruch automatisch neu gestartet wird. Außerdem muss der SQLAgent-Dienst (Instanzname) ausgeführt werden. Es empfiehlt sich, die Instanz „SQLAgent“ auf „Automatic“ zu setzen.

Weitere Informationen zum Task „Report Warehouse Loader“ finden Sie in der *Sophos NAC Advanced Installationsanleitung*.

9 Probleme mit Alerts

Dieser Abschnitt beschreibt die Fehlerbehebung bei Problemen mit Alerts.

9.1 Compliance Manager

Gesendete Alerts werden nicht empfangen

Ursache: Das Ereignisprotokoll ist voll.

Lösung: Überprüfen Sie, ob für das Ereignisprotokoll genug Speicherplatz auf dem Compliance Anwendungsserver vorhanden ist.

Ursache: Der E-Mail-Server wurde nicht richtig konfiguriert.

Lösung: Suchen Sie im Ereignisprotokoll des Compliance Anwendungsservers nach Fehlern. Die SMTP-Verbindung (an TCP-Port 25) zwischen dem Compliance Anwendungsserver und dem E-Mail-Server muss funktionieren. Überprüfen Sie außerdem, ob der richtige E-Mail-Server in Compliance Manager konfiguriert wurde (**Configure System > Alerts** und dort die Einstellung **Alert E-mail Server**).

Ursache: Der Alert Service läuft möglicherweise nicht.

Lösung: Starten Sie den Alert Service auf dem Compliance Anwendungsserver und stellen Sie ihn auf „Automatic“.

Ursache: Der Alert wurde in Compliance Manager nicht richtig konfiguriert.

Lösung: Im Allgemeinen empfiehlt es sich, Richtlinien und Alerts vor dem Einsatz in einer Arbeitsumgebung anhand einer Testgruppe zu testen. So stellen Sie sicher, dass alle Einstellungen richtig sind.

10 Serverprobleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Serverproblemen, die **nicht** vom Agenten verursacht wurden.

10.1 Compliance Anwendungsserver

SQL Server kann vom Compliance Anwendungsserver in Sophos NAC Advanced nicht erreicht werden

Ursache: Der Compliance Anwendungsserver ist nicht ordnungsgemäß für die Kommunikation mit den Compliance Datenbanken verbunden.

Lösung: Verfahren Sie zum Überprüfen der Verbindung auf dem Compliance Anwendungsserver über ein Sophos NAC Advanced-Dienstkonto mit Zugriff auf die Compliance Datenbanken wie folgt:

1. Erstellen Sie eine neue Textdatei auf dem Desktop des Compliance Anwendungsservers.
2. Benennen Sie die Datei „conn.udl“ um. Die .udl-Erweiterung **muss** verwendet werden.
3. Sobald sie erstellt ist, doppelklicken Sie auf die Datei „conn.udl“.
4. Klicken Sie im Fenster „Data Link Properties“ auf die Registerkarte **Provider**.
5. Wählen Sie **Microsoft OLE DB Provider for SQL Server** und klicken Sie auf **Next**.
6. Geben Sie den SQL-Servernamen oder die Serverinstanz ein oder treffen Sie eine Auswahl. Dies **muss** derselbe Name sein, den Sie bei der Installation des Compliance Anwendungsservers angegeben haben.
7. Klicken Sie auf **Use Windows NT Integrated security**.
8. Klicken Sie auf **Select the database on the server**.
9. Wählen Sie im Listenfenster **PolicyStore**.
10. Klicken Sie auf **Test Connection**.

Mögliche Ursachen für Verbindungsprobleme werden unter [Installation der Compliance-Datenbanken](#) (Seite 3) und „Die Komponenten des Compliance Anwendungsservers oder des RADIUS-Servers können keine Verbindung zu den Compliance Datenbanken" herstellen“ im folgenden Abschnitt dargelegt: [SQL-Server](#) (Seite 25).

10.2 RADIUS-Server

SQL-Server ist nicht über den RADIUS-Server ansprechbar

Ursache: Die Verbindung zwischen dem RADIUS-Server und den Compliance Datenbanken ist nicht ordnungsgemäß eingerichtet.

Lösung: Um die Verbindung zu überprüfen, führen Sie folgende Schritte auf dem RADIUS-Server durch. Verwenden Sie dazu ein Sophos NAC Advanced-Dienstkonto mit Zugriff auf die Compliance Datenbanken:

1. Erstellen Sie eine neue Textdatei auf dem Desktop des RADIUS-Servers.
2. Benennen Sie die Datei „conn.udl“ um. Die .udl-Erweiterung **muss** verwendet werden.
3. Sobald sie erstellt ist, doppelklicken Sie auf die Datei „conn.udl“.
4. Klicken Sie im Fenster „Data Link Properties“ auf die Registerkarte **Provider**.

5. Wählen Sie **Microsoft OLE DB Provider for SQL Server** und klicken Sie auf **Next**.
6. Geben Sie den SQL-Servernamen oder die Serverinstanz ein oder treffen Sie eine Auswahl. Dies **muss** derselbe Name sein, den Sie bei der Installation des RADIUS-Servers angegeben haben.
7. Klicken Sie auf **Use Windows NT Integrated security**.
8. Klicken Sie auf **Select the database on the server**.
9. Wählen Sie im Listenfenster **PolicyStore**.
10. Klicken Sie auf **Test Connection**.

Mögliche Ursachen für Verbindungsprobleme werden unter [Installation der Compliance-Datenbanken](#) (Seite 3) und „Die Komponenten des Compliance Anwendungsservers oder des RADIUS-Servers können keine Verbindung zu den Compliance Datenbanken herstellen“ im folgenden Abschnitt dargelegt: [SQL-Server](#) (Seite 25).

10.3 SQL-Server

Die Komponenten des Compliance Anwendungsservers oder des RADIUS-Servers können keine Verbindung zu den Compliance Datenbanken herstellen.

Ursache: Die Berechtigungen für Sophos NAC Advanced sind in den Compliance Datenbanken nicht ordnungsgemäß eingerichtet.

Lösung:

1. Öffnen Sie auf dem Compliance Anwendungsserver das Services Snap-in.
2. Prüfen Sie im Sophos NAC Host-Dienst, unter welcher Kontenkennung der Dienst läuft.
3. Überprüfen Sie, ob die Kontenkennung über Zugriffsberechtigungen für die Compliance Datenbanken verfügt.

10.4 Ereignisprotokoll

Im Ereignisprotokoll des Compliance Anwendungsservers werden Fehler in Zusammenhang mit dem Patch Loader oder Current Definition Loader angezeigt

Ursache: Der Compliance Anwendungsserver verfügt nicht über Internetzugriff.

Lösung:

1. Stellen Sie sicher, dass der Compliance Anwendungsserver über Internetzugang verfügt.
2. Wenn ein Proxyserver verwendet wird, muss er im Compliance Manager konfiguriert werden. Klicken Sie auf **Configure System > Server Settings** . Klicken Sie auf den Namen des Servers und machen Sie im Feld **Server Details** die erforderlichen Angaben zum Proxyserver.
3. Wenn weiterhin Fehler zum Patch Loader oder Current Definition Loader angezeigt werden, wenden Sie sich an den [technischen Support](#) (Seite 35).

Hinweis: Wenn der Compliance Anwendungsserver nicht über eine Internetverbindung verfügt, lässt sich Current Definition Loader nicht ohne Weiteres updaten. Da diese Datei stündlich upgedatet wird, verlieren Daten schnell ihre Aktualität. Die Datei umfasst die aktuellen Daten für die aktuellen Signaturen für Viren- und Spywareschutzanwendungen.

11 Enforcer-Probleme

Dieser Abschnitt beschreibt die Fehlerbehebung bei Enforcer-Problemen.

11.1 Netzwerkzugriff

Dem Endpoint wird der Netzwerkzugriff verweigert, wenn er zugelassen werden sollte (oder umgekehrt). Der Endpoint wird isoliert, wenn er nicht isoliert werden sollte. Oder im Dialogfeld „Agent Results“ werden falsche Meldungen angezeigt

Ursache: Dieses Problem kann neben dem Problem „Endpoint empfängt die falsche Richtlinie“ oder „Endpoint führt keine Überprüfung mit einer aktuellen Richtlinie durch“ auftreten.

Weitere Informationen finden Sie unter [Prüfung und Durchsetzung von Richtlinien](#) (Seite 12).

Lösung: Überprüfen Sie anhand des Agent Session Reports von Compliance Manager, ob der Endpoint die richtige und aktuelle Richtlinie empfängt. Wenn dies nicht der Fall ist, befolgen Sie die Schritte zur Fehlerbehebung unter „Endpoint empfängt die falsche Richtlinie“ oder „Endpoint führt keine Überprüfung mit einer aktuellen Richtlinie durch“. Wenn der Agent die richtige und aktuelle Richtlinie empfängt, fahren Sie mit den anderen Schritten in diesem Abschnitt fort.

Ursache: Agent Enforcer, RADIUS Enforcer oder DHCP Enforcer verweigert Zugriff auf den Endpoint.

Lösung: In Compliance Manager kann der Agent Enforcer-, RADIUS Enforcer- oder DHCP-Enforcer-Report Aufschluss darüber geben, warum der Enforcer Zugriff für den Endpoint verweigert hat. Außerdem könnte die Benutzerauthentifizierung durch den RADIUS Enforcer fehlgeschlagen sein.

Ursache: Der Richtlinie sind die falschen Agent Enforcer Access Templates zugeordnet. Oder diese Access Templates sind nicht richtig eingestellt.

Lösung: Überprüfen Sie in Compliance Manager, ob den Agenten- und Konformitätszuständen in der Richtlinie die richtigen Agent Enforcer Access Templates zugewiesen wurden. Überprüfen Sie, ob die in der Richtlinie verwendeten Agent Enforcer Access Templates die erforderlichen Netzwerkressourcen enthalten. Die Netzwerkressourcen müssen außerdem die richtigen Namen für ausführbare Dateien, Ports/Protokolle oder IP-Adressen besitzen, sofern zutreffend.

Die Agent Enforcer Access Template, die in der Richtlinie standardmäßig auf den Konformitätszustand „Non-Compliant“ übertragen wird, gibt in internen Netzwerken, die private IP-Adressen verwenden, den Zugriff auf alle Sophos Produkte und auf das Internet frei. Alle übrigen Datenbewegungen nach außen werden blockiert. Sie können diese Einstellungen ändern, indem Sie eine neue Agent Enforcer Access Template erstellen und sie dem Konformitätszustand „Non-Compliant“ in der Richtlinie des Endpoints zuweisen.

Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Um einen Konformitätszustand durchzusetzen, müssen Sie den Richtlinienmodus auf „Enforce“ setzen.

Ursache: Falsche RADIUS Enforcer oder DHCP Enforcer Access Templates oder RADIUS Enforcer oder DHCP Enforcer Access Templates mit falschen Einstellungen sind der Richtlinie bzw. den Enforcer-Einstellungen zugeordnet.

Lösung: Überprüfen Sie anhand von Compliance Manager, ob die richtigen RADIUS Enforcer oder DHCP Enforcer Access Templates auf die richtigen Access und Compliance States in der Richtlinie und in den Enforcer-Einstellungen übertragen wurden. Vergewissern Sie sich, dass die RADIUS Enforcer oder DHCP Enforcer Access Templates die korrekten Einstellungen enthalten.

Wenn Sie eine Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ oder „Remediate“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert. Um einen Konformitätszustand durchzusetzen, müssen Sie den Richtlinienmodus auf „Enforce“ setzen.

Ursache: RADIUS Enforcer oder DHCP Enforcer Access Templates wurde eine falsche Priorität zugeordnet.

Lösung: Überprüfen Sie in Compliance Manager, ob den RADIUS Enforcer oder DHCP Enforcer Access Templates in der Richtlinie oder in den Enforcer-Einstellungen die richtige Priorität zugewiesen wurde. Ordnen Sie speziellen bzw. einschränkenden Access Templates eine höhere Priorität zu als allgemeineren Access Templates. Die speziellen bzw. einschränkenden Access Templates bieten eine bestimmte IP-Adresse oder einen einschränkenden IP-Adressenbereich. Im Gegensatz dazu bieten die allgemeineren Access Templates einen umfangreicheren IP-Adressenbereich.

Ursache: Ausführbare Netzwerkressource wird von der Software nicht erkannt.

Lösung: Der Name des ausführbaren Prozesses muss dem im Windows Task Manager unter **Prozesse** angezeigten Namen entsprechen.

Die Software erkennt nur ausführbare Dateien auf der Winsock-Ebene. Die Anwendung wird nur erkannt, wenn sie auf der Winsock-Ebene ausgeführt wird.

Ursache: Netzwerkressourcen wurde eine falsche Priorität zugeordnet.

Lösung: Überprüfen Sie in Compliance Manager, ob den Netzwerkressourcen in der Agent Enforcer Access Template die richtige Priorität zugewiesen wurde. Ordnen Sie speziellen bzw. einschränkenden Netzwerkressourcen eine höhere Priorität zu als allgemeinen Netzwerkressourcen. Wenn einem Endpoint mehr als eine Netzwerkressource zugewiesen ist, bestimmt die erste passende Netzwerkressource den Netzwerkzugriff für die Endpoint-Sitzung. Ausführbare Netzwerkressourcen werden vor Port-/Protokoll-Netzwerkressourcen analysiert.

Ursache: Endpoint wurde fälschlicherweise von der Überprüfung ausgeschlossen (oder umgekehrt).

Lösung: Sorgen Sie über Compliance Manager dafür, dass der Endpoint **keine** Exemption ist, wenn er auf Konformität überprüft wird. Der Endpoint muss folglich eine Exemption sein, wenn er **nicht** auf Konformität überprüft werden soll.

Die entsprechenden RADIUS Enforcer oder DHCP Enforcer Access Templates müssen auf die Exemptions übertragen werden.

Außerdem muss den Exemptions in der Exemptions-Liste die richtige Priorität zugeordnet sein. Ordnen Sie speziellen bzw. einschränkenden Exemptions eine höhere Priorität zu als allgemeineren Exemptions. Wenn einem Endpoint mehr als eine Exemption zugewiesen ist, bestimmt die erste passende Exemption den Netzwerkzugriff für die Endpoint-Sitzung. Wenn außerdem einer bestimmten Exemption mehr als eine Access Template zugewiesen ist, wird die erste Template verwendet, die die übereinstimmende IP-Adresse des RADIUS-Clients, DHCP Servers oder DHCP-Relays enthält.

Ursache: Die individuellen Regeln zur Anwendungserkennung sind in Compliance Manager falsch festgelegt.

Lösung:

1. Überprüfen Sie die individuellen Regeln zur Anwendungserkennung in Compliance Manager auf ihre Richtigkeit. Weitere Informationen finden Sie unter „Anwendung wird auf dem Endpoint nicht erkannt oder Erkennung schlägt fehl“ im Abschnitt *Prüfung und Durchsetzung von Richtlinien* (Seite 12).
2. Aktivieren Sie auf dem Agenten die Protokollierungsstufe „Brief Trace“. Aktivieren Sie das Kontrollkästchen „Protokollierung aktivieren“ im Fenster mit der Versionsinfo. Achten Sie darauf, dass in der Agent Configuration Template, die der Richtlinie des Endpoints zugewiesen wurde, die Protokollierung des Agenten auf Fehler- und Warnmeldungen, Informationen sowie die Erstellung kurzer Ablaufverfolgungsmeldungen eingestellt ist. Versuchen Sie, die Erkennungsprobleme anhand des API-Protokolls des Agenten (<GUID>_trace.log) zu beheben.

Hinweis: Protokollierung beeinträchtigt die Leistung. Aus diesem Grund empfiehlt es sich, die Protokollierung nur zur Fehlersuche zu aktivieren und danach wieder zu deaktivieren. Protokolldateien für Windows 2000 und Windows XP befinden sich im Verzeichnis <Laufwerk>:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Sophos\Sophos NAC\Logs. Protokolldateien für Windows Vista und Windows 7 befinden sich im Verzeichnis <Laufwerk>:\Programmdaten\Sophos\Sophos NAC\Logs.

Ursache: Die zur Richtlinie gehörigen Profile oder individuellen Anwendungen enthalten möglicherweise nicht das Betriebssystem des Endpoints und werden deshalb nicht ordnungsgemäß überprüft.

Lösung:

1. Überprüfen Sie in Compliance Manager, ob das Betriebssystem des Endpoints in der zugewiesenen Richtlinie als Betriebssystemprofil angegeben ist und ob auch individuellen Anwendungen, die mit der Richtlinie (über Anwendungsprofile) in Zusammenhang stehen, dieses Betriebssystem zugewiesen ist.
2. Sehen Sie sich über Compliance Manager den Non-Compliance Detail Report oder den Agent Session Report und den Assessment Details-Link an, um sicherzustellen, dass der Agent die Anwendungen überprüft.

Ursache: Dem Agent Policy Update Threshold zufolge ist der letzte Richtlinienabruf des Endpoints veraltet.

Lösung: Der letzte Richtlinienabruf des Endpoints muss in dem im Feld „Agent Policy Update Threshold“ in Compliance Manager (**Configure System > Enforcer Settings**) angegebenen Zeitraum stattgefunden haben. Rufen Sie die Richtlinie über eine vom Benutzer eingeleitete Konformitätsprüfung über die Menüoption „Konformität überprüfen“ des Quarantine Agent-Symbols im Statusbereich der Taskleiste ab.

Ursache: Das Kontrollkästchen „Override Enforcers“ in Compliance Manager (**Configure System > Enforcer Settings**) wurde aktiviert.

Lösung: Deaktivieren Sie das Kontrollkästchen „Override Enforcers“ und stellen Sie sicher, dass dem Access State „Default“ die richtige Access Template für diesen RADIUS oder DHCP Enforcer zugewiesen wurde.

Ursache: Compliance Agent läuft nicht auf dem Endpoint.

Hinweis: Dieses Problem tritt nur beim Quarantine Agent auf.

Lösung:

1. Stellen Sie sicher, dass der Compliance Agent läuft.
2. Der Agent API-Dienst muss aktiv sein.

Ursache: Die in der Richtlinie festgelegte Einstellung der Agent Enforcement Action (im Bereich DHCP Agent Settings) ist auf **None** eingestellt und der Endpoint verwendet immer noch eine nicht konforme IP-Adresse.

Hinweis: Dieses Problem trifft nur für DHCP Enforcement zu.

Lösung: Wenn die in der Richtlinie festgelegte DHCP Agent Enforcement Action auf **None** eingestellt ist und der Zustand des Endpoints sich von nicht konform auf konform geändert hat, empfängt der Endpoint möglicherweise keine konforme IP-Adresse. Ändern Sie die Einstellung der Agent Enforcement Action auf **Release Renew**, speichern Sie die Richtlinie und führen Sie am Endpoint eine vom Benutzer eingeleitete Konformitätsprüfung durch.

Ursache: In der Richtlinie ist die Einstellung „Agent Enforcement Action“ (im Bereich „802.1x Agent Settings“) in der Richtlinie auf None eingestellt, und der Endpoint ist immer noch einem VLAN in Quarantäne zugewiesen.

Hinweis: Dieses Problem trifft nur für 802.1x Enforcement zu.

Lösung: Wenn die „802.1x Agent Enforcement Action“ auf None eingestellt ist und der Zustand des Endpoints sich von nicht konform in konform geändert hat, wurde der Endpoint möglicherweise nicht neu authentifiziert und einem konformen VLAN zugewiesen. Ändern Sie die Einstellung der Agent Enforcement Action in **Reauthentication**, speichern Sie die Richtlinie und führen Sie am Endpoint eine vom Benutzer eingeleitete Konformitätsprüfung durch.

Ursache: Meldung bzgl. Zugriffsverweigerung oder Quarantäne wird nicht angezeigt.

Lösung:

1. Überprüfen Sie, ob eine Meldung erstellt wird, ob sie mit der richtigen Profilbedingung verbunden ist und die Bedingung am Endpoint erfüllt wurde. Sehen Sie sich in Compliance Manager den Non-Compliance Detail Report oder den Agent Session Report und den Assessment Details-Link für die Profildetails sowie die angezeigten Meldungen an, um festzustellen, warum der Endpoint keinen Zugriff erhielt oder isoliert wurde und keine Meldung erhalten hat.
2. Überprüfen Sie, ob sich die Richtlinie im Modus „Remediate“ bzw. „Enforce“ befindet. Im Modus „Report Only“ werden keine Meldungen angezeigt. Wenn Sie eine Agent Enforcer Access Template verwenden, die den Netzwerkzugriff im Modus „Report Only“ verhindert, wird allen Endpoints ungeachtet ihres Konformitätszustands der Zugriff verweigert.
3. Die richtigen Access Templates müssen auf die entsprechenden Richtlinienzugriffs- und Konformitätszustände übertragen sein. Überprüfen Sie, ob die Access Templates über die richtigen Einstellungen und Netzwerkressourcen verfügen.

Ursache: Die Installation von Sicherheitsanwendungen auf dem Endpoint könnte zu Problemen führen.

Lösung:

1. Sehen Sie sich in Compliance Manager den Non-Compliance Detail Report oder den Agent Session Report und den Assessment Details-Link für Details zur Konformitätsprüfung an, um das Problem des Agenten zu ermitteln.
2. Überprüfen Sie, ob Sie den richtigen Anwendungsnamen in Verbindung mit dem Profil verwenden, das der Richtlinie zugewiesen wurde. Anwendungen werden in Compliance Manager unter dem Hauptproduktnamen aufgelistet. Unter Umständen wird die Anwendung unter einem anderen Namen vertrieben. Um den Hauptproduktnamen zu ermitteln, überprüfen Sie das installierte Produkt oder wenden Sie sich an den Hersteller.
3. Die festgelegten Sicherheitsanwendungen müssen auf dem Endpoint erwartungsgemäß funktionieren. Weitere Informationen erhalten Sie auf der Website der Sicherheitsanwendung, in den Hinweisen zur Fehlersuche und ggf. beim Support.

Ursache: Unbestimmte Netzwerkzugriffsprobleme.

Lösung:

1. Die Richtlinie muss korrekt sein.
2. Sehen Sie sich in Compliance Manager den Non-Compliance Detail Report oder den Agent Session Report und den Assessment Details-Link für Details zur Konformitätsüberprüfung an.
3. Sehen Sie sich in Compliance Manager den Agent Session Report an und sorgen Sie dafür, dass der Agent die korrekte Richtlinie und Richtlinienversion erhält.
4. Sehen Sie sich in Compliance Manager den Agent Enforcer, RADIUS Enforcer, DHCP Enforcer, RADIUS Exemption oder DHCP Exemption Report für weitere Informationen zum Netzwerkzugriff und zur Fehlersuche bei Ausnahmen an.

11.2 802.1x

Authentifizierung des Benutzers nicht am 802.1x Authentifikator/Switch möglich

Lösung: Suchen Sie im Systemereignisprotokoll des Compliance Anwendungsservers im IAS-Eintrag nach dem Benutzer. Wenn der folgende Fehler angezeigt wird, liegt wahrscheinlich ein Netzwerkzugriffsproblem vor: „The request was rejected by a third-party extension DLL file.“

Wichtig: Weitere Informationen finden Sie unter [Netzwerkzugriff](#) (Seite 26).

Lösung: Suchen Sie im Systemereignisprotokoll des Compliance Application Servers im IAS-Eintrag nach dem Benutzer. Wenn einer der folgenden Fehler aufgeführt ist, liegt wahrscheinlich ein Authentifizierungsproblem vor: „The connection attempt did not match any remote access policy.“ oder „The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request.“

Wichtig: Weitere Informationen finden Sie unter [Konfigurationseinstellungen des RADIUS Enforcers](#) (Seite 31).

IAS kann den Endpoint nicht authentifizieren

Ursache: Laut einem Systemfehler auf dem Compliance Anwendungsserver ist EAP kein gültiges Protokoll. Daher ist die RAS-Richtlinie des IAS nicht für das EAP-Protokoll konfiguriert.

Lösung: Suchen Sie im Systemereignisprotokoll des Compliance Anwendungsservers nach Fehlern. Wenn eine Meldung darauf hinweist, dass EAP ein ungültiges Protokoll sei, bearbeiten Sie das Profil der RAS-Richtlinie auf dem Compliance Anwendungsserver und ergänzen Sie es um die zum Endpoint passenden EAP-Typen (**Authentication > EAP Methods**).

Am 802.1x Authentifikator/Switch wird ein falsches VLAN zugewiesen

Ursache: In der Richtlinie ist die Einstellung „Agent Enforcement Action“ (im Bereich „802.1x Agent Settings“) in der Richtlinie auf None eingestellt, und der Endpoint ist immer noch einem VLAN in Quarantäne zugewiesen.

Lösung: Wenn die „802.1x Agent Enforcement Action“ auf None eingestellt ist und der Zustand des Endpoints sich von nicht konform in konform geändert hat, wurde der Endpoint möglicherweise nicht neu authentifiziert und einem konformen VLAN zugewiesen. Ändern Sie die Einstellung der Agent Enforcement Action in **Reauthentication**, speichern Sie die Richtlinie und führen Sie am Endpoint eine vom Benutzer eingeleitete Konformitätsprüfung durch.

Ursache: Die Einstellungen der RADIUS Access Template in Compliance Manager sind nicht korrekt.

Lösung: Für jeden Gerätehersteller gelten andere RADIUS-Attribute. Informationen zu den entsprechenden RADIUS-Attributen für ein bestimmtes Gerät entnehmen Sie bitte der Dokumentation zum Gerät.

Ursache: Die Einstellungen der RADIUS Access Template in Compliance Manager enthalten keine zum 802.1x Authentifikator/Switch passende IP-Adresse.

Lösung: Stellen Sie sicher, dass die Einstellungen der RADIUS Access Template die zum 802.1x Authentifikator/Switch passende IP-Adresse in der IP-Adressenliste enthalten.

Ursache: Über Compliance Manager konfigurierte VLANs existieren nicht auf dem 802.1x Authentifikator/Switch.

Lösung: Fügen Sie das entsprechende VLAN zum 802.1x Authentifikator/Switch hinzu.

Der Agent kann nicht im Besucher-VLAN des 802.1x Authentifikators/Switches eingesetzt werden.

Ursache: Das Besucher-VLAN des 802.1x Authentifikators/Switches verweigert den Zugang zum Compliance Anwendungsserver.

Lösung: Sorgen Sie dafür, dass das Besucher-VLAN des 802.1x Authentifikators/Switches den Zugriff auf den Compliance Anwendungsserver ermöglicht.

11.3 Konfigurationseinstellungen des RADIUS Enforcers

Benutzer kann sich im VPN nicht am Netzwerkgerät authentifizieren

Ursache: Dem Endpoint wird eine RADIUS Enforcer Access Template zugewiesen, die irrtümlicherweise den Zugriff verweigert.

Lösung: Ermitteln Sie über den RADIUS Enforcer Report, welche Access Template aus welchem Grund dem Endpoint zugewiesen wird.

Die richtigen RADIUS Enforcer Access Templates müssen auf die entsprechenden Access und Compliance States in der Richtlinie und in den Enforcer-Einstellungen übertragen sein. Überprüfen Sie, ob die Access Templates über die richtigen Einstellungen und Netzwerkressourcen verfügen.

Ursache: Die RAS-Richtlinie ist entweder falsch eingerichtet oder der Benutzer wurde nicht in den Benutzerspeicher aufgenommen.

Lösung:

1. Ermitteln Sie in Compliance Manager über den RADIUS Enforcer Report, warum der Benutzer über den RADIUS Enforcer nicht authentifiziert werden konnte.
2. Überprüfen Sie die RAS-Richtlinien. Diese Ursache lässt sich im Systemereignisprotokoll im IAS-Eintrag des Benutzers nach dem folgenden Grund überprüfen: „The connection attempt did not match any remote access policy.“ For a sample remote access policy, see the *Sophos NAC Advanced Installationsanleitung*.

Ursache: Der Remote-RADIUS-(Proxy-)Server hat die Anfrage verweigert.

Lösung:

1. Ermitteln Sie in Compliance Manager über den RADIUS Enforcer Report, warum der Benutzer über den RADIUS Enforcer nicht authentifiziert werden konnte.
2. Überprüfen Sie, ob alle Einstellungen auf dem authentifizierenden RADIUS-Server korrekt sind. Diese Ursache lässt sich im Systemereignisprotokoll im IAS-Eintrag des Benutzers nach dem folgenden Grund überprüfen: „The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request.“ Bei der aufgeführten IP-Adresse des Authentifizierungsservers handelt es sich außerdem um die IP-Adresse des Remote-RADIUS-Servers, der die Authentifizierungsanfrage des Benutzers abgewiesen hat. Wenn dies der Fall ist, finden Sie weitere Informationen in den Remote-RADIUS-Serverprotokollen.

Ursache: Authentifizierungstypen zwischen der RAS-Richtlinie des IAS und dem Netzwerkgerät stimmen nicht miteinander überein.

Bei dem Netzwerkgerät kann es sich um einen RAC, einen VPN-Konzentrator oder ein anderes Netzwerkgerät handeln, das eine Authentifizierung erfordert.

Hinweis: For more information on using the Authentication Test tool to diagnose issues, see the *Sophos NAC Advanced Tools-Anleitung*.

Lösung: Führen Sie über das Authentication Test-Tool einen Test durch. Wählen Sie die Authentifizierungsmethode des Netzwerkgeräts. Ein nicht übereinstimmender Authentifizierungstyp zeigt einen Zugriffsverweigerungsfehler an, der ungefähr wie folgt aussieht:

„Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS.“

Wenn Sie keine RADIUS-Server einsetzen, befindet sich im Systemereignis-Protokoll eine Meldung, die wie folgt aussieht:

„Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy.“

Dieses Problem beheben Sie wie folgt:

- Geben Sie in der Konfiguration des Netzwerkgeräts den Authentifizierungstyp an, oder geben Sie für die RAS-Richtlinie des IAS die Authentifizierungsmethode des Netzwerkgeräts an.
- Beim Einsatz von RADIUS-Proxyservern geben Sie in der Konfiguration des Netzwerkgeräts den Authentifizierungstyp des Remote-RADIUS-Servers an, oder geben Sie in der Konfiguration des Remote-RADIUS-Servers die Authentifizierungsmethode des Netzwerkgeräts an.

12 Probleme mit Anwendungen anderer Hersteller

Dieser Abschnitt enthält Hinweise zur Fehlerbehebung bei Problemen mit Anwendungen anderer Hersteller.

12.1 Anwendungen anderer Hersteller

Eine andere Anwendung funktioniert nicht

Ursache: Die Agent Enforcer Access Template verhindert die Ausführung einer anderen Anwendung.

Lösung: Die mit der Richtlinie des Endpoints verbundene Agent Enforcer Access Template muss korrekt sein. Versuchen Sie, die Quarantäne auf dem Endpoint außer Kraft zu setzen. Wenn die Anwendung nach Deaktivierung der Quarantäne funktioniert, stellen Sie sicher, dass die Netzwerkressourcen der Anwendung in der mit der Richtlinie des Endpoints verbundenen Agent Enforcer Access Template enthalten sind. Die Netzwerkressourcen müssen außerdem die richtigen Namen für ausführbare Dateien, Ports/Protokolle oder IP-Adressen besitzen, sofern zutreffend.

13 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

14 Rechtlicher Hinweis

Copyright © 2011 Sophos Limited. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Marken von Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.