



Endpoint Insights – Konfigurationsleitfaden

für Version 11,1



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Kontaktinformationen

Der RSA-Link unter <https://community.rsa.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens Dell ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Juli 2018

Inhalt

NetWitness Endpoint Insights – Übersicht	5
Endpoint-Serverkonfiguration	7
Konfigurieren der Weiterleitung von Metadaten für Agents von NetWitness Endpoint 11.1	10
Konfigurieren der Weiterleitung von Metadaten	10
Starten der Weiterleitung von Metadaten zum Log Decoder	11
Beenden der Weiterleitung von Metadaten zum Log Decoder	12
Entfernen der Weiterleitung von Metadaten	12
Metadatenzuordnungen für Endpunkte	12
JSON-Schema für Metadatenzuordnungen	12
Anzeigen der Metadatenzuordnungen	13
Hinzufügen oder Ändern von Metadatenzuordnungen	15
Anzeigen der benutzerdefinierten Metadatenzuordnungen	16
Konfigurieren der Scanplanung	17
Konfigurieren der Datenaufbewahrungs-Policy	19
Inaktive Agents managen	21
Integrieren von NetWitness Endpoint 4.4.0.2 oder höher in NetWitness Endpoint 11.1	23
Konfigurieren des Clientzertifikats auf dem NetWitness Endpoint 4.4.0.2-Konsolenserver (für Option 1)	23
Aktivieren der Weiterleitung von Metadaten in NetWitness Endpoint 4.4.0.2 (für Option 1)	27
Aktivieren der Weiterleitung der Metadaten von NetWitness Endpoint 4.4.0.2 zum Log Decoder (für Option 2)	27
Aktivieren von Rechnern zur Weiterleitung von Metadaten von NetWitness Endpoint 4.4.0.2 zum NetWitness Endpoint-Server (für Optionen 1 und 2)	27

Endpoint-Referenzen	30
Registerkarte „Allgemein“	31
Workflow	31
Was möchten Sie tun?	32
Überblick	32
Registerkarte „Datenaufbewahrungsplaner“	34
Workflow	34
Was möchten Sie tun?	34
Überblick	35
Registerkarte „Scanplanung“	38
Workflow	38
Was möchten Sie tun?	38
Überblick	39
Registerkarte „Packager“	40
Was möchten Sie tun?	40
Troubleshooting	41
Probleme bei der Kommunikation mit Agenten	41
Probleme mit dem Packager	42
Probleme mit der Scanplanung	42
Probleme mit Integrität und Zustand	43
Probleme mit der Metadatenkonfiguration	45
Installationsproblem	46
Probleme mit der Suche nach inaktiven Agenten	46

NetWitness Endpoint Insights – Übersicht

Hinweis: Die Informationen in diesem Leitfaden gelten für Version 11.1 und höher.

RSA NetWitness Endpoint sammelt Endpunktdaten von Windows-, Mac- oder Linux-Hosts, die für Untersuchungen, Berichte, Warnmeldungen und die Durchführung von Analysen verwendet werden können. Analysten können zu jedem beliebigen Point-in-Time sofortige Scans durchführen, um detaillierte Einblicke in das Hostverhalten zu erhalten. Darüber hinaus kann Endpoint Protokolle von Windows-Hosts erfassen. NetWitness Endpoint Insights führt mit Endpoint Hybrid und Endpoint Log Hybrid zwei neue Hosttypen ein. Sie können in Ihrer Bereitstellung nur eine Instanz des Hosttyps installieren. Das heißt, Sie können entweder eine Instanz von Endpoint Hybrid oder eine Instanz von Endpoint Log Hybrid bereitstellen. Nach der Bereitstellung können Sie den Typ nicht mehr ändern.

Endpoint Hybrid erfasst und managt Endpunktdaten (Hostdaten). Dieser Hosttyp erzeugt Metadaten für Untersuchungen, Analysen, Warnmeldungen und Berichte. Konfiguration und Management ähneln denen eines Log Decoders oder Packet Decoders. Auf dem Endpoint Hybrid-Host wird ein Nginx-Server ausgeführt (im Reverse-Proxy-Modus), der Daten von Endpoint Agent empfängt. Auf dem Endpoint Hybrid-Host werden folgende Services ausgeführt:

- Endpoint-Server: Managt über Nginx empfangene Daten, speichert sie in der MongoDB-Datenbank und sendet Metadaten an den Log Decoder.
- Log Decoder: Erfasst Daten vom Endpoint-Server und verarbeitet die Metadaten.
- Concentrator: Aggregiert Metadaten vom Log Decoder und stellt sie für alle Upstream-Komponenten wie Investigate, Reporting Engine und Event Stream Analysis zur Verfügung, ähnliche wie bei anderen NetWitness Decoder- und Concentrator-Einrichtungen.

Endpoint Log Hybrid erfasst sowohl Endpunkt- als auch Protokolldaten. Zusätzlich zu den auf dem Endpoint Hybrid-Host ausgeführten Services wird auf dem Endpoint Log Hybrid-Host ein Log Collector-Service ausgeführt. Er erfasst Protokolle von Windows-Hosts sowie von allen weiteren Ereignisquellen, die zur Protokollerfassung in der NetWitness Suite unterstützt werden.

Der *Leitfaden für die ersten Schritte mit Hosts und Services* enthält die nötigen Informationen, um die Services der NetWitness Suite zu verstehen und sie installieren zu können.

Die **Basiskonfiguration** umfasst Folgendes:

- Installieren von Agents auf Hosts
- Konfigurieren der Weiterleitung von Endpunktdaten, der Scanplanung und von Aufbewahrungs-Policies
- Definieren von Integritäts- und Zustands-Policies zur Überwachung des Endpoint-Servers

Sie können die erforderlichen Einstellungen über die Optionen der NetWitness Suite-Benutzeroberfläche unter **Administration > Services > Konfiguration** vornehmen.

The screenshot shows the NetWitness Suite Administration console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, and the 'Services' tab is selected. The left sidebar shows 'Groups' with 'All' selected. The main area displays a table of services with columns for Name, Licensed, Host, Type, Version, and Actions. The 'Endpoint Server' is selected, and its configuration options are visible in a dropdown menu.

Name	Licensed	Host	Type	Version	Actions
1760Node0 - Admin Server	✓	1760Node0	Admin Server	11.1.0.0	⚙️
1760Node0 - Broker	✓	1760Node0	Broker	11.1.0.0	⚙️
1760Node0 - Config Server	✓	1760Node0	Config Server	11.1.0.0	⚙️
1760Node0 - Investigate Server	✓	1760Node0	Investigate Server	11.1.0.0	⚙️
1760Node0 - Orchestration Server	✓	1760Node0	Orchestration Server	11.1.0.0	⚙️
1760Node0 - Reporting Engine	✓	1760Node0	Reporting Engine	11.1.0.0	⚙️
1760Node0 - Respond Server	○	1760Node0	Respond Server		⚙️
1760Node0 - Security Server	✓	1760Node0	Security Server	11.1.0.0	⚙️
1760NodeX - Concentrator	✓	1760NodeX	Concentrator	11.1.0.0	⚙️
1760NodeX - Endpoint Server	✓	1760NodeX	Endpoint Server	11.1.0.0	⚙️
1760NodeX - Log Decoder	✓	1760NodeX	Log Decoder	11.1.0.0	⚙️

Configuration options for the selected service (Endpoint Server):

- Config Explore
- View
- Delete
- Edit
- Start
- Stop
- Restart

Page 1 of 1 | Displaying 1 - 11 of 11

Endpoint-Serverkonfiguration

Dieses Thema enthält allgemeine, zur Konfiguration des Services „Endpoint-Server“ erforderliche Aufgaben.



Aufgaben	Beschreibung
Installieren von Endpoint Hybrid oder Endpoint Log Hybrid	<p>Siehe hierzu <i>Installationshandbuch für physische Hosts</i> und <i>Leitfaden zur Einrichtung von virtuellen Hosts</i>.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Hinweis: Registrieren Sie nach der Installation von Endpoint Hybrid oder Endpoint Log Hybrid die Host-IP-Adresse des Endpoint-Servers wie folgt mit dem NW-Server:</p> <ol style="list-style-type: none"> Stellen Sie über SSH eine Verbindung mit dem NW-Server her. Navigieren Sie zum Verzeichnis <code>/opt/rsa/saTools/bin</code>. <pre>cd /opt/rsa/saTools/bin</pre> Führen Sie das Skript <code>register-endpoint</code> aus, wobei Sie die Endpoint-Host-IP-Adresse angeben. <pre>./register-endpoint-ip -v --host-addr <ip-address></pre> <p>Es dauert einige Minuten, bis das Skript die Endpoint-Server-IP-Adresse aktualisiert.</p> </div>

Aufgaben	Beschreibung
Konfigurieren der Weiterleitung von Metadaten für Agents von NetWitness Endpoint 11.1	<p>Ähnlich wie in NetWitness Logs and Packets können Sie die Endpunktmetadaten in den Ansichten „Navigation“ und „Ereignisanalyse“ anzeigen. Sie können auch Berichte und Warnmeldungen für die Endpunktdaten erzeugen. Die Option „Endpunktmetadaten“ ist standardmäßig deaktiviert. Der Agent muss mit aktivierter Option „Endpunktmetadaten“ installiert sein, um Metadaten weiterleiten zu können.</p>
<p>Installieren von Agents auf Hosts</p>	<p>Das Endpoint Agent-Installationsprogramm wird auf der Registerkarte „Packager“ unter ADMIN > Services > Konfiguration > Endpoint-Server über die NetWitness Suite-Benutzeroberfläche erzeugt. Der Packager ist eine ZIP-Datei, die ausführbare und Konfigurationsdateien zum Erzeugen von Agent-Installationsprogrammen für die Betriebssysteme Linux, Mac und Windows enthält. Sie können auf einem Host nur eine Version des Agent installieren. Wenn eine frühere Version eines Agent installiert ist (z. B. 4.4), deinstallieren Sie diesen Agent, um die Version 11.1 des Agent zu installieren.</p> <p>Wenn der Agent installiert ist, wird er in der Ansicht Untersuchen > Hosts angezeigt. Standardmäßig werden zum ersten Mal die Endpunktdaten angezeigt. Um nachfolgende Endpunktdaten zu erfassen, müssen Sie entweder einen Scan planen oder einen Ad-Hoc-Scan durchführen. Ein Scan ruft Daten wie Treiber, Prozesse, DLLs, (ausführbare) Dateien, Services, automatische Ausführungen, Sicherheitsinformationen, Systemkonfigurationen und Skripte ab, die auf dem Host gefunden werden.</p> <p>Wenn der Agent für die Protokollsammlung konfiguriert ist, sammelt der der Scan Protokolle von Windows-Hosts und leitet sie an einen Log Decoder oder Remote Log Decoder weiter. Weitere Informationen zur Installation des Endpoint-Agent finden Sie im <i>Endpoint Insights Agent-Installationshandbuch</i>.</p>
<p>Untersuchen von Endpunktdaten</p>	<p>Sie können die Endpunktdaten in den Ansichten Untersuchen > Hosts und Untersuchen > Dateien untersuchen. Weitere Informationen finden Sie im <i>Leitfaden zu Investigate</i>.</p>
Konfigurieren der Scanplanung	<p>Planen Sie einen Scan so, dass er täglich oder wöchentlich ausgeführt wird.</p>


Aufgaben	Beschreibung
Konfigurieren der Datenaufbewahrungs-Policy	<p>Definieren Sie Datenaufbewahrungs-Policies, um die Endpunktdaten basierend auf ihrem Alter oder der Größe des Speichers optimal zu speichern und zu managen.</p> <p>Standardmäßig werden die Agent-Daten von 30 Tagen aufbewahrt.</p>
Inaktive Agents managen	<p>Standardmäßig werden Agents (einschließlich aller erfassten Endpunktdaten), die seit 90 Tagen nicht mehr mit dem Endpoint-Server kommuniziert haben, automatisch gelöscht.</p>

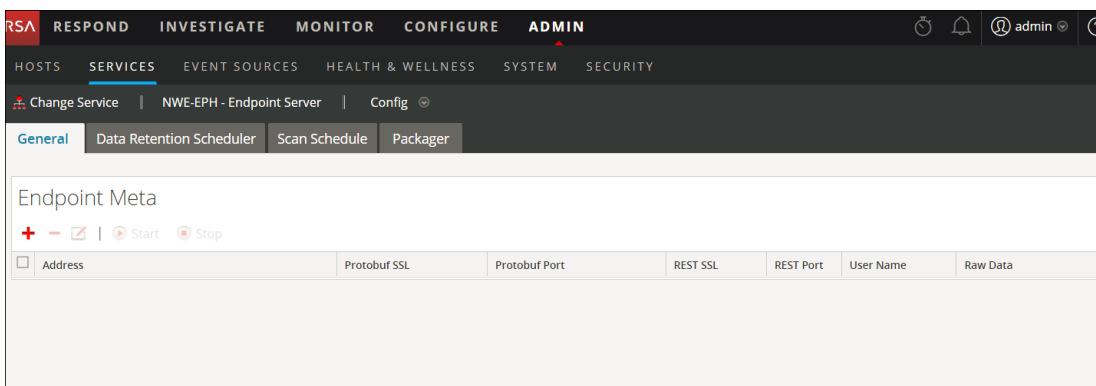
Konfigurieren der Weiterleitung von Metadaten für Agents von NetWitness Endpoint 11.1

Sie können die Endpunktmeterdaten in NetWitness Investigate (Ansichten **Navigation** und **Ereignisanalyse**) anzeigen, ähnlich wie in NetWitness Logs and Packets. Sie müssen die Weiterleitung für Metadaten aktivieren, um die folgenden Kategorien weiterleiten zu können:

Betriebssystem	Kategorien
Windows	Datei, Service, DLL, Prozess, Aufgabe, Autorun und Rechner
Linux	Datei, geladene Bibliothek, Systemd, Prozess, Cron, Initd und Rechner
Mac	Datei, Daemon, Prozess, Aufgabe, Dylib, Autorun und Rechner

Konfigurieren der Weiterleitung von Metadaten

1. Navigieren Sie zu **ADMIN > Services**.
2. Wählen Sie in der Ansicht „Services“ den Service **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Allgemein**.



5. Klicken Sie in der Symbolleiste auf **+**.
Das Dialogfeld „Verfügbare Services“ wird angezeigt.
6. Wählen Sie den Log Decoder-Service aus und klicken Sie auf **OK**.
Das Dialogfeld „Service hinzufügen“ wird angezeigt. Sie können nur einen Log Decoder-Service hinzufügen.

Add Service

Please provide administrator credentials for the service:

Username

Password

Raw Data

REST SSL ⓘ

REST Port

Protobuf SSL ⓘ

Protobuf Port


Cancel **Save**

7. Geben Sie die Administratoranmeldedaten für die Authentifizierung ein.
8. (Optional) Wenn Sie die Option „Rohdaten“ aktivieren, wird eine kurze Zusammenfassung der Sitzung zusammen mit den Metadaten gesendet.
9. (Optional) Wenn Sie in Log Decoder SSL auf dem REST-Port aktiviert haben, wählen Sie die Option **REST-SSL** aus. Standardmäßig sind die REST-Ports für Nicht-SSL 50202 und für SSL 56202.
10. Wählen Sie die Option **Protobuf-SSL** aus, um SSL auf Protobuf zu aktivieren. Standardmäßig ist der Protobuf-Port 50202.
11. Klicken Sie auf **Speichern**.


Führen Sie nach dem Konfigurieren der Weiterleitung von Metadaten folgende Aktionen durch:

- Starten Sie die Erfassung auf dem Log Decoder.
- Starten Sie die Aggregation auf dem Concentrator.
- Fügen Sie den Log Decoder als Service im **Concentrator** hinzu.

Starten der Weiterleitung von Metadaten zum Log Decoder


1. Wählen Sie in der Konfigurationsansicht „Endpointmetadaten“ den Service aus.
2. Klicken Sie auf  **Start**.
Der Endpoint-Server leitet die Metadaten zum Log Decoder.

Beenden der Weiterleitung von Metadaten zum Log Decoder

1. Wählen Sie in der Konfigurationsansicht „Endpunktmetadaten“ den Service aus.
2. Klicken Sie auf  **Stop** .
Der Endpoint-Server beendet die Weiterleitung der Metadaten zum Log Decoder.

Entfernen der Weiterleitung von Metadaten

Hinweis: Stellen Sie sicher, dass Sie den Service beenden, bevor Sie die Weiterleitung von Metadaten entfernen.

1. Wählen Sie in der Konfigurationsansicht „Endpunktmetadaten“ den Service aus.
2. Klicken Sie auf  .
3. Klicken Sie auf **Anwenden**.

Metadatenzuordnungen für Endpunkte

Sie können die Standard-Metadatenzuordnungen anzeigen oder die Metadatenzuordnungen für Endpunkte ändern.

JSON-Schema für Metadatenzuordnungen

Alle Metadatenzuordnungen werden mit dem JSON-Schema konfiguriert. Hier ist ein Beispiele für ein JSON-Schema:

```
{
  "metaKeyPairs" : [
    {
      "metaKeyPairsCategory" : "",
      "keyPairs" : [
        {
          "endpointJpath" : "",
          "metaName" : "",
          "type" : "",
          "enabled" : true
        },
        {
```

```
        "endpointJpath" : "",
        "metaName" : "",
        "type" : "",
        "enabled" : true
    }
}
]
```

Die folgenden APIs werden verwendet, um die Metadatenzuordnungen anzuzeigen oder zu ändern:

- `get-default`: Gibt die Standardkonfigurationen für die Metadatenzuordnungen des Endpunkts zurück.
- `get-custom`: Gibt die benutzerdefinierten Konfigurationen für die Metadatenzuordnungen des Endpunkts zurück.
- `set-custom`: Sie können die Metadatenzuordnungen des Endpunkts anpassen.

Anzeigen der Metadatenzuordnungen

So zeigen Sie die Metadatenzuordnungen des Endpunkts an:

1. Führen Sie auf dem NW-Server über die Befehlszeile den Befehl `nw-shell` aus.
2. Führen Sie den Befehl `login` aus und geben Sie die Anmeldedaten ein.
3. Stellen Sie mit folgendem Befehl eine Verbindung zum Endpoint-Server her:
`connect --host <IP address> --port <number>`

Hinweis: Der Standardport ist 7050.

4. Führen Sie folgende Befehle aus:
`cd endpoint/meta`
`cd get-default`
`invoke`

Der folgende Bildschirm zeigt die Standard-Metadatenzuordnungen an:

```

    {
      "endpointJpath" : "users/sessionType",
      "metaName" : "logon_type",
      "type" : "text",
      "enabled" : true
    },
    {
      "endpointJpath" : "hostFileEntries/hosts",
      "metaName" : "dhost",
      "type" : "text",
      "enabled" : true
    },
    {
      "endpointJpath" : "securityConfigurations",
      "metaName" : "event_state",
      "type" : "text",
      "enabled" : true
    }
  ]
},
{
  "metaKeyPairsCategory" : "MACHINE_IDENTITY",
  "keyPairs" : [
    {
      "endpointJpath" : "_id",
      "metaName" : "agent.id",
      "type" : "text",
      "enabled" : true
    }
  ],
}

```

So deaktivieren Sie eine Standard-Metadatenzuordnung:

Geben Sie für „endpointJpath“ denselben Wert ein und legen Sie den Parameter „enabled“ auf false fest.

Beispiel: Wenn der Wert für „endpointJpath“ `Category` ist und der Parameter „enabled“ auf true festgelegt ist, geben Sie für „endpointJpath“ denselben Wert ein und legen Sie den Parameter „enabled“ auf false fest.

```

{
  "metaKeyPairsCategory" : "COMMON",
  "keyPairs" : [
    {
      "endpointJpath" : "Category",
      "metaName" : "category",
      "type" : "text",
      "enabled" : true
    }
  ],
}

```

Hinweis: Ändern Sie im Schema nicht den Wert für „metaKeyPairsCategory“: „COMMON“, „COMMON_MACHINE“, „COMMON_MACHINE_FOR_EVENTS“.

So ändern Sie den Metanamen oder den Metatyp:

Geben Sie für „endpointJpath“ denselben Wert ein und geben Sie für „metaName“ und „type“ Werte ein.

Hinweis: Der Wert von „metaName“ muss in der Datei „table-map.xml“ des Log Decoder, in der Datei „index-concentrator.xml“ oder in der Datei „index-concentrator-custom.xml“ des Concentrator vorhanden sein, damit der Wert von „metaName“ in der Ansicht „Untersuchen“ angezeigt wird.

Hinzufügen oder Ändern von Metadatenzuordnungen

Führen Sie zum Hinzufügen oder Ändern der Metadatenzuordnungen die API `set-custom` aus. Die `metaKeyPairs`-Konfiguration in der JSON-Datei sollte dem JSON-Schema der über die API `get-default` empfangenen Standardkonfiguration entsprechen.

1. Führen Sie auf dem NW-Server über die Befehlszeile den Befehl `nw-shell` aus.
2. Führen Sie den Befehl `login` aus und geben Sie die Anmeldedaten ein.
3. Stellen Sie mit folgenden Befehlen eine Verbindung zum Endpoint-Server her:
`connect --host <IP address> --port <number>`

Hinweis: Die Standardportnummer ist 7050)

4. Führen Sie folgende Befehle aus:

```
cd endpoint/meta
cd set-custom
invoke -file <json file>
```

Sie können neue `metaKeys` hinzufügen, indem Sie der Datei, die hochgeladen wird, mit der API `set-custom` Einträge hinzufügen. Das folgende Beispiel zeigt, wie Sie eine neue Metadatenzuordnung hinzufügen:

```
[root@NODE0-1982-SIGNED ~]# nw-shell
RSA NetWitness Shell. Version: 2.9.2
See "help" to list available commands, "help connect" to get started.
offline » login
user: admin
password: *****
admin@offline » connect --host [REDACTED] --port 7050
Connected to endpoint-server ([REDACTED])
admin@Folder:/rsa » cd endpoint/meta/set-custom
admin@Method:/rsa/endpoint/meta/set-custom » invoke --file /custom.json
admin@Method:/rsa/endpoint/meta/set-custom » cd ../get-custom
admin@Method:/rsa/endpoint/meta/get-custom » invoke
{
  "metaKeyPairs" : [
    {
      "metaKeyPairsCategory" : "NETWORK",
      "keyPairs" : [
        {
          "endpointJpath" : "file/checksumSha1",
          "metaName" : "checksum",
          "type" : "text",
          "enabled" : true
        }
      ]
    }
  ]
}
admin@Method:/rsa/endpoint/meta/get-custom » █
```

Anzeigen der benutzerdefinierten Metadatenzuordnungen

Um die benutzerdefinierten Metadatenzuordnungen anzuzeigen, führen Sie die API `get-custom` aus.


Hinweis: Die API `get-custom` gibt nur dann Werte zurück, wenn die Metadatenzuordnungen mit der API `set-custom` geändert wurden.

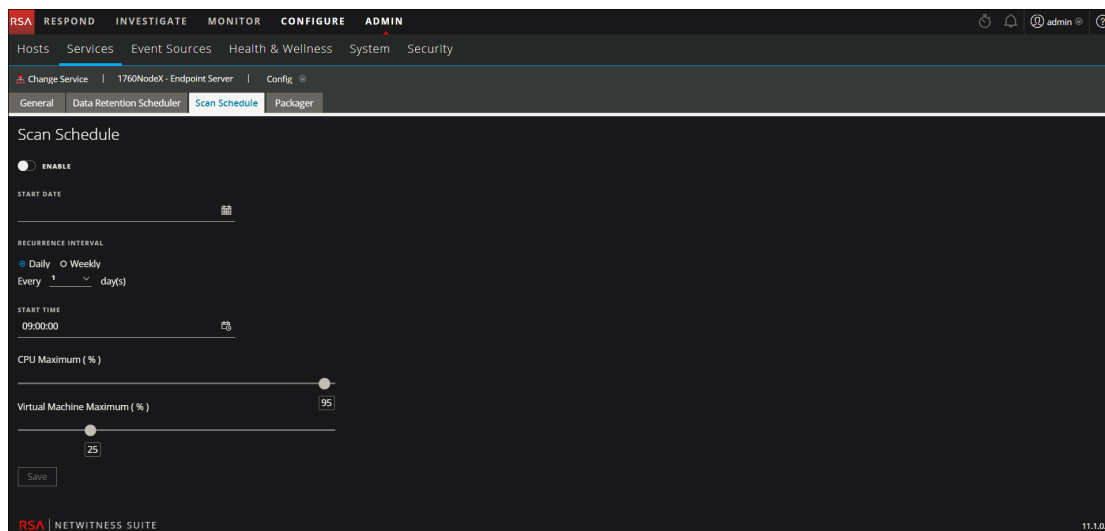
Konfigurieren der Scanplanung

Sie können einen Scan so planen, dass er täglich oder wöchentlich ausgeführt wird.

Hinweis: Sie können nur einen Plan konfigurieren, der dann für alle Agents gilt.

So konfigurieren Sie eine Scanplanung:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht „Services“ den Service **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Scanplanung**.



5. Klicken Sie auf den Umschalter **Aktivieren**, um zur Skanconfiguration umzuschalten.
6. Wählen Sie das **Startdatum** aus.
7. Wählen Sie das Wiederholungsintervall aus („Täglich“ oder „Wöchentlich“).

Hinweis: Die eingegebenen Werte beziehen sich auf die Zeitzone des Agent.

8. Für einen täglichen Scan:
 - Wählen Sie für das Wiederholungsintervall **Täglich** aus.
 - Geben Sie die Häufigkeit des Scans in Tagen ein.

9. Für einen wöchentlichen Scan:
 - Wählen Sie für das Wiederholungsintervall **Wöchentlich** aus.
 - Geben Sie die Häufigkeit des Scans in Wochen ein.
 - Wählen Sie den Wochentag aus.
10. Geben Sie die Startzeit des Scans ein.
11. Legen Sie mit dem Schieberegler den Wert für „Maximalleistung CPU (%)“ fest. Dadurch wird der CPU-Grenzwert für den Agent von NetWitness Endpoint sichergestellt. Wenn die Agents auf den virtuellen Maschinen ausgeführt werden, legen Sie mit dem Schieberegler den Wert für „Maximalleistung virtuelle Maschine (%)“ fest.
12. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Hinweis: Falls ein Agent den Scan zur geplanten Zeit nicht durchführen kann, weil der Rechner ausgeschaltet ist oder der Agent-Service angehalten wurde, basiert der nächste Scan auf dem Zeitunterschied zwischen dem aktuellen Zeitpunkt und dem Zeitpunkt des nächsten geplanten Scans.


Beispiel: Jeden Mittwoch um 18:00 Uhr soll ein Scan durchgeführt werden. Der Agent-Service wurde jedoch vor der Startzeit des Scans angehalten. Wenn der Service am Donnerstag um 10:00 Uhr wieder ausgeführt wird, führt der Agent umgehend einen Scan durch, sobald das System vollständig betriebsbereit ist.

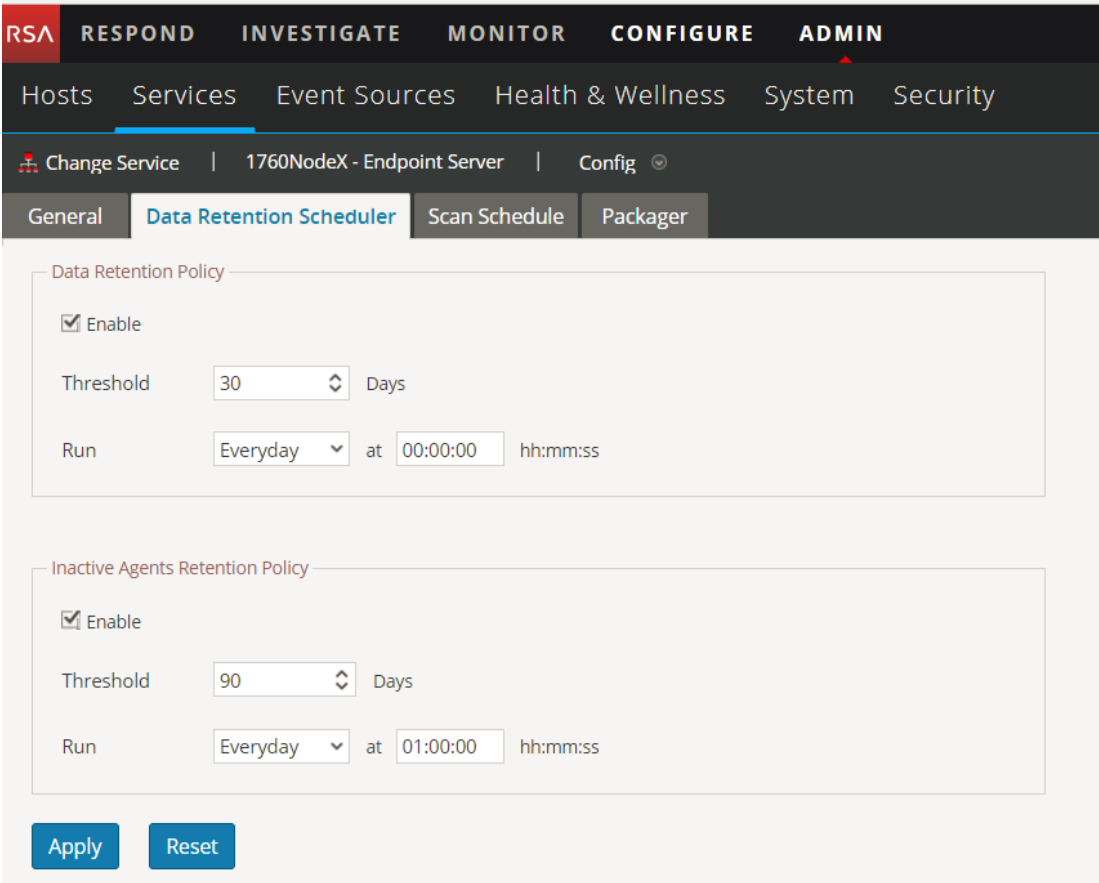
Wird der Service jedoch erst am darauffolgenden Montag um 13:00 Uhr wieder ausgeführt, wird der Scan am kommenden Mittwoch um 18:00 Uhr durchgeführt.

Konfigurieren der Datenaufbewahrungs-Policy

Ein Administrator kann die Aufbewahrungs-Policies so konfigurieren, dass die Endpunktdaten basierend auf dem Alter oder Größe des Speichers aufbewahrt werden. Standardmäßig sind Tage und größenbasierte Aufbewahrungs-Policies aktiviert.

So ändern Sie die Konfiguration für eine altersbasierte Aufbewahrung:

1. Navigieren Sie zu **Admin > Services**.
2. Wählen Sie in der Ansicht „Services“ den Service **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Datenaufbewahrungsplaner**.




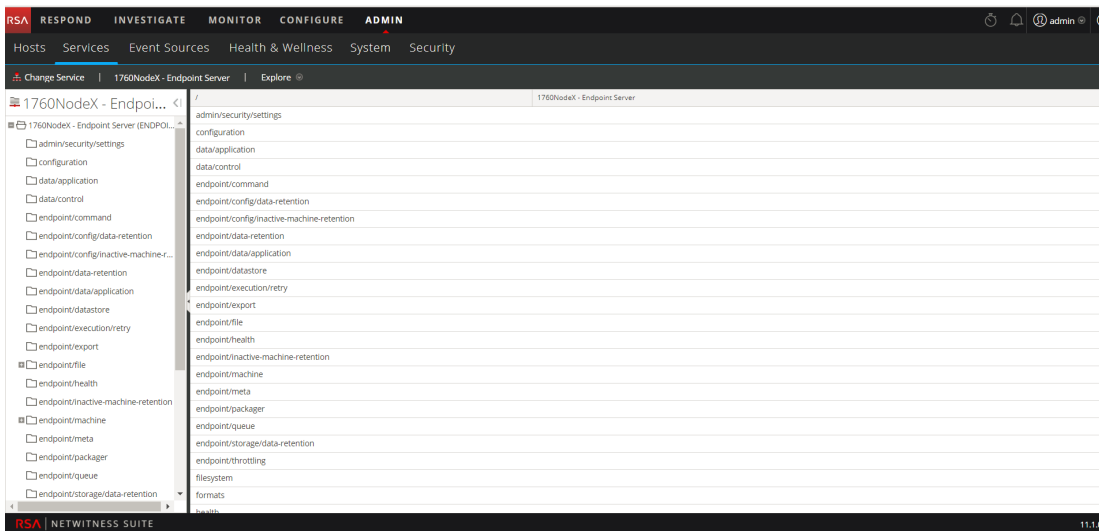
The screenshot shows the RSA Endpoint Insights configuration interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The current view is for the '1760NodeX - Endpoint Server' configuration. The 'Data Retention Scheduler' tab is selected, showing two sections: 'Data Retention Policy' and 'Inactive Agents Retention Policy'. Both sections have an 'Enable' checkbox checked, a 'Threshold' field set to 30 Days, and a 'Run' field set to 'Everyday' at '00:00:00' hh:mm:ss. At the bottom, there are 'Apply' and 'Reset' buttons.

5. Im Bereich **Datenaufbewahrungs-Policy** ist für **Schwellenwert** standardmäßig 30 Tage festgelegt und „Täglich“ für **Ausführen**. Das bedeutet, dass nur Endpunktdaten für 30 Tage aufbewahrt und die älteren Daten aus der Datenbank gelöscht werden.
6. Klicken Sie auf **Anwenden**.

So ändern Sie die Konfiguration für eine größenbasierte Aufbewahrung:

Für die größenbasierte Aufbewahrung ist der `rollover-after`-Wert standardmäßig auf 80 und `rollover-chunk-size` auf 10 festgelegt. Das bedeutet Folgendes: Wenn die Speichergröße 80 Prozent des für die Datenträgerpartition zugewiesenen Speicherplatzes überschreiten, werden 10 Prozent der älteren Endpunktdaten aus der Datenbank gelöscht. Sie können diese Werte jedoch wie folgt ändern:

1. Navigieren Sie im Hauptmenü zu **Admin > Services**.
2. Wählen Sie in der Ansicht „Services“ den Service **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Durchsuchen** aus. Die Ansicht „Durchsuchen“ wird angezeigt.




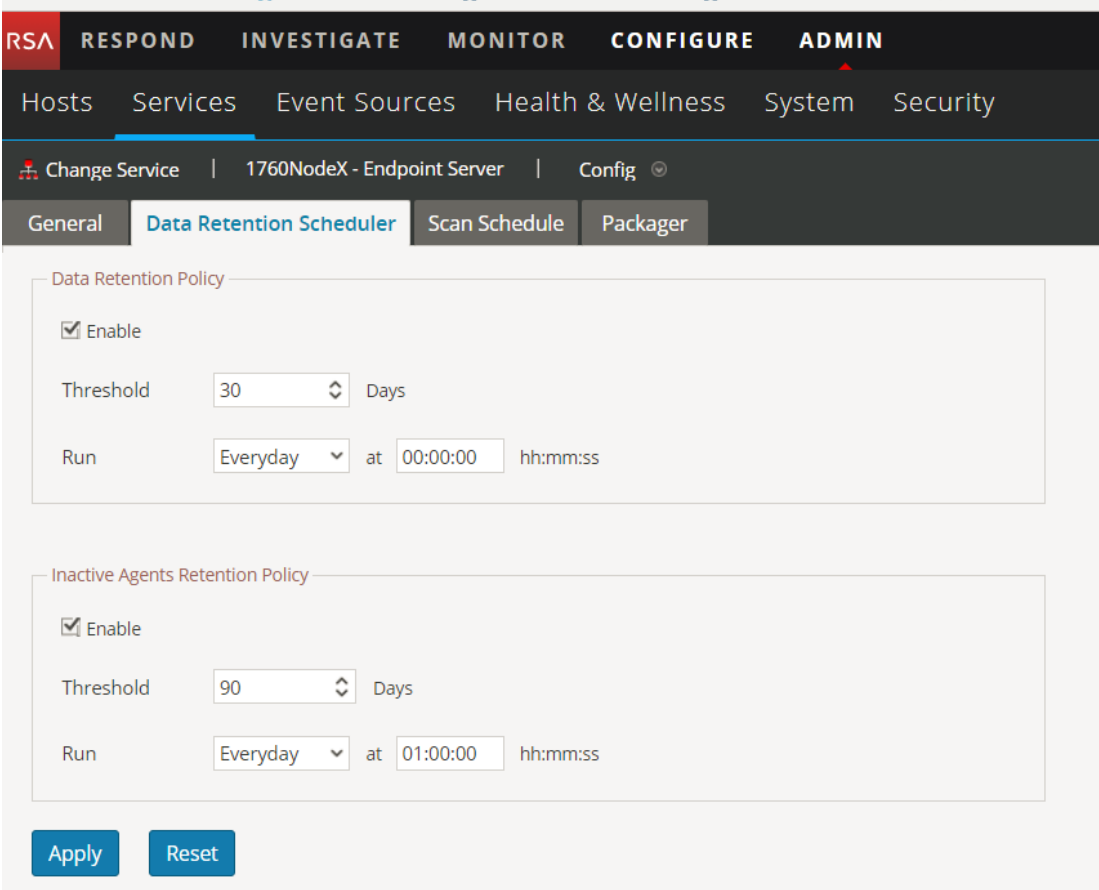
4. Wählen Sie im linken Bereich **endpoint/config/data-retention** aus.
5. Bearbeiten Sie die Konfigurationen basierend auf Ihren Anforderungen.

Inaktive Agents managen

Ein Administrator kann die Aufbewahrungs-Policy für inaktive Agents so konfigurieren, dass die Daten von inaktiven Agents vom Endpoint-Server gelöscht werden. Durch das Löschen erfasst der Endpoint-Server keine Daten mehr von diesen Agents. Diese Option ist standardmäßig aktiviert.

So konfigurieren Sie die Aufbewahrungs-Policy für inaktive Agents:

1. Navigieren Sie zu **Administration** > **Services**.
2. Wählen Sie in der Ansicht „Services“ die Option **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie > **Ansicht** > **Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Datenaufbewahrungsplaner**.



The screenshot shows the RSA Endpoint Insights configuration interface. The top navigation bar includes RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The current view is for the '1760NodeX - Endpoint Server' configuration, with a 'Config' dropdown menu. The 'Data Retention Scheduler' tab is selected, showing two policy sections: 'Data Retention Policy' and 'Inactive Agents Retention Policy'. Both sections have an 'Enable' checkbox checked, a 'Threshold' field (30 days for Data Retention, 90 days for Inactive Agents), and a 'Run' field (Everyday at 00:00:00 for Data Retention, Everyday at 01:00:00 for Inactive Agents). At the bottom, there are 'Apply' and 'Reset' buttons.

5. Im Bereich **Aufbewahrungsrichtlinie für inaktive Agents** ist für **Schwellenwert** standardmäßig 90 Tage festgelegt und „Täglich“ für **Ausführen**. Das bedeutet, dass die Daten von Agents, die sein 90 Tagen nicht mehr mit dem Endpoint-Server kommuniziert

haben, aus der Datenbank gelöscht werden.

6. Klicken Sie auf **Anwenden**.

Hinweis: Die Aufbewahrungsrichtlinie für inaktive Agents gilt nicht für Agents der Version NetWitness Endpoint 4.4.0.2 oder höher.

Integrieren von NetWitness Endpoint 4.4.0.2 oder höher in NetWitness Endpoint 11.1

Sie können die Endpunktmetadaten für NetWitness Endpoint 4.4.0.2 auf eine der folgenden Arten konfigurieren:

- **(Option 1) Integrieren Sie den NetWitness Endpoint 4.4.0.2-Konsolenserver in einen Endpoint Hybrid- oder Endpoint Log Hybrid-Host.** Die Daten der Agents von NetWitness Endpoint 4.4.0.2 oder höher stehen in den Ansichten **Untersuchen > Hosts** sowie **Dateien** zur Verfügung. Die Endpunktmetadaten können Sie in den Ansichten **Untersuchen > Navigation** und **Ereignisanalyse** anzeigen. Stellen Sie für diese Option sicher, dass der Endpoint-Server für die Weiterleitung von Metadaten konfiguriert ist.
- **(Option 2) Integrieren den Service „Meta Integrator“ in NetWitness Endpoint 4.4.0.2 direkt in einen Log Decoder.** Sie können die Endpunktmetadaten in den Ansichten **Untersuchen > Navigation** und **Ereignisanalyse** anzeigen. Die Daten der Agents von NetWitness Endpoint 4.4 sind in den Ansichten **Untersuchen > Hosts** sowie **Dateien** nicht verfügbar.

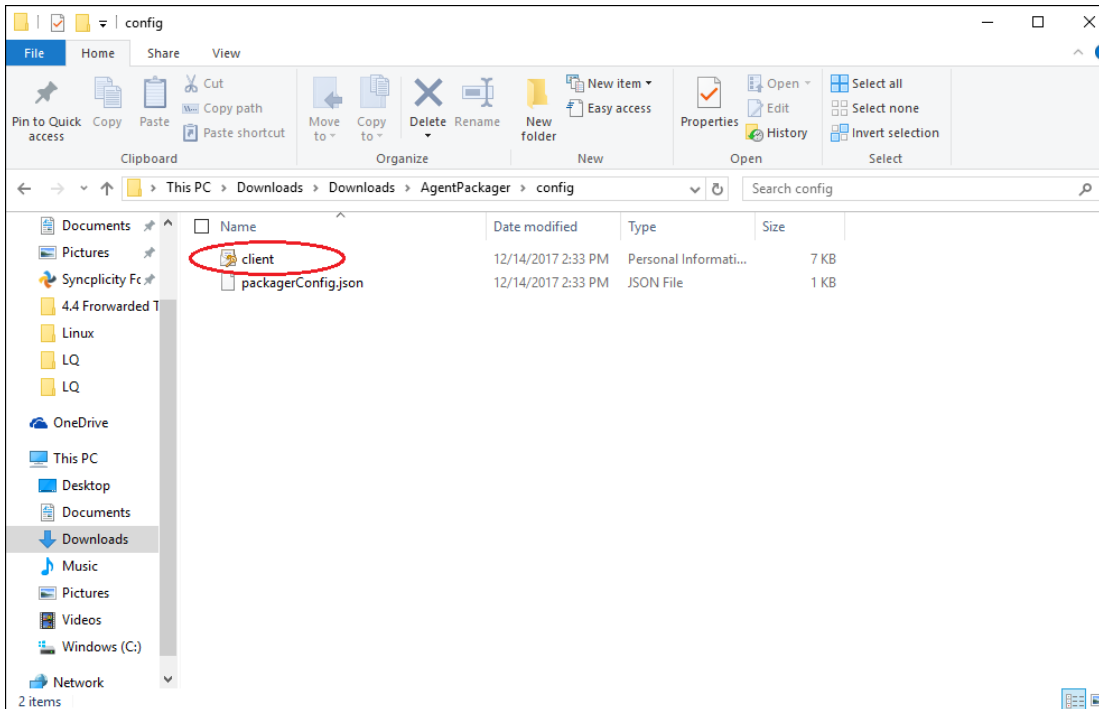
Zusätzlich zu den für die Agents von NetWitness Endpoint 11.1 genannten Kategorien werden für die Agents von NetWitness Endpoint 4.4.0.2 oder höher auch die folgenden Kategorien weitergeleitet: Datei-, Netzwerk-, Registrierungs- und Prozessereignis.

Konfigurieren des NetWitness Endpoint 4.4.0.2-Konsolenservers

Konfigurieren des Clientzertifikats auf dem NetWitness Endpoint 4.4.0.2-Konsolenserver (für Option 1)

Der NetWitness Endpoint 4.4.0.2-Konsolenserver muss dasselbe Clientzertifikat verwenden, das auch die Agents von NetWitness Endpoint 11.1 verwenden, um die Metadaten an den Endpoint-Server weiterzuleiten.

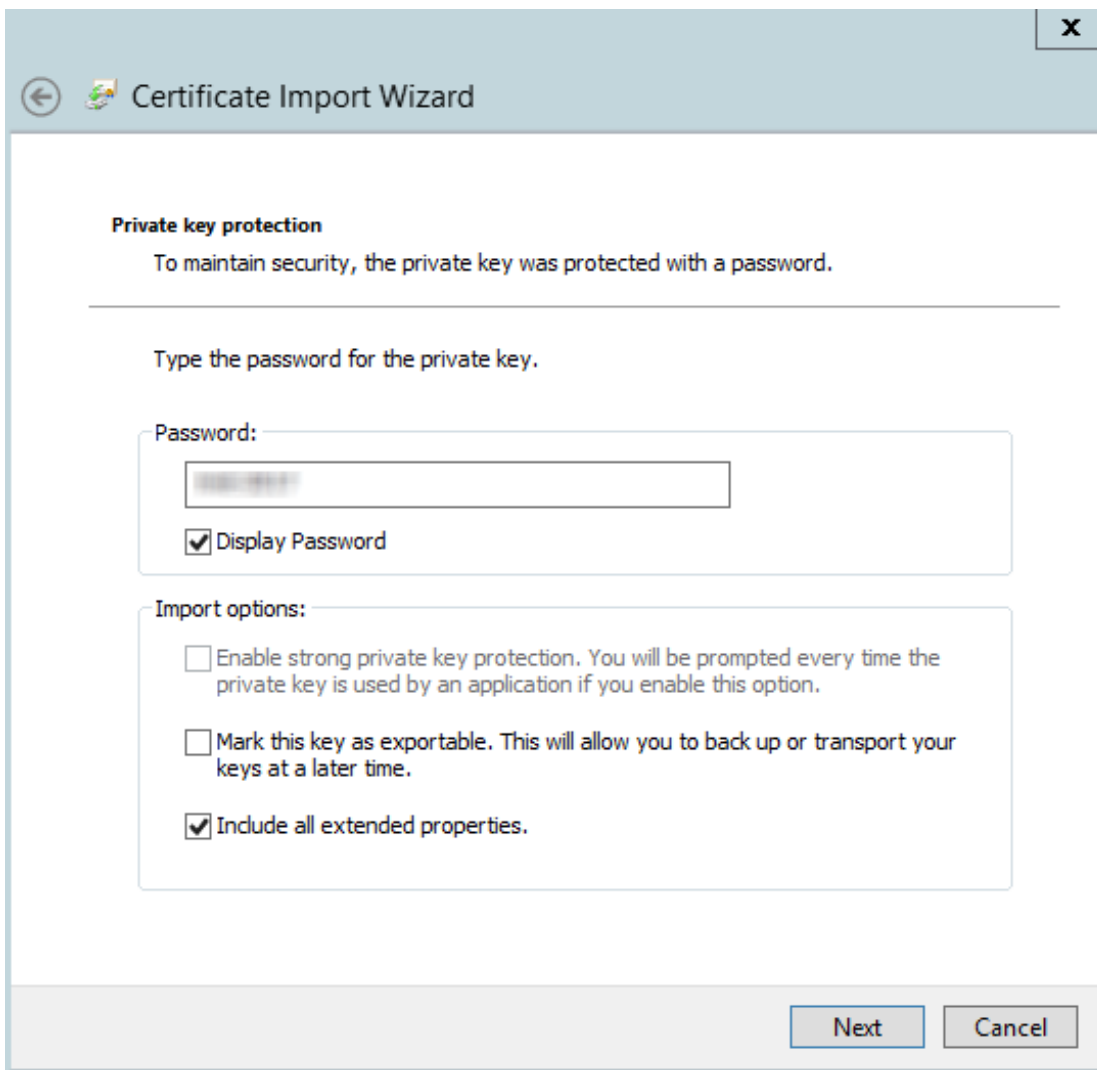
1. Laden Sie den Agent-Packager herunter. Weitere Informationen finden Sie im *Endpoint Insights Agent-Installationshandbuch*.
2. Extrahieren Sie die Datei **AgentPackager.zip** und beziehen Sie aus dem Ordner „Config“ das Clientzertifikat.
3. Kopieren Sie das Clientzertifikat auf den NetWitness Endpoint 4.4-Konsolenserver.



4. Doppelklicken Sie auf die Datei **client**.
Das Dialogfeld **Certificate Import Wizard** wird angezeigt.
5. Wählen Sie als Speicherort **Lokaler Rechner** aus und klicken Sie auf **Weiter**.

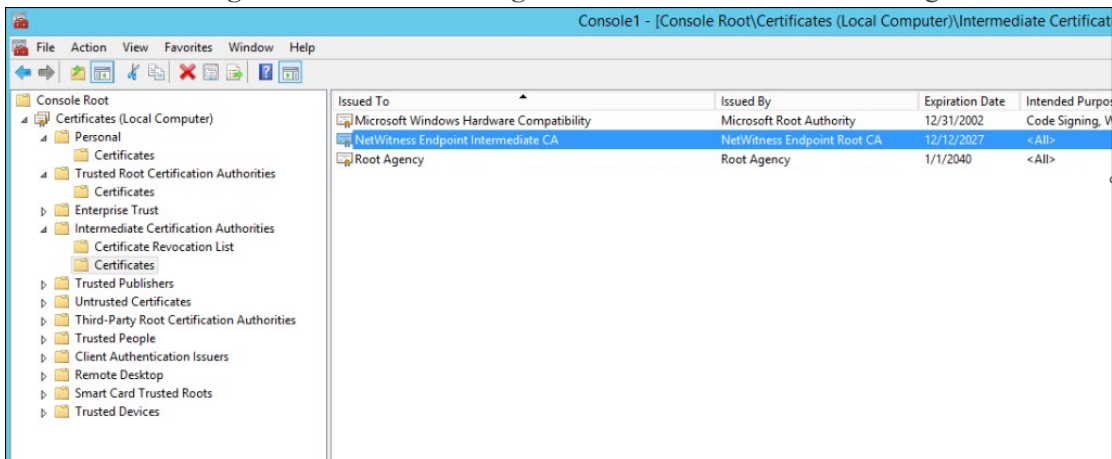


- Suchen Sie die Datei, die Sie importieren möchten, und klicken Sie auf **Weiter**.
- Geben Sie das gleiche Passwort ein, das Sie beim Erzeugen des Agent-Packager verwendet haben.



8. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

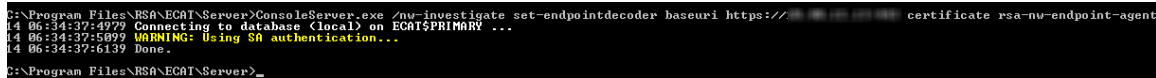
Das Zertifikat wird unter **Persönlich, Zwischenzertifizierungsstelle > Zertifikat und Vertrauenswürdige Stammzertifizierungsstellen** auf dem Konsolenserver gelistet.



Aktivieren der Weiterleitung von Metadaten in NetWitness Endpoint 4.4.0.2 (für Option 1)

Um die Weiterleitung von Metadaten für die ausgewählten Agents von NetWitness Endpoint 4.4.0.2 zu aktivieren, führen Sie den folgenden Befehl aus:

```
ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT HOST> certificate <CERTIFICATE DISPLAY NAME>.
```



```
C:\Program Files\RSA\ECAT\Server>ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://... certificate rsa-nw-endpoint-agent
14 06:34:37:4979 Connecting to database <local> on ECAT$PRIMARY ...
14 06:34:37:5099 WARNING: Using SA authentication...
14 06:34:37:6139 Done.
C:\Program Files\RSA\ECAT\Server>
```

Beispiel: ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://<Ip Address>:443 certificate rsa-nw-endpoint-agent

Aktivieren der Weiterleitung der Metadaten von NetWitness Endpoint 4.4.0.2 zum Log Decoder (für Option 2)

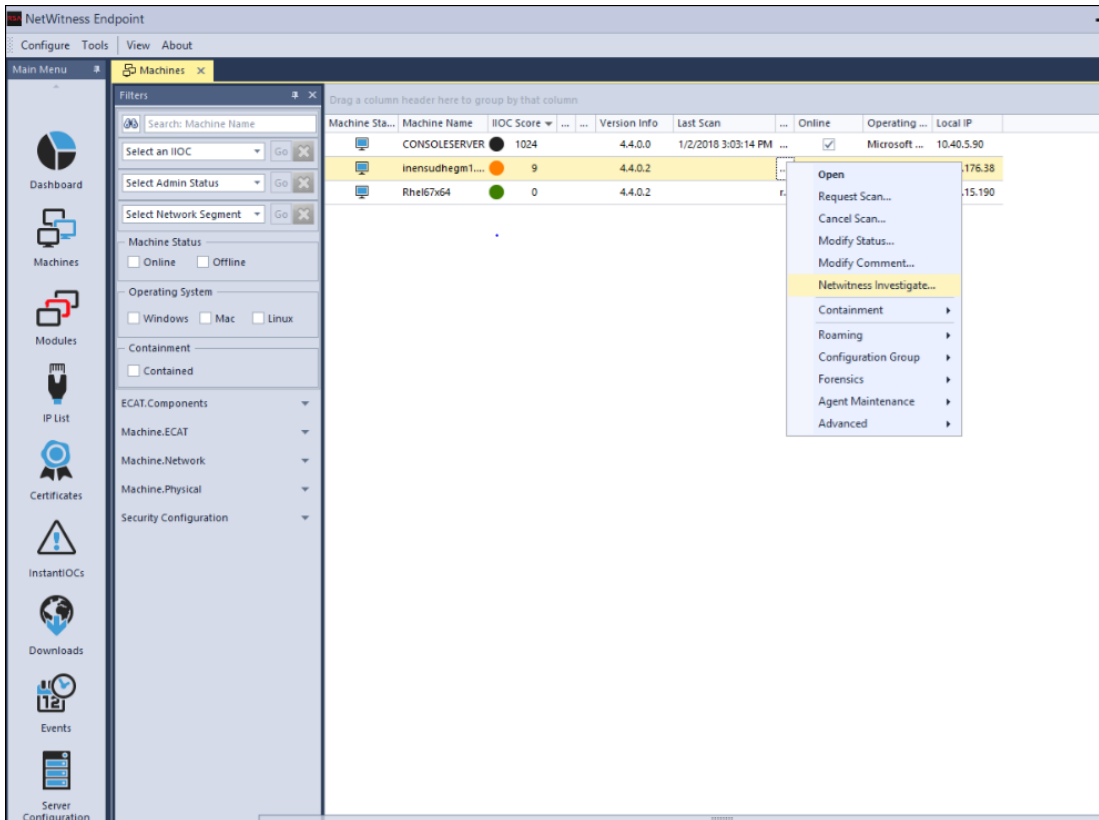
Um den Service „Metadata Integrator“ für die ausgewählten Agents von NetWitness Endpoint 4.4.0.2 zu aktivieren, führen Sie den folgenden Befehl aus:

```
ConsoleServer.exe /nw-investigate enable.
```

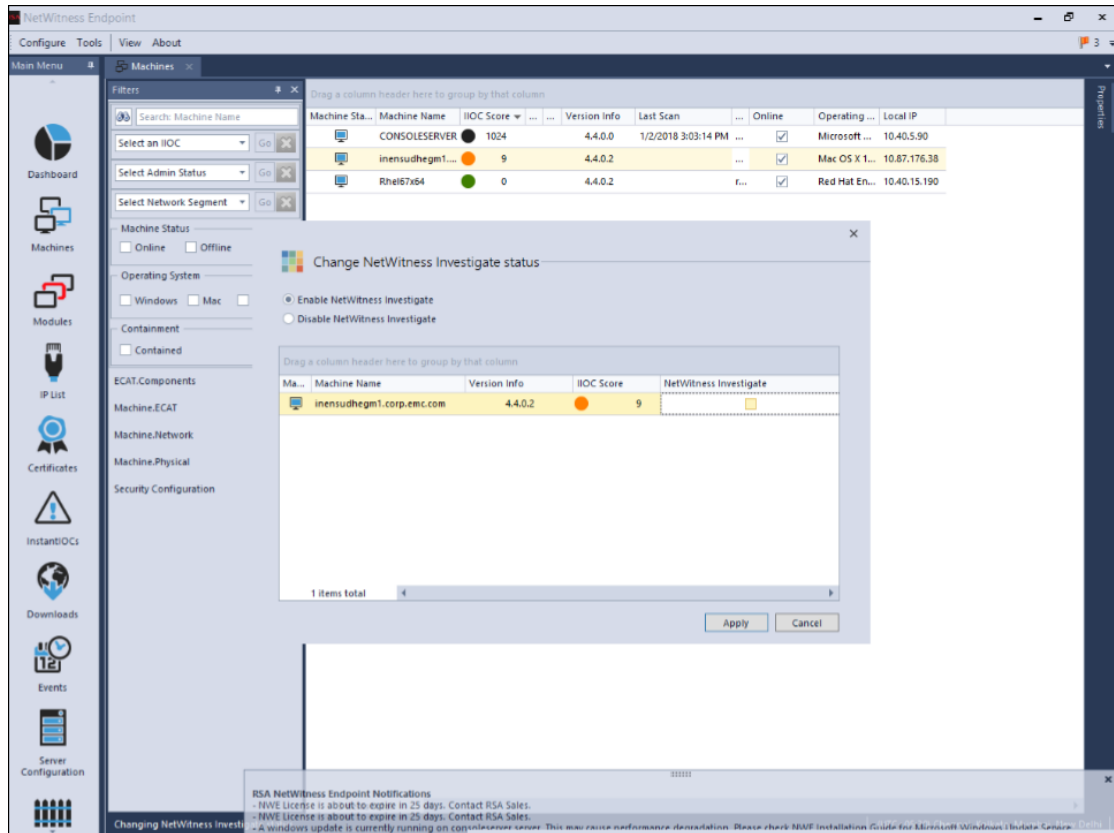
Aktivieren von Rechnern zur Weiterleitung von Metadaten von NetWitness Endpoint 4.4.0.2 zum NetWitness Endpoint-Server (für Optionen 1 und 2)

Nachdem Sie eine der oben genannten Optionen verwendet haben, um die Weiterleitung von Metadaten zu aktivieren, gehen Sie folgendermaßen vor, um die Rechner zur Weiterleitung von Metadaten zu aktivieren.

1. Öffnen Sie die Benutzeroberfläche von NetWitness Endpoint 4.4.0.2.
2. Klicken Sie im linken Bereich auf **Rechner**. Die Liste der verfügbaren Rechner werden angezeigt.



3. Wählen Sie die Rechner aus, für die Sie Metadaten zum NetWitness Endpoint-Server weiterleiten möchten.
4. Klicken Sie mit der rechten Maustaste und wählen Sie die Option **NetWitness Investigate** aus.
Das Dialogfeld „Status von NetWitness Investigate ändern“ wird angezeigt.



5. Wählen Sie die Option **NetWitness Investigate aktivieren** aus.
6. Klicken Sie auf **Anwenden**.
7. Um zu überprüfen, ob die Option **NetWitness Investigate aktivieren** aktiviert ist, wiederholen Sie Schritt 4.


Endpoint-Referenzen

Dieser Abschnitt soll Ihnen helfen, den Zweck der Ansicht „Services-Konfiguration“ für den Endpoint-Server zu verstehen. Für jede Konfiguration gibt es eine kurze Einführung und eine Tabelle zu „Was möchten Sie tun?“ mit Links zu verwandten Verfahren. Außerdem enthält er Workflows und Übersichten zur Hervorhebung wichtiger Funktionen in der Benutzeroberfläche.

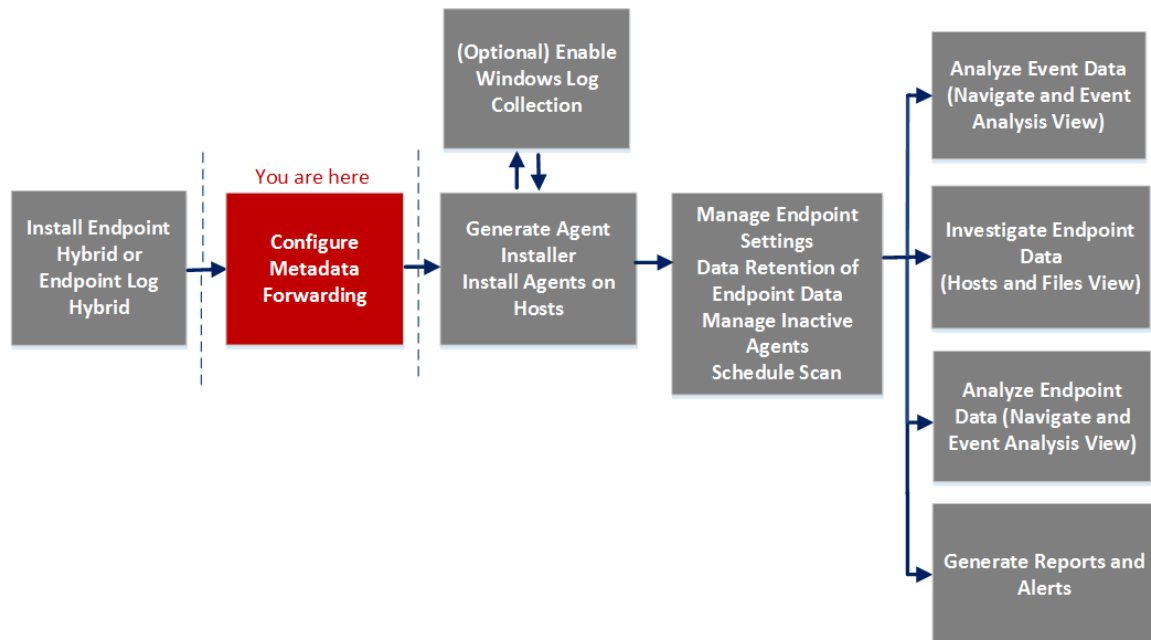
Sie können die vollständigen Service-Nodes in einer Baumstruktur in der Ansicht „Durchsuchen“ zu einem Service anzeigen. Weitere Informationen finden Sie im Thema „Ansicht „Durchsuchen“ für einen Service“ im *Leitfaden für die ersten Schritte mit Hosts und Services*.

Registerkarte „Allgemein“

Auf der Registerkarte **Allgemein** können Sie die Weiterleitung der Endpunkt-Metadaten konfigurieren. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht „Services“ die Option **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Allgemein**.

Workflow



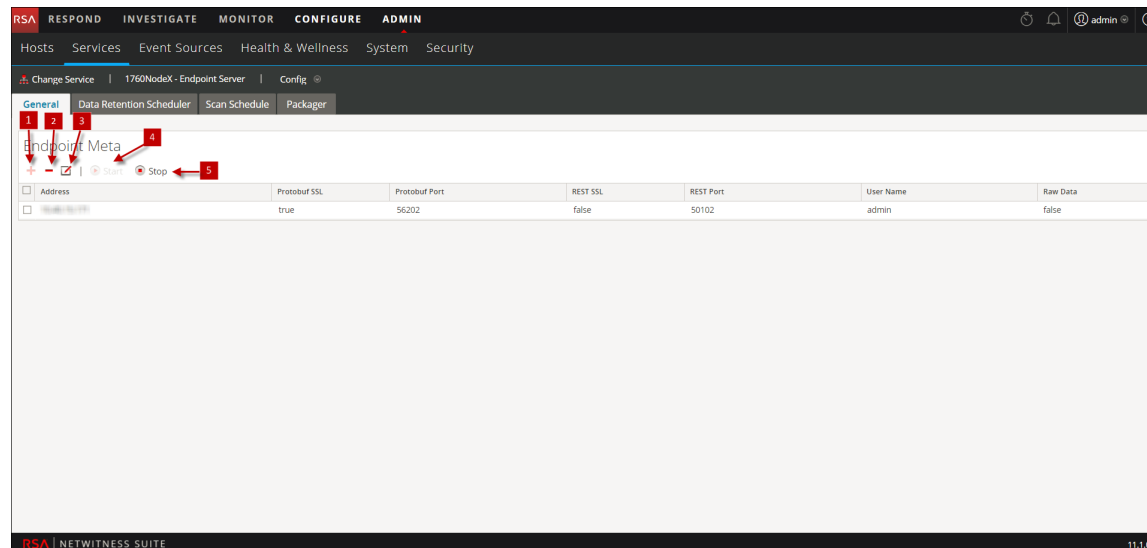
Was möchten Sie tun?

Rolle	Ziel	Anleitung
Administrator	Konfigurieren der Weiterleitung von Endpunkt-Metadaten für Agents von NetWitness Endpoint 11.1	Konfigurieren der Weiterleitung von Metadaten
Administrator	Konfigurieren der Weiterleitung von Endpunkt-Metadaten für Agents von NetWitness Endpoint 4.4.0.2 oder höher	Integrieren von NetWitness Endpoint 4.4.0.2 oder höher in NetWitness Endpoint 11.1





*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Überblick

In der folgenden Abbildung ist ein Beispiel der Registerkarte Allgemein gezeigt.



1 Klicken Sie auf **+**, um das Dialogfeld **Verfügbare Services** anzuzeigen.


- 2 Um den hinzugefügten Service zu löschen, klicken Sie auf .
- 3 Klicken Sie auf , um die Informationen für den hinzugefügten Service zu bearbeiten.
- 4 Klicken Sie auf  **Start**, um die Weiterleitung der Endpunkt-Metadaten zu starten.
- 5 Klicken Sie auf  **Stop**, um die Weiterleitung der Endpunkt-Metadaten zu beenden.

In der folgenden Tabelle werden die Felder auf der Registerkarte „Allgemein“ beschrieben.

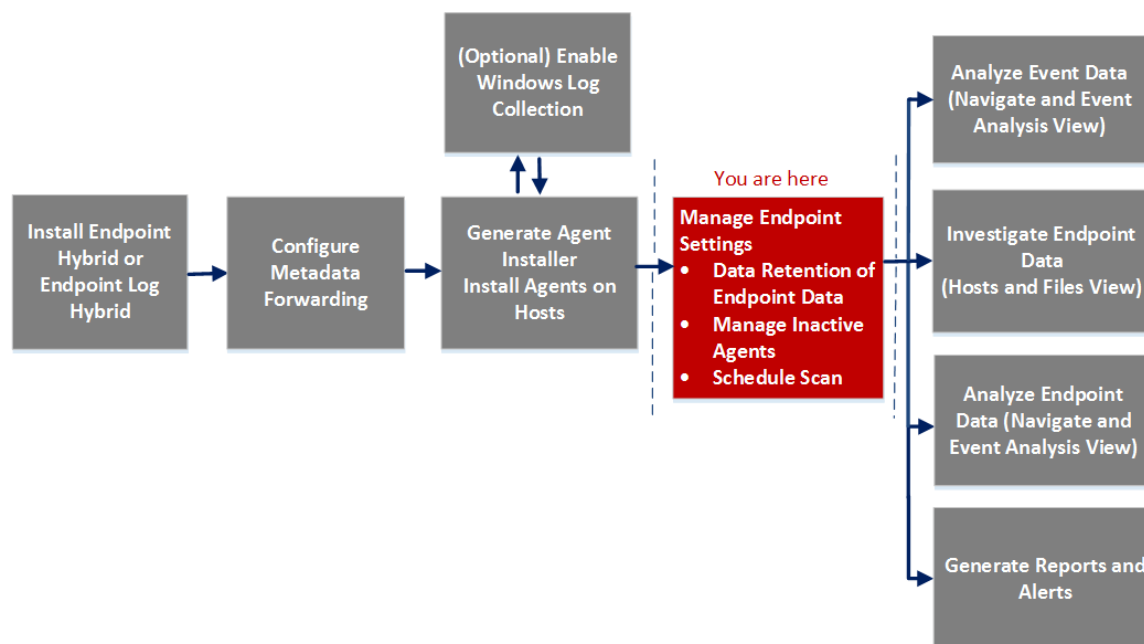
Feld	Beschreibung
Adresse	Zeigt die IP-Adresse des Log Decoder an.
Protobuf-SSL	Gibt an, ob SSL auf Protobuf aktiviert ist. Diese Option ist standardmäßig deaktiviert.
Protobuf-Port	Zeigt den Port für Protobuf an. Der Standardport ist 50202.
REST-SSL	Gibt an, ob SSL für den REST-Port im Log Decoder aktiviert ist. Diese Option ist standardmäßig deaktiviert.
REST-Port	Zeigt den Port für die REST-Kommunikation an. Der Standardwert ist 50202 (für Nicht-SSL) und 56202 (für SSL).
Benutzername	Zeigt den Benutzernamen an.
Rohdaten	Sendet eine kurze Zusammenfassung der Sitzung zusammen mit den Metadaten, wenn aktiviert. Diese Option ist standardmäßig deaktiviert.

Registerkarte „Datenaufbewahrungsplaner“

Auf der Registerkarte **Datenaufbewahrungsplaner** können Sie Policies für die Datenaufbewahrung und inaktive Agents konfigurieren. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht „Services“ die Option **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Datenaufbewahrungsplaner**.

Workflow



Was möchten Sie tun?

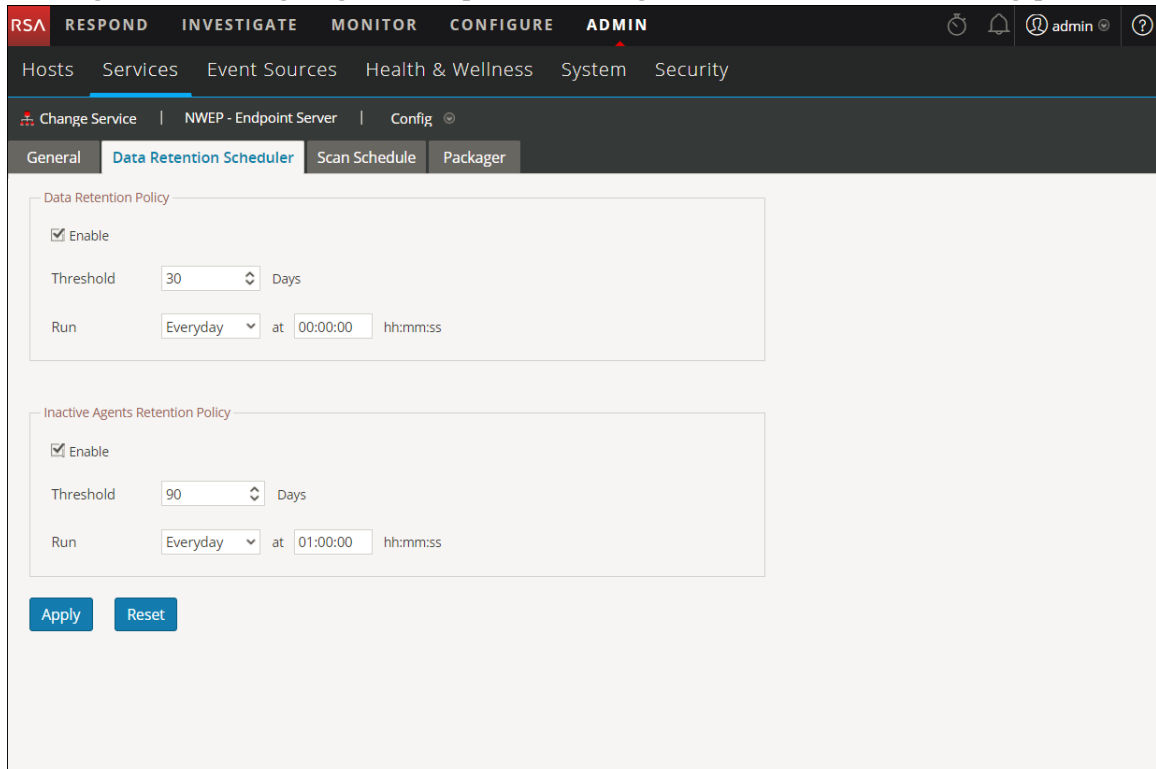
Rolle	Ziel	Anleitung
Administrator	Konfigurieren der Datenaufbewahrungs-Policy*	Konfigurieren der Datenaufbewahrungs-Policy

Rolle	Ziel	Anleitung
Administrator	Konfigurieren von Policies für inaktive Agents*	Inaktive Agents managen

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Überblick

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Datenaufbewahrungsplaner“.



Funktionen

In der folgenden Tabelle sind die Felder für die Datenaufbewahrungs-Policy enthalten.

Feld	Beschreibung
Aktivieren	Ermöglicht die Konfiguration der Datenaufbewahrungs-Policy. Diese Option ist standardmäßig aktiviert.

Feld	Beschreibung
Schwellenwert	Zeigt die Anzahl der Tage, die Endpunktdaten in der Datenbank aufbewahrt werden. Standardmäßig beträgt der Schwellenwert 30 Tage. Daten, die älter als 30 Tage sind, werden aus der Datenbank gelöscht.
Ausführen	Zeigt den Zeitplan für die Ausführung des Datenaufbewahrungsjobs an. Standardmäßig erfolgt die Datenbanküberprüfung täglich um 00:00:00 Uhr. Sie können die Häufigkeit („Täglich“, „Wochentage“, „Wochenenden“ oder „Benutzerdefiniert“, wobei bei „Benutzerdefiniert“ ein oder mehrere Tage der Woche ausgewählt werden können) und die Zeit für die Ausführung des Jobs aus der Drop-down-Liste auswählen.
Anwenden	Überschreibt etwaige vorhandene Pläne für diesen Service und wendet den neuen Zeitplan sofort an.
Zurücksetzen	Setzt den Zeitplan auf die Standardeinstellungen zurück.


In der folgenden Tabelle sind die Felder für die Aufbewahrungs-Policy für inaktive Agents enthalten.

Felder	Beschreibung
Aktivieren	Ermöglicht die Konfiguration der Policy für inaktive Agents. Diese Option ist standardmäßig aktiviert.
Schwellenwert	Zeigt die Anzahl der Tage an, die inaktive Agents auf dem Endpoint-Server beibehalten werden. Standardmäßig beträgt der Schwellenwert 90 Tage.
Ausführen	Zeigt den Zeitplan für die Ausführung des Aufbewahrungsjobs für inaktive Agents an. Standardmäßig erfolgt die Datenbanküberprüfung täglich um 00:00:00 Uhr. Sie können die Häufigkeit („Täglich“, „Wochentage“, „Wochenenden“ oder „Benutzerdefiniert“, wobei bei „Benutzerdefiniert“ ein oder mehrere Tage der Woche ausgewählt werden können) und die Zeit für die Ausführung des Jobs aus der Drop-down-Liste auswählen.

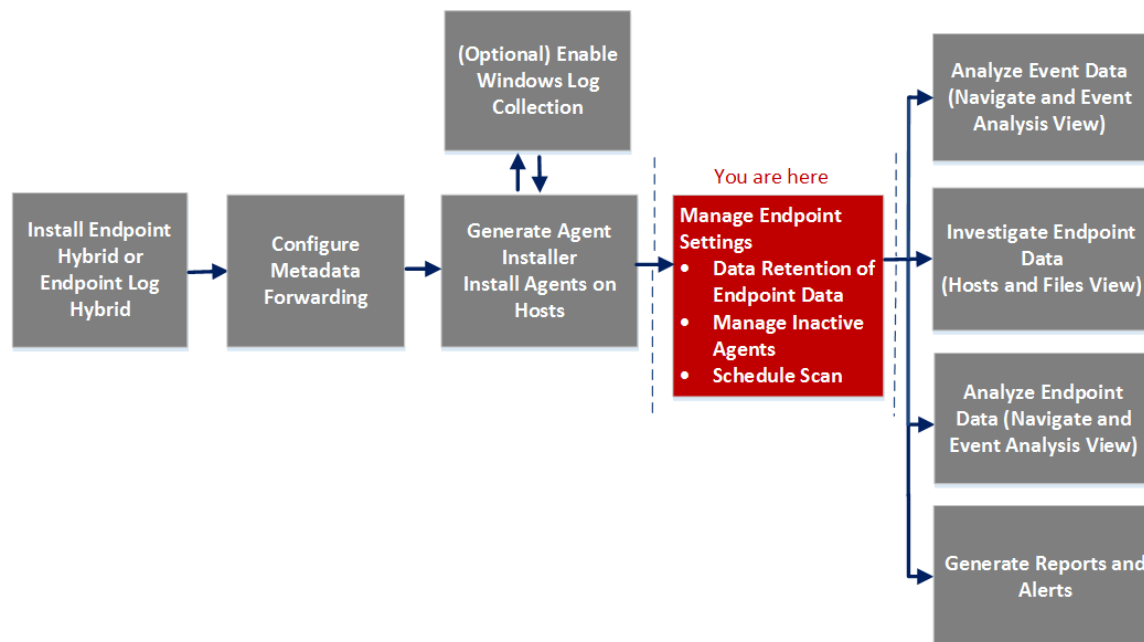
Felder	Beschreibung
Anwenden	Überschreibt etwaige vorhandene Pläne für diesen Service und wendet die neuen Einstellungen sofort an.
Zurücksetzen	Setzt den Zeitplan auf die Standardeinstellungen zurück.

Registerkarte „Scanplanung“

Auf der Registerkarte **Scanplanung** können Sie den Scan-Zeitplan konfigurieren. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht „Services“ die Option **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Scanplanung**.

Workflow



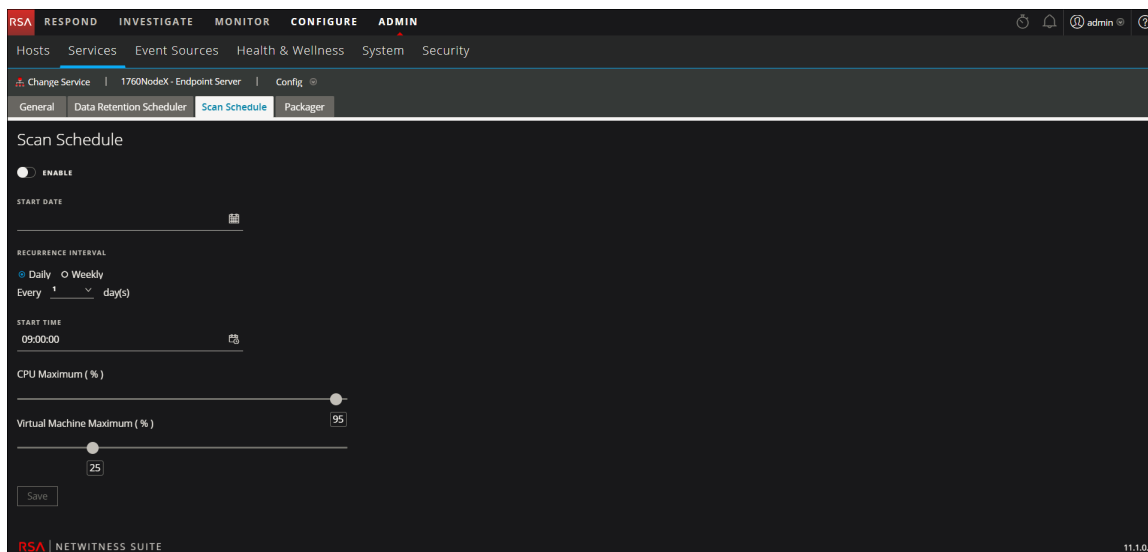
Was möchten Sie tun?

Rolle	Ziel	Anleitung
Administrator	Konfigurieren der Scanplanung*	Konfigurieren der Scanplanung

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Überblick

In der folgenden Abbildung ist ein Beispiel der Registerkarte „Scanplanung“ gezeigt.




In der folgenden Tabelle werden die Felder auf der Registerkarte „Scanplanung“ beschrieben. Die eingegebenen Werte beziehen sich auf die Zeitzone des Agent.

Feld	Beschreibung
Aktivieren	Wählen Sie diese Option zum Konfigurieren des Scans aus. Diese Option ist standardmäßig deaktiviert.
Startdatum	Geben Sie das Datum für den Start des Scans an.
Wiederholungsintervall	Wählen Sie das Wiederholungsintervall (Täglich oder Wöchentlich) aus und legen Sie die Häufigkeit in Tagen fest.
Startzeit	Geben Sie die Zeit für den Start des Scans an.
Maximaleistung CPU (%)	Legen Sie mit dem Schieberegler den Wert fest. Dadurch wird der CPU-Grenzwert für den Agent von NetWitness Endpoint sichergestellt.
Maximaleistung virtuelle Maschine (%)	Legen Sie mit dem Schieberegler den Wert fest. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Hinweis: Verwenden Sie diese Option, wenn Agents auf virtuellen Maschinen ausgeführt werden. Dies gilt nur für Windows-Agents.</p> </div>

Registerkarte „Packager“

Auf der Registerkarte **Packager** können Sie einen Agent-Packager und ein Agent-Installationsprogramm erzeugen. So greifen Sie auf diese Ansicht zu:

1. Navigieren Sie zu **Administration > Services**.
2. Wählen Sie in der Ansicht „Services“ die Option **Endpoint-Server** aus.
3. Klicken Sie auf  und wählen Sie **> Ansicht > Konfiguration** aus.
4. Klicken Sie auf die Registerkarte **Packager**.

Was möchten Sie tun?

Rolle	Ziel	Anleitung
Administrator	Erzeugen eines Agent-Packager zur Erfassung von Endpunktdaten*	<i>Endpoint Insights Agent-Installationshandbuch</i>
Administrator	Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung*	
Administrator	Erzeugen eines Agent-Installationsprogramms*	

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Weitere Informationen zum Erzeugen eines Agent finden Sie im *Endpoint Insights Agent-Installationshandbuch*.

Troubleshooting

Dieser Abschnitt enthält Informationen zu möglichen Problemen bei Verwendung von RSA NetWitness Endpoint Insights.

Probleme bei der Kommunikation mit Agenten

Problem	Agent kann nicht mit dem Endpoint Server kommunizieren.
Erläuterung	<p>Dies kann eine der folgenden Ursachen haben:</p> <ul style="list-style-type: none"> • Im Agent-Packager: <ul style="list-style-type: none"> • Server-IP ist falsch • Der angegebene Port ist für die Kommunikation mit dem Endpoint Server nicht verfügbar. • Endpoint-Server oder Nginx-Server wird nicht ausgeführt. • Firewall oder IP-Tabellenregeln blockieren die Verbindung zwischen dem Host und dem Endpoint Server. • Agent ist inaktiv oder wurde manuell über die Benutzeroberfläche gelöscht.
Lösung	<ul style="list-style-type: none"> • Prüfen Sie, ob der Endpoint Server und Nginx-Server erreichbar sind. • Deinstallieren Sie den Agent, starten Sie den Host neu und installieren den Agent neu. • Aktualisieren Sie ggf. die Firewall oder die IP-Tabellenregeln.
Problem	Agent braucht lange zum Scannen.
Erläuterung	In manchen Fällen dauert der NetWitness Endpoint-Scanvorgang lang. Dies liegt an der CPU-Auslastung durch andere Virenschutzprogramme (z. B. Windows Defender, McAfee, Norton usw.), die möglicherweise auf den Agent-Maschinen installiert sind.
Lösung	Es wird empfohlen, die Datei „NWEAgent.exe“ zur Whitelist der Virenschutz-Suite von Windows hinzuzufügen.

Probleme mit dem Packager

Meldung	Failed to load the client certificate.
Problem	Falsches Zertifikatpasswort.
Erläuterung	Beim Erzeugen des Installationsprogramms für den Agent stimmt das Zertifikatpasswort nicht mit dem Passwort überein, das beim Herunterladen des Agent-Packager über die Benutzeroberfläche angegeben wurde.
Lösung	Geben Sie das richtige Passwort für das Zertifikat an.

Meldung	An unexpected error has occurred attempting to retrieve this data.
Problem	Beim Versuch, die Registerkarte „Packager“ aufzurufen, wird sie mit der Meldung geöffnet.
Erläuterung	Endpoint Server ist möglicherweise ausgefallen oder nicht erreichbar.
Lösung	Prüfen Sie den Status des Endpoint Server unter Admin > Service . Wenn der Service nicht ausgeführt wird, starten Sie den Endpoint Server.

Probleme mit der Scanplanung

Meldung	An unexpected error has occurred attempting to retrieve this data.
Problem	Beim Versuch, die Registerkarte „Scanplanung“ aufzurufen, wird sie mit der Meldung geöffnet.
Erläuterung	Endpoint Server ist möglicherweise ausgefallen oder nicht erreichbar.
Lösung	Prüfen Sie den Status des Endpoint Server unter Admin > Service . Wenn der Service nicht ausgeführt wird, starten Sie den Endpoint Server.

Probleme mit Integrität und Zustand

Verhalten	Endpoint-Metadaten sind in der Ansicht Untersuchen > Navigation oder Ereignisanalyse nicht verfügbar.
Problem	Die Integritätsprüfung des Meta-Ld-Buffer zeigt im Abschnitt für Integrität und Zustand den Status Fehlerhaft mit den folgenden Ausnahmen an: dataprocessor-5] WARN MetaManagement Meta Forwarding waiting for free buffer in Log decoder
Lösung	Achten Sie auf Folgendes: <ul style="list-style-type: none"> • Erfassung ist auf dem Log Decoder aktiviert. • Metadaten sind ordnungsgemäß konfiguriert.

Verhalten	Bei Endpoint NetWitness 4.4.0.2 erreichen Metadaten den Endpoint Server nicht.
Problem	Die Integrität des Meta-Ld-Buffer zeigt im Abschnitt für Integrität und Zustand den Status Fehlerhaft mit den folgenden Ausnahmen an: dataprocessor-5] WARN MetaManagement Meta Forwarding waiting for free buffer in Log decoder
Erläuterung	Achten Sie auf Folgendes: <ul style="list-style-type: none"> • Zertifikat wurde erhalten und auf den NetWitness 4.4.0.2-Konsolenserver importiert. • Die NetWitness-Option „Untersuchen“ ist in der Benutzeroberfläche von NetWitness Endpoint aktiviert. • Metadaten-Weiterleitung ist im NetWitness 4.4.0.2-Konsolenserver konfiguriert.

Verhalten	Die Integritätsprüfung der Data.Application.Connection-Health-Statistik für Endpoint Server zeigt den Status Fehlerhaft an.
-----------	--

Problem	Mongo- oder Endpoint Server-Service ist nicht aktiv.
Erläuterung	Details zu Fehlern finden Sie in den Endpoint Server-Protokollen in /var/log/netwitness/endpoint-server/endpoint-server.log.
Lösung	Starten Sie den Mongo- oder Endpoint Server-Service neu.

Verhalten	Die Integritätsprüfung der Endpoint.Health.Overall-Health-Statistik zeigt den Status Fehlerhaft an.
Problem	Mongo- oder Endpoint Server-Service ist nicht aktiv.
Erläuterung	Prüfen Sie die anderen Endpoint Server-Integritätsstatistiken (z. B. Data.Application.Connection-Health, Endpoint.Health.Ld-Buffer-Health), um zu sehen, welche Statistiken den Status „Fehlerhaft“ aufweisen. Wenn eine den Status „Fehlerhaft“ aufweist, zeigt die Gesamtintegrität von Endpoint Server „Fehlerhaft“ an.
Lösung	Die Lösung für diese Statistiken finden Sie im Abschnitt Probleme mit Integrität und Zustand .

Problem	Agent-Ablehnungsanzahl übersteigt den Alarmschwellenwert.
Erläuterung	Die Anzahl abgelehnter Agenten übersteigt eine bestimmte Grenze und Ihre benutzerdefinierte Richtlinie wird ausgelöst. Beispiel: Die Anzahl abgelehnter Agenten in den letzten 5 Stunden entspricht 10 Prozent der bereitgestellten Agenten.
Lösung	Prüfen Sie die allgemeine Integrität des Endpoint Server und die Guidelines zur Dimensionierung.

Problem	Die Speichergröße der Datenanwendungsstatistik hat den Alarmschwellenwert überschritten.
Erläuterung	Die Speicherkapazität der Datenanwendung hat den Schwellenwert (z. B. 75 %) überschritten und die benutzerdefinierte Policy wird ausgelöst.
	Hinweis: Standardmäßig löscht der Server automatisch die älteren Daten, wenn 80 % des Speicherplatzes belegt sind.

Lösung	Prüfen Sie den in der Aufbewahrungs-Policy festgelegten Schwellenwert.
--------	--

Problem	Die Integritätsprüfung der Data.Application.Connection-Health-Statistik zeigt den Status „Fehlerhaft“ oder „Schwerwiegend“ an.
Erläuterung	Der Mongo-Service ist ausgefallen.
Lösung	Überprüfen Sie, ob der Mongo-Service ausgeführt wird, und prüfen Sie die Endpoint Server-Protokolle auf Fehlerdetails.

Problem	Die Anzahl der Agent-Anforderungen zeigt für einen Alarmschwellenwert 0 an.
Erläuterung	<p>Die Anzahl der Agent-Anforderungen zeigt für den ganzen Tag oder die ganze Woche 0 an. Dies kann eine der folgenden Ursachen haben:</p> <ul style="list-style-type: none"> • Im Agent-Packager: <ul style="list-style-type: none"> • Server-IP ist falsch • Der angegebene Port ist für die Kommunikation mit dem Endpoint Server nicht verfügbar. • Endpoint-Server oder Nginx-Server wird nicht ausgeführt. • Firewall oder IP-Tabellenregeln blockieren die Verbindung zwischen dem Host und dem Endpoint Server. • Agent ist inaktiv oder wurde manuell über die Benutzeroberfläche gelöscht.
Lösung	<ul style="list-style-type: none"> • Prüfen Sie, ob der Endpoint Server und Nginx-Server erreichbar sind. • Deinstallieren Sie den Agent, starten Sie den Host neu und installieren den Agent neu. • Aktualisieren Sie ggf. die Firewall oder die IP-Tabellenregeln.

Probleme mit der Metadatenkonfiguration

Verhalten	Der Konsolenserver zeigt eine Meldung an.
Problem	Auf dem Konsolenserver wird die folgende Meldung angezeigt: <i>Console Server will Log Processed batch as 1. "rsa-nw-endpoint-agent will be used to make SSL connection with NetWitness suite.</i>

Erläuterung	Wenn Sie einen schnellen Scan auf dem NetWitness Endpoint 4.4-Server für einen Agent oder eine Maschine ausführen, wird eine Meldung angezeigt.
Lösung	Überprüfen Sie die Metadatenkonfiguration.

Installationsproblem

Verhalten	NetWitness Suite erlaubt die Installation mehrerer Instanzen von Endpoint Hybrid oder Endpoint Log Hybrid.
Problem	Nur eine Instanz von Endpoint Hybrid oder Endpoint Log Hybrid kann für Endpunktdaten verwendet werden.
Erläuterung	Während der Installation von Endpoint Hybrid oder Endpoint Log Hybrid können Sie erfolgreich eine andere Instanz installieren.
Lösung	Sie müssen alle Instanzen von Endpoint Hybrid oder Endpoint Log Hybrid bis auf diejenigen löschen, die Sie für Endpunktdaten verwenden möchten.

Probleme mit der Suche nach inaktiven Agenten

Problem	Ein Agent ist möglicherweise nicht aktiv oder hat über einen längeren Zeitraum nicht mit dem Endpoint Server kommuniziert.
Erläuterung	Eine Liste der inaktiven Agenten finden Sie in der Mongo-Datenbank mit der Agent-ID. Mit diesen Informationen können Sie nach weiteren Informationen über die inaktiven Agenten suchen.
Lösung	<p>Führen Sie folgende Schritte aus, um inaktive Agenten in Ihrer Bereitstellung zu suchen:</p> <ol style="list-style-type: none"> Öffnen Sie die Endpoint Server-Protokolldatei über <code>/var/log/netwitness/endpoint-server/endpoint-server.log</code> und suchen Sie nach der Zeichenfolge „Agent <ID> ist nicht vorhanden“. Kopieren Sie die Agent-ID, die in der Protokolldatei angezeigt wird. Suchen Sie in der Protokolldatei für den NGINX-Zugriff (<code>/var/log/nginx/access.log</code>) nach der Agent-ID, um die folgenden Details eines inaktiven Agent abzurufen: <ul style="list-style-type: none"> IP-Adresse

- Datum und Uhrzeit, als der Agent deaktiviert wurde
- Speicherort

