

**PLUSCARD** **Service-Gesellschaft für Kreditkarten-Processing** **mbH**

**QRadar SIEM**

**Installationsanleitung**

Autor: Bruno Oliveira

SVA System Vertrieb Alexander GmbH

Freibergerstr. 39

01067 Dresden

Datum: 16.09.2017

Version: 0.3

Inhalt

[1 Dokumentinformationen 2](#_Toc492580156)

[1.1 Verteiler 2](#_Toc492580157)

[1.2 Versionshistorie 2](#_Toc492580158)

[2 System-/Applikationsbeschreibung 3](#_Toc492580159)

[2.1 Übersichtsplan (QRadar) 3](#_Toc492580160)

[2.2 Übersichtsplan der Hardware Komponenten 4](#_Toc492580161)

[3 Installation und Konfiguration 6](#_Toc492580162)

[3.1 Installation und Updates 6](#_Toc492580163)

[3.2 Logquellen 7](#_Toc492580164)

[4 Systemparameter 9](#_Toc492580165)

[5 System-/Applikationssicherheit 10](#_Toc492580166)

[5.1 Autorisierung 10](#_Toc492580167)

[5.2 Funktionsbenutzer 10](#_Toc492580168)

[5.3 Benutzer- und Berechtigungsverwaltung 10](#_Toc492580169)

[5.4 Rollen und Verantwortungsbereiche 10](#_Toc492580170)

[5.5 Monitoring und Alarmierung 11](#_Toc492580171)

[5.6 Maßnahmen zur Lokalisierung von Fehlern 13](#_Toc492580172)

[6 Use Cases und Regeln 14](#_Toc492580173)

[7 Wartungsmaßnahmen 15](#_Toc492580174)

[8 Glossar 16](#_Toc492580175)

[9 Anleitung 17](#_Toc492580176)

[10 Sonstiges 29](#_Toc492580177)

[10.1 TLS-Konfiguration 29](#_Toc492580178)

[10.1.1 Zertifikate 29](#_Toc492580179)

[10.1.2 DummyLogsource 29](#_Toc492580180)

[10.2 Wincollect Configuration Console - Installation 30](#_Toc492580181)

[10.3 Wincollect Configuration Console - Konfiguration 32](#_Toc492580182)

[10.4 Wincollect Debug 33](#_Toc492580183)

# Dokumentinformationen

## Verteiler

|  |  |
| --- | --- |
| Name | Firma/Abteilung |
| Andreas Haschick | Inexio/Pluscard |
| Tim Schuch | Inexio/Pluscard |
|  |  |

Tabelle 1: Verteiler

## Versionshistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Datum | Bearbeiter/Autor | Grund der Änderung | Status |
| 0.1 | 07.09.17 | Bruno Oliveira | Initialversion | Draft |
| 0.2 | 07.09.2017 | Oliver Braun | Erste Anpassungen | draft |
| 0.3 | 16.09.17 | Bruno Oliveira | Anpassungen | Draft |
|  |  |  |  |  |
|  |  |  |  |  |

Tabelle 2: Versionshistorie

# System-/Applikationsbeschreibung

Dieses Dokument beschreibt die Installation und Konfiguration von IBM QRadar SIEM bei der Pluscard. QRadar-SIEM wurde in der Version 7.3.0 Patch 3 installiert. Unter den neuen Features von der installierten Version sind folgende Eigenschaften nennenswert:

* Events per second and flows per minute are now combined in to shared license pools that can be distributed as administrators require across the deployment.
* QRadar updates the core operating system to Red Hat Enterprise 7.3.
* New installations can now use Logical Volume Management (LVM) for disk and partition management.
* Activation keys are no required as administrators can select an installation type based on the performance of the appliance.
* Log source limits are removed after updating to QRadar 7.3.0. Administrates can have an unlimited number of log sources in their deployment.
* QRadar now uses TLS v1.2 for secure communications between hosts and for internal communications.
* Tenants in QRadar can now create their on reference data collections.
* Tenants in QRadar can now create their own custom event/flow properties; however, the MSSP administrator is the only user that can optimize these custom properties.
* HA performance has been improved on Event Collector appliances (15xx) to reduce collection downtime during a failover.
* HA now provides new sensors to detect new or unique failover scenarios,.
* Two new appliance types are now available: 1. An M5 xx29 for use as an All-in-One 3129, Flow Processor 1729, or an Event Processor 1629. 2. An M5 xx48 high performance appliance for large systems or high throughput processing with 28 cores and 18TB of SSD storage.
* A number of API updates have been made to support new features.
* Ariel Query Language (AQL) now supports session queries, bitwise operators, and explicit start, stop, and begin functions.
* An updated app framework and a new App Node is available to host QRadar apps off of the Console to preserve resources.
* Remote Networks and Remote Services user interfaces are now improved.

## Übersichtsplan (QRadar)

Das gesamte Konstrukt besteht aus zwei 3105 All-in-One Appliances, die als HA-Cluster am Standort Saabrücken betrieben werden.

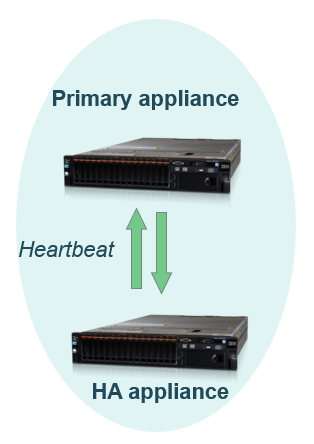


Abbildung 1

Jede Appliance fungiert als Console, Event Collector und Event Processor. Dies bedeutet, dass alle Netzwerkkomponenten Events direkt an die Appliances schicken. Die Events werden aufbereitet und in QRadar-Format umgewandelt, sodass QRadar sie verarbeiten kann. Die Replikation findet mittels „Distributed Replicated Block Device“ (DRDB) statt. Bei Ausfall des aktiven Knoten schwenkt Qradar automatisch auf den anderen Knoten.

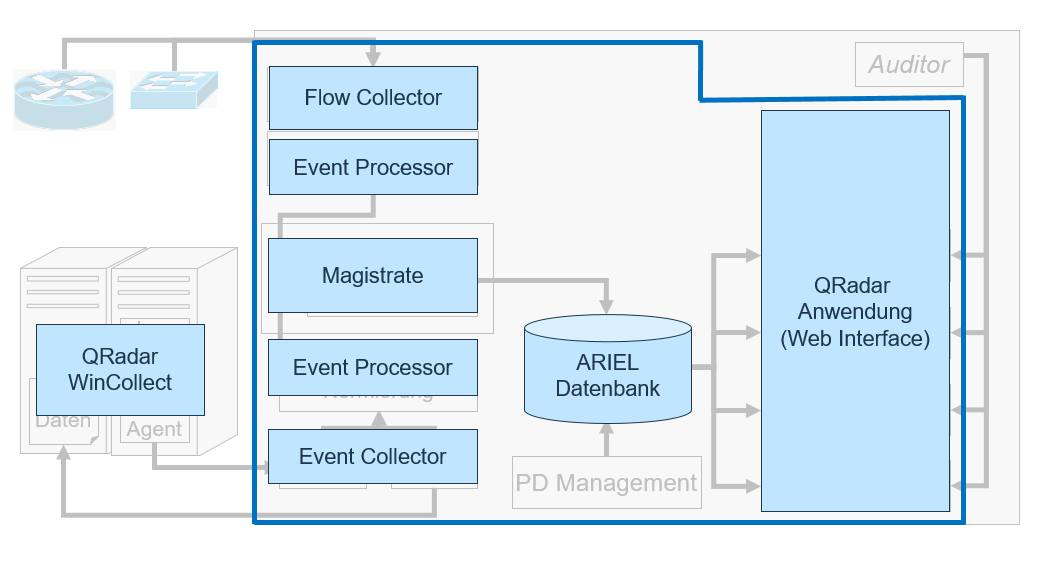


Abbildung 2

## Übersichtsplan der Hardware Komponenten

In diesem Abschnitt werden die Eigenschaften der physischen QRadar-Appliances aufgelistet.

Abbildung 3

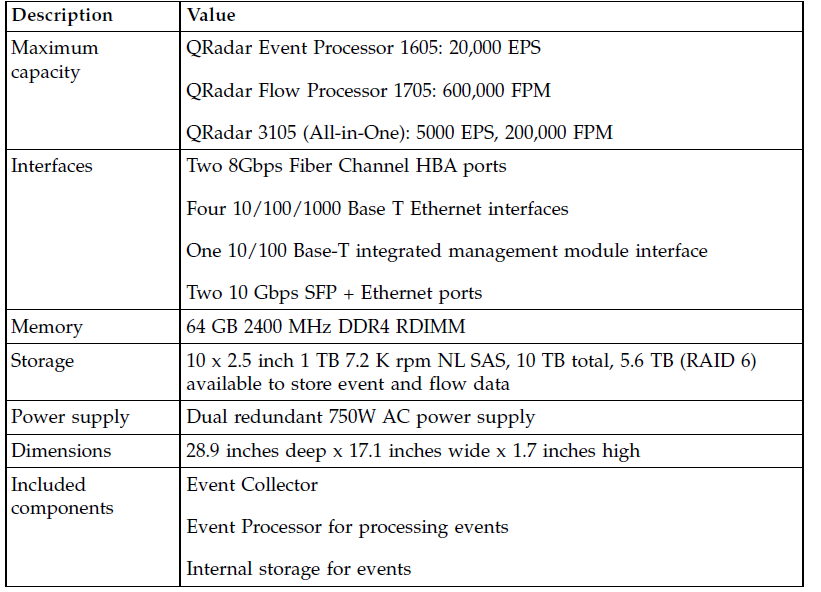


Abbildung 4

Zurzeit sind beide Appliances mit Lizenzen ausgestattet, die ermöglichen, 1000 EPS (Events per Second) zu verarbeiten. Die Lizenzen können bis auf 5000 EPS erweitert werden. Zur Zeit der Installation werden keine Flows an QRadar geschickt.

# Installation und Konfiguration

In diesem Abschnitt werden Details über die QRadar-Installation und Konfiguration beschrieben.

## Installation und Updates

Beide Appliances kommen mit QRadar SIEM in der Version 7.3.0 vorab installiert. Daher wurde eine Neuinstallation nicht durchgeführt, sondern der Patch 3 für die genannte Version wurde eingespielt, sodass die Installation auf dem aktuellen Stand ist. Die erste Appliance wurde mit der IP-Adresse 20.194.44.10 konfiguriert. Der zweiten Appliance wurde die IP-Adresse 20.194.44.12 zugewiesen. Die IP-Vergabe sowie weitere Parameter wie DNS-Server und Gateway erfolgte über das IMM-Interface auf beiden Systemen. Jedes IMM-Interface verfügt über eine IP-Adresse für den Fernzugriff. Die IP-Adressen lauten: 20.194.197.230 und 20.194.197.231. Bonding für die Ethernet-Interfaces der Appliances wurde auch konfiguriert und getestet. Die Interfaces eno1 und eno2 wurden zu einer virtuellen Netzwerkkarte bond0 zusagemmengefasst. Nachdem beide Appliances erreichbar waren, wurde die HA-Beziehung hergestellt. Die virtuelle IP-Adresse für das Cluster blieb die IP-Adresse des ersten Knoten, der eine neue IP-Adresse (20.194.44.11) bekam. Für die Heartbeat-Tests sowie für die DRDB-Replikation wurde ein zusätzliches Interface (ens3f1) über ein Crossover-Kabel konfiguriert.

|  |  |  |
| --- | --- | --- |
| Device | IP | FQDN |
| Cluster IP (VIP) | 20.194.44.10 | Qradar-cluster.pluscard.de |
| Cluster Node 1 | 20.194.44.11 | Qradar-cluster-primary.pluscard.de |
| Cluster Node 2 | 20.194.44.12 | Qradar-cluster-secondary.pluscard.de |
| Cluster Node 1 (IMM) | 20.194.37.230 |  |
| Cluster Node 2 (IMM) | 20.194.37.231 |  |

Tabelle 4 – Zuordnung der IPs

Der aktuelle Status der Systeme sowie der Cluster-Beziehung kann auf QRadar unter „Admin->System Configuration->System and License Management“ angesehen werden. Die Replikation mittels DRDB wurde angestoßen und hat circa 18 Stunden gedauert. Ein Failover-Test wurde erfolgreich durchgeführt.

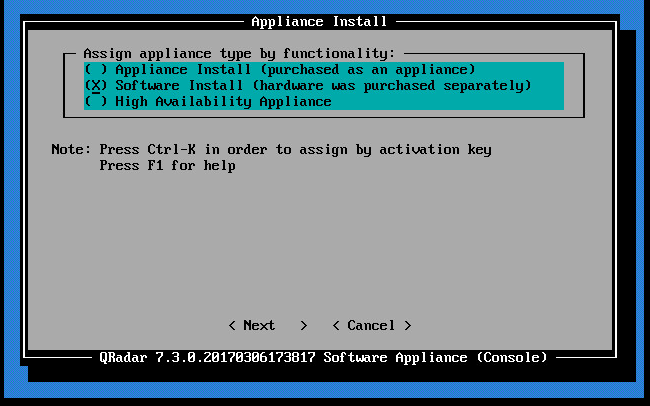


Abbildung 5

Die QRadar-Appliances können über einen Webproxy die aktuellen Updates herunterladen. Nachdem die Paramenter des Proxy-Servers eingetragen wurden, konnte QRadar den Update Server erreichen. QRadar prüft, ob neue Updates vorhanden sind.

Für die Einrichtung der QRadar-Appliances wurde ein einfaches Passwort verwendet. Dieses Passwort gilt für sowohl den Root-Account (Console) als auch den Admin-Account (Weboberfläche) und muss vor dem produktiven Betrieb geändert werden.

Für das Auführen von Skrippten sowie Wartungsmaßnahmen wurde der Account „admin\_sva“ auf der Shell-Ebene angelegt.

## Logquellen

Nachdem QRadar in Betrieb genommen wurde, konnten die ersten Log-Quellen eingebunden werden. Svamon schickte die ersten Events an QRadar, welche von QRadar normalisiert und als Log-Quellen erkannt wurden. Anschließend wurden Logquellen mittels Wincollect eingebunden. Aufgrund besonderer Anforderung an Verfügbarkeit wurde Wincollect Standalone eingesetzt. Wincollect kümmert sich um das Abholen von Events sämtlicher Windows-Systemen und schickt sie an QRadar. Für Wincollect wurde ein lokaler Puffer von 6 GB für das Zwischenspeichern von Events wurde konfiguriert. Wenn die Kommunikation zwischen Wincollect und QRadar unterbrochen wird, werden Events lokal gespeichert und automatisch an QRadar weitergeleitet, sobald die Kommunikation wiederhergestellt wird. So wird sichergestellt, dass keine Windows-Events verloren gehen.

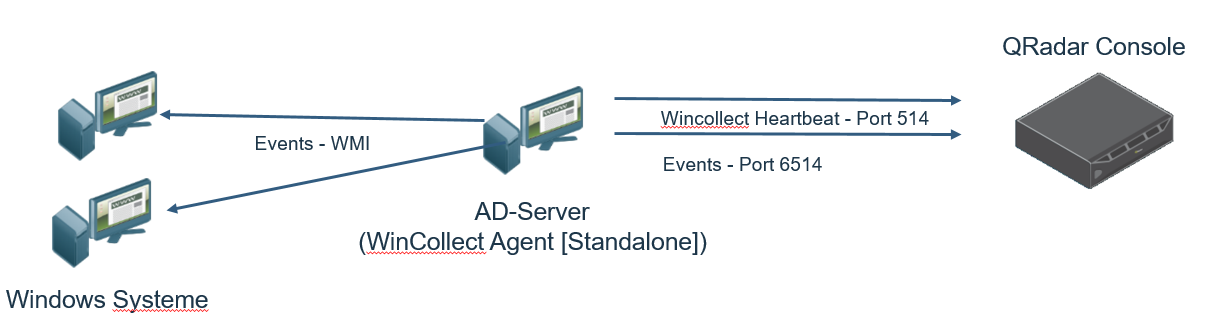


Abbildung 6

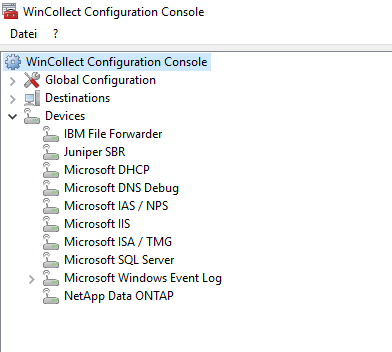
Wincollect wurde lokal auf beiden Active Directory Servern installiert. Ein weiterer Server dient als Event-Kollektor für Windows Systeme. Auf diesem Kollektor wurden Wincollect und die Wincollect Configuration Console installiert. In der Console ist es möglich, sogenannte „Devices“ hinzuzufügen, deren Events von dem Wincollect-Agenten abgeholt werden.  
  


Abbildung 7

Die Kommunikation zwischen Wincollect und QRadar erfolgt verschlüsselt. Das Zertifikat wurde von QRadar selbst ausgestellt und signiert,ist es 10 Jahre gültig. Ein QRadar Service Account für das Auslesen von Logs der Windows-Systeme wurde angelegt. Dieser Account wurde der Protokolllesergruppe der Domäne hinzugefügt.

# Systemparameter

Während der Installation wurden Änderungen vorgenommen, die von der Standard QRadar-Installation abweichen. Dieser Abschnitt beschreibt diese Einstellungen und begründet, warum d Standardwerte geändert wurden.

|  |  |  |  |
| --- | --- | --- | --- |
| Konfiguration | Standardwert | Anpassung | Grund |
| Coalescing | Deaktiviert | Aktiviert | Alle Events mit ihren Payloads werden gespeichert und nicht mehr zusammengefasst. |
| X-Force-Proxy | Deaktiviert | Aktiviert | QRadar befindet sich hinter einem Proxy. |
| X-Force-Feed aktiviert | Deaktiviert | Aktiviert | Tägliche Updates mit IP- und URL-Information. |
| Threat Content Pack | Nicht Installiert | Installiert | Paket beinhaltet neue Regeln und Building Blocks. |
| Update-Proxy | Nicht konfiguriert | Konfiguriert | QRadar befindet sich hinter einem Proxy. |
| Retention | 30 Tage | 395 Tage | Vergrößerung der Aufbewahrungszeit. |
| Zertifikat für die Weboberfläche | Selbst-signiert | Pluscard-Zertifikat | Anbindung an die bestehende PKI-Infrastruktur. |
| Timeout für Login |  | 3 Versuche |  |
| Hashwert für Event-Datenbank | Nicht aktiviert | Aktiviert |  |
| ICMP | Nicht erlaubt | Mittels iptables erlaubt | Troubleshooting wird vereinfacht. |

Tabelle 5 – Änderungen der Standardwerte

# System-/Applikationssicherheit

QRadar bietet Mechanismen zur Sicherung gegen Unbefugte. Außerdem ist es möglich, durch ein Berechtigungskonzept Rollen und Security Profile zu definieren. Backup-Policies sorgen dafür, dass sowohl Konfigurationsdaten als auch Protokolldaten abgesichert werden, damit das System im Fehlerfall schnell und einfach wiederhergestellt werden kann. . In diesem Abschnitt wird auf einige dieser Mechanismen eingegangen.

## Autorisierung

Für die Interaktion mit externen Dienst ist ein sogenannter Token erforderlich. Diese Tokens werden im Reiter „Admin“ unter Authorized Services erzeugt ermöglichen die Kommunikation mit QRadar über beispielsweise die RESTful API. Nachdem ein Token generiert wurde, muss man die Änderungen vornehmen, indem man „Deploy Changes“ anstoßt.

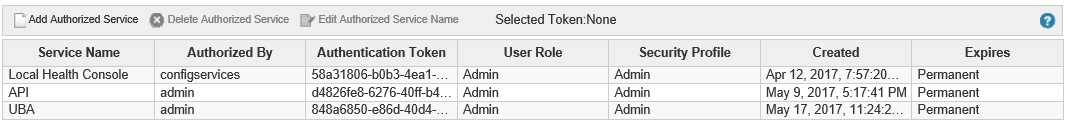


Abbildung 8

## Funktionsbenutzer

Abgesehen von der LDAP-Integration ermöglicht QRadar, Benutzer lokal zu verwalten. Keine zusätzlichen Funktionsbenutzer wurden angelegt. Der Admin-Account ist momentan das einzige Konto, das lokal verwaltet wird und vom Domain Controller unabhängig ist. In einem Ausfallsszenario (z.B. Ausfall von AD) kann sich nur der Admin-Benutzer anmelden.

## Benutzer- und Berechtigungsverwaltung

In dem Domain Controller wurde eine Benutzergruppe namens qradar-admins angelegt, in der sich Benutzer befinden, die auf das QRadar-System zugreifen dürfen. Die Benutzer in dieser Gruppe verfügen über keine besonderen Berechtigungen für QRadar, da alle Berechtigungen lokal auf QRadar verwaltet werden.

## Rollen und Verantwortungsbereiche

Es ist sinnvoll, Rollen und Security-Profile zu definieren, damit eingeloggte Benutzer nur bestimmte Bereiche sehen dürfen, für die sie die erforderlichen Berechtigungen besitzen. Außerdem können Benutzer nur bestimmt Änderung innerhalb ihrer berechtigten Bereiche durchführen. Eine Rolle beinhaltet die Menge der Funktionen, die einem Benutzer zur Verfügung steht. Das folgende Bild veranschaulicht alle Berechtigungen, die ein Benutzer besitzen kann. Außerdem kann man die Rollen sehen, die während der Konfiguration definiert wurden.

* Admin

Die Admin-Rolle besitzt alle Berechtigungen und dient als Notfall, da die Verbindung mit dem Domain Controller unterbrochen werden kann und somit andere Benutzer ausgesperrt werden. Der Admin-Account wird lokal verwaltet und ist vom Domain Controller unabhängig.

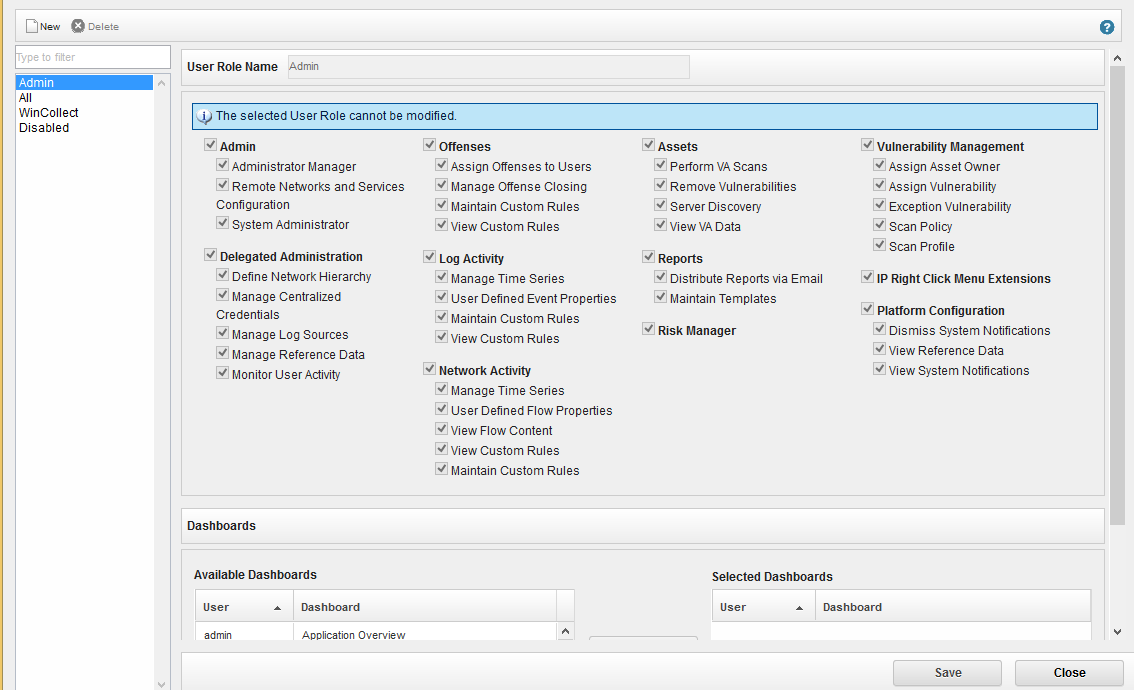


Abbildung 9

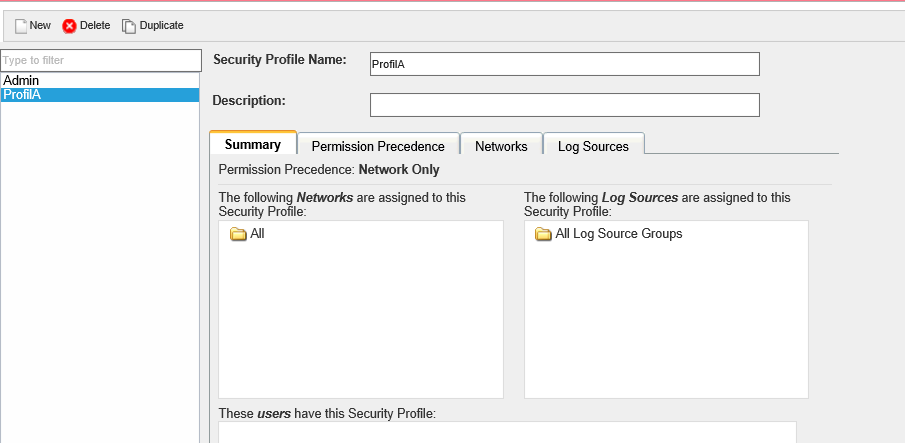


Abbildung 10

## Monitoring und Alarmierung

Es gibt mehrere Stellen, wo der aktuelle Status der QRadar-Systeme geprüft werden kann.

Auf der Weboberfläche befindet sich im Menü die der Reiter „Messages“. Dort können verschiedene Meldungen vom System angesehen werden. Wenn beispielsweise ein Schwellenwert überschritten wird, wird man benachrichtigt, solange die E-Mail-Konfigurationen (z.B. SMTP-Server und Empfänger-Adresse) korrekt sind.

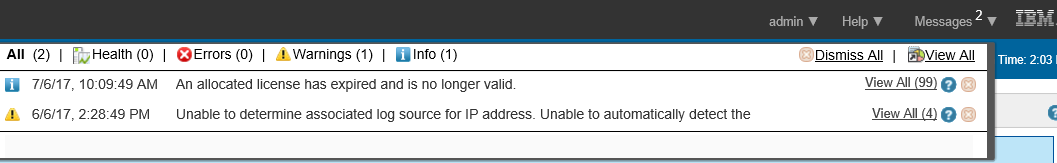


Abbildung 11

Im Reiter „Admin“ unter „Global System Notifications“ kann man Schwellenwerte für bestimmte Komponenten definieren. Auf dem QRadar-System der Pluscard sind Standartwerte eingetragen.

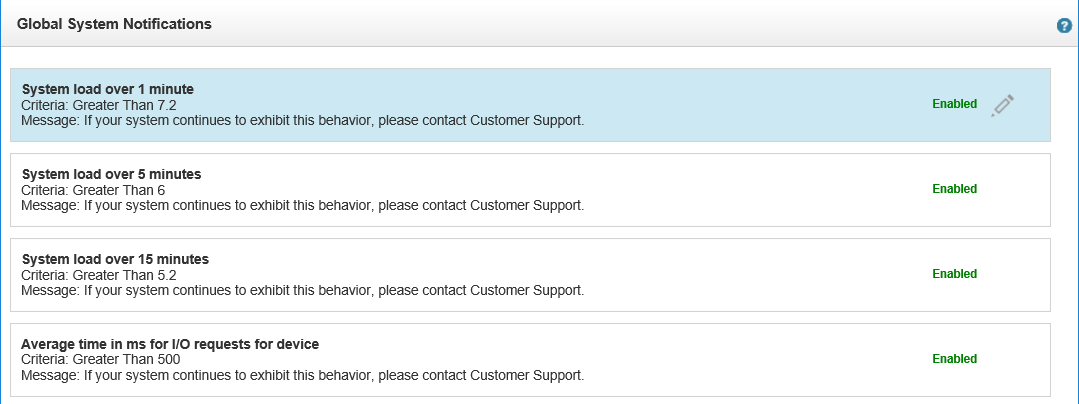


Abbildung 12

Im Reiter „Admin“ unter „System Health“ werden die Performance-Informationen der QRadar-System gezeigt.

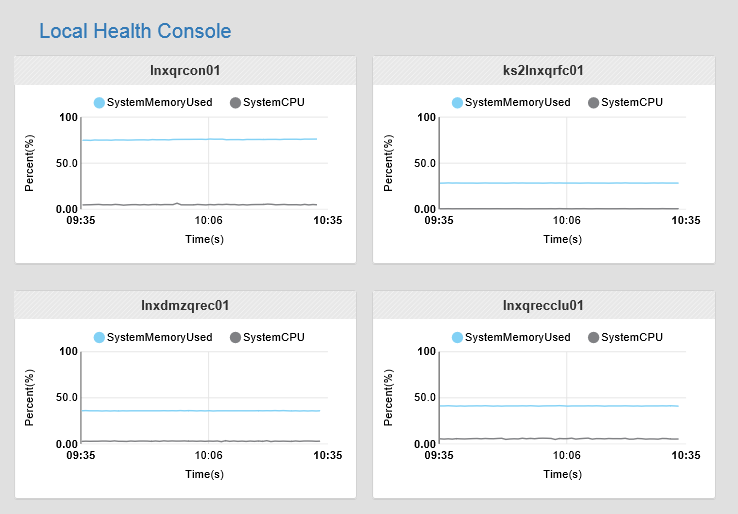


Abbildung 13

Unter „System and License Management“ befindet sich der Lizenzpool. Dort können Informationen bezüglich Lizenzen abgerufen werden.

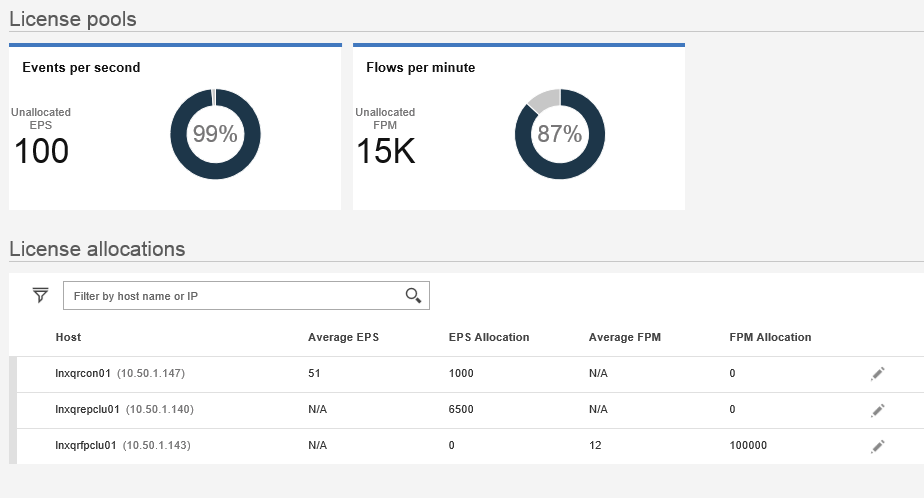


Abbildung 14

## Maßnahmen zur Lokalisierung von Fehlern

Wie im vorherigen Abschnitt beschrieben wurde, es gibt mehrere Orte auf der Weboberfläche, wo ein Benutzer Information bezüglich Fehler im System ansehen kann. Darüber hinaus können interne Protokolldaten von QRadar für Support-Zwecke über die Weboberfläche unter „System and License Management“ heruntergeladen werden. Außerdem ist es möglich, interne Protokolldaten von QRadar anzuschauen. Dafür ist eine Console-Verbindung über SSH erforderlich. Wichtige Log-Dateien sind:

* /var/log/qradar.log
* /var/log/qradar.error
* /var/log/qradar-sql.log
* /opt/tomcat6/catalina.out
* /var/log/qflow.debug

# Use Cases und Regeln

# Wartungsmaßnahmen

# Glossar

# Anhang

## Wincollect-Anleitung

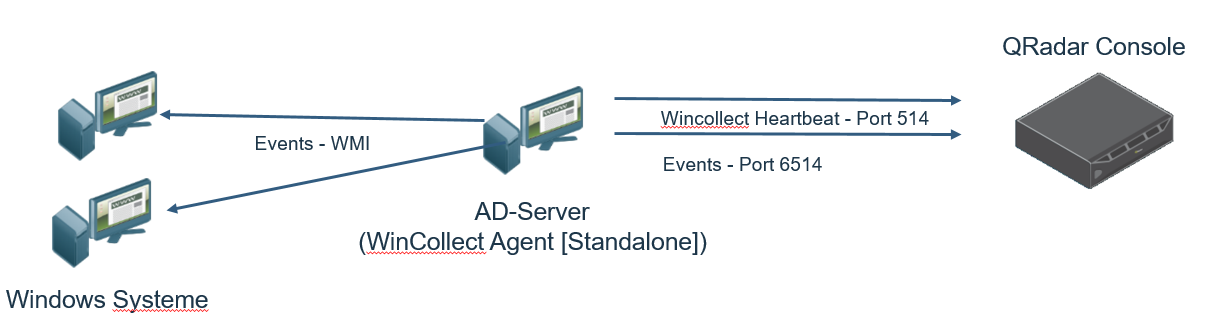
Dieses Dokument beschreibt die Installation von dem Wincollect-Agenten 7.2.6 im Stand-Alone Modus. In diesem Modus schickt der Wincollect-Agent Events an QRadar über TCP/UDP 514 oder TLS über den Port 6514. Es besteht auch die Möglichkeit, Events von anderen Windows-Systemen mittels Wincollect Configuration Console abzurufen und sie zu speichern, falls die Kommunikation mit QRadar vorübergehend unterbrochen wird.   
  


Abbildung 15

Download-Links:

-Patch Installer und Configuration Console

<https://sva-de.sharefile.eu/d-s870a668779f471f9>

MD5 Hash: 365f5dcc9817faf0ae94ba70f432457b

-X64-Version

<https://sva-de.sharefile.eu/d-s66f87db51b24fe08>

MD5 Hash: 2c8ee7ca91fc34e1e33d042c8ac8a6f9

1. Führen Sie das Installationsprogramm (X86 oder X64) aus.
2. Klicken Sie auf „Next“.

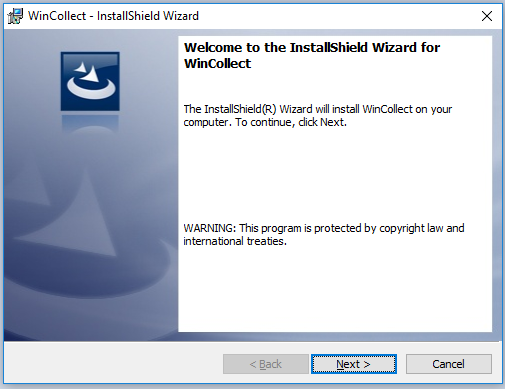


Abbildung 16

1. Klicken Sie auf „Next“.

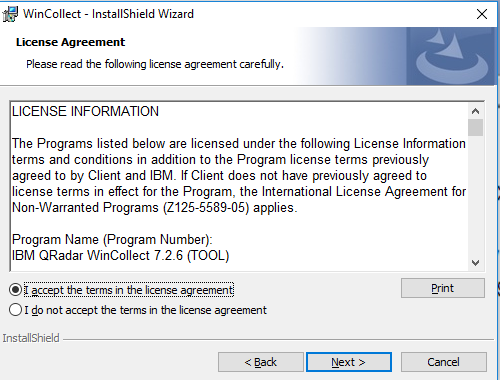


Abbildung 17

1. Geben Sie den Benutzer- und Organisationsnamen ein. Diese Information ist für QRadar irrelevant.

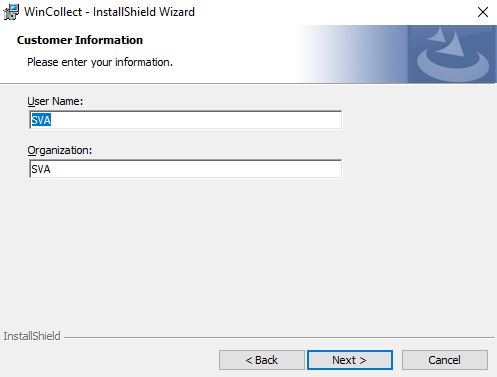


Abbildung 18

1. Klicken Sie auf „Next“.

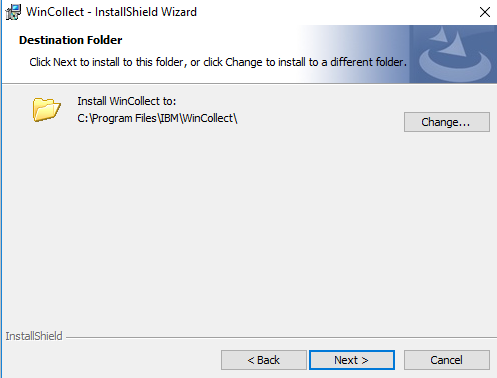


Abbildung 19

1. Wählen Sie „Stand Alone“ und klicken Sie auf Next.

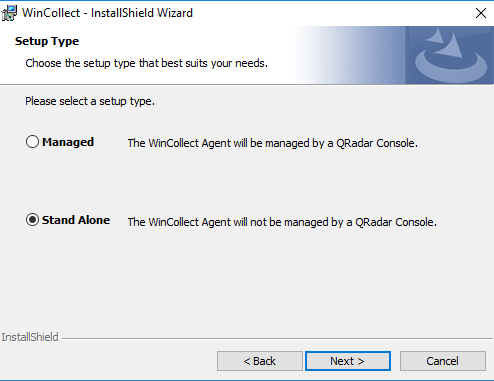


Abbildung 20

1. Setzen Sie einen Haken bei „Create Log Source“. Geben Sie einen Namen für die „Log Source“ an sowie die Hostname-Information dieser Quelle unter „Log Source Identifier“. Beide Namen können gleich sein. Setzen Sie einen Haken bei jeder Art von Event Logs, die der Agent weiterleiten soll.

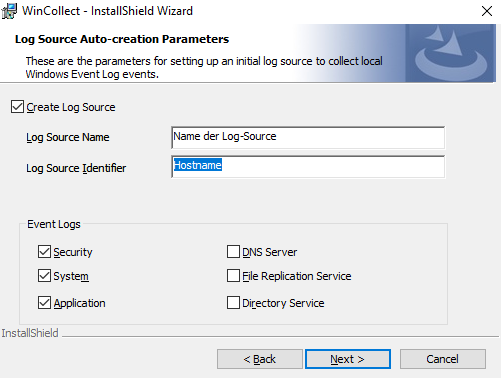


Abbildung 21

1. Unter „Destination Name“ geben Sie einen beliebigen Namen ein. Unter „Hostname/IP“ geben sie die IP-Adresse bzw. virtuelle IP-Adresse von dem Event Collector(QRadar). Vergewissern Sie sich, dass das Weiterleiten von Ereignissen über TCP Port 514 läuft, wenn Sie Events unverschlüsselt schicken möchten. Für den Fall, dass Sie TLS einsetzen möchten, setzen Sie die Portnummer 6514 und wählen Sie TCP(TLS) aus. Fügen Sie das TLS-Zertifikat ein. Das Zertifikat befindet sich unter /opt/qradar/conf/trusted\_certificates/tls-syslog.cert. Klicken Sie auf „Next“

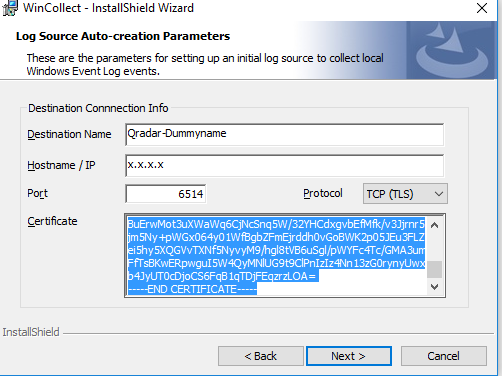


Abbildung 22

1. Wählen Sie ein Event Rate Tuning Profil (Für die meisten Server lassen Sie die Standard-Werte. Für AD-Server wählen Sie High Event Rate Event Server):
   1. Für 3000 ms (Empfehlung)
      1. Default (Endpoint) ->33-50 EPS
      2. Typical Server -> 166-250 EPS
      3. High Event Rate Server 416-625 EPS
   2. Für 1000 ms
      1. Default (Endpoint) 100-150 EPS
      2. Typical Server 500-750 EPS
      3. High Event Rate Server 1250-1875 EPS
2. Klicken Sie auf „Next“.

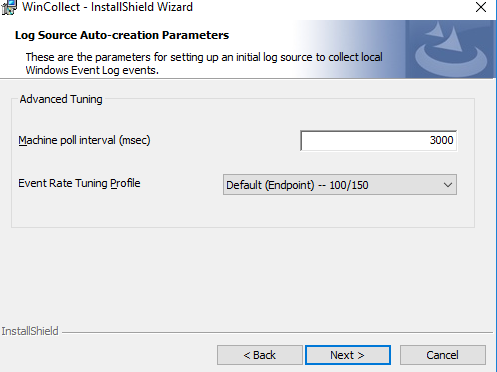


Abbildung 23

1. Klicken Sie auf „Next“.

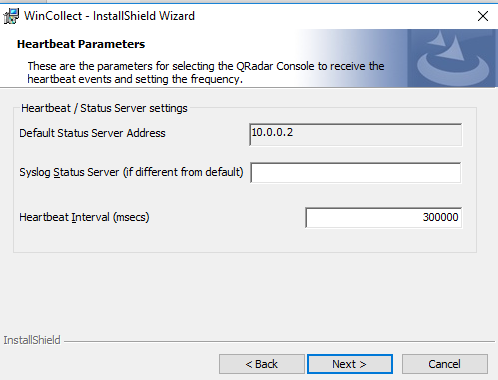


Abbildung 24

1. Nun bekommen Sie den Befehl für weitere WinCollect-Installationen, damit Sie den Agenten nicht mehr über das GUI installieren müssen. Dafür müssen Sie nur den Befehl bezüglich der neuen Log-Quelle anpassen. Beispiel:   
     
   wincollect-7.2.6-27.x64.exe /s /v"/qn INSTALLDIR=\"C:\Program Files\IBM\WinCollect\" LOG\_SOURCE\_AUTO\_CREATION\_ENABLED=True LOG\_SOURCE\_AUTO\_CREATION\_PARAMETERS=""Component1.AgentDevice=DeviceWindowsLog&Component1.Action=create&Component1.LogSourceName=**MY+Log+Source**&Component1.LogSourceIdentifier=**10.0.0.2**&Component1.Dest.Name=**My+Event+Collector**&Component1.Dest.Hostname=**10.0.0.1**&Component1.Dest.Port=514&Component1.Dest.Protocol=TCP&Component1.Log.Security=**true**&Component1.Log.System=**true**&Component1.Log.Application=**true**&Component1.Log.DNS+Server=**false**&Component1.Log.File+Replication+Service=**false**&Component1.Log.Directory+Service=**false**&Component1.RemoteMachinePollInterval=**1000**&Component1.EventRateTuningProfile=**Typical+Server**&Component1.MinLogsToProcessPerPass=**500**&Component1.MaxLogsToProcessPerPass=**750**"""
2. Klicken Sie auf „Next“.

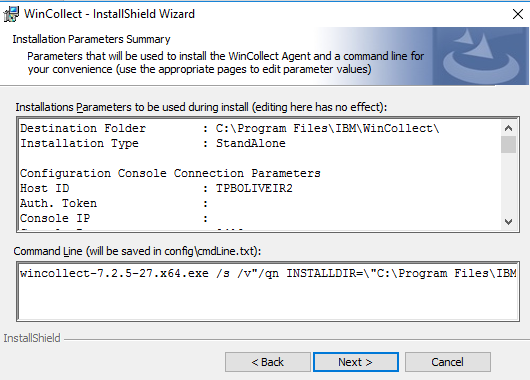


Abbildung 25

1. Klicken Sie auf „Next“, um WinCollect zu installieren.

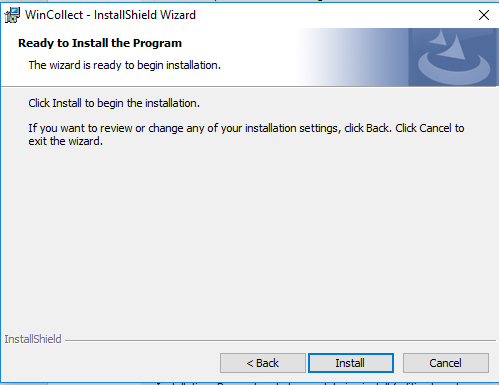


Abbildung 26

## Sonstiges

## TLS-Konfiguration

### Zertifikate

Die QRadar-Zertifikate befinden sich unter /opt/qradar/conf/trusted\_certificates. Für die verschlüsselte Kommunikation zwischen QRadar und Logquellen wird das Zertifikat syslog-tls.cert verwendet. Es handelt sich hierbei um ein selbst-signiertes Zertifikat. Man kann ein neues Zertifikat erstellen und das alte von IBM/QRadar ersetzen. Dafür muss man zuerst die Datei „/opt/qradar/conf/syslog-tls.keystore“ löschen und in QRadar „Full Deployment“ anstoßen. Danach wird ein neues Zertifikat erzeugt und als syslog-tls.cert gespeichert. (Das alte Zertifikat wird ersetzt)

Falls Sie Ihr eigenes Zertifikat benutzen möchten, müssen Sie Ihr Zertifikat in dem Keystore aufnehmen. Zunächst sieht man den Inhalt vom Keystore an, indem man das folgende Script ausführt:

/opt/qradar/bin/syslog\_tls\_import\_cert.sh

Für das importieren von eigenen Zertifikaten reicht der folgende Befehl:

/opt/qradar/bin/syslog\_tls\_import\_cert.sh -a **TLS** -k /**tmp/Certificates/ia.key** -c **/tmp/Certificates/ia.crt**

Die fettgedruckten Parameter müssen je nach Installation angepasst werden.

### DummyLogsource

Um zu wissen, ob QRadar Events an einem Port erwartet, muss man einen Befehl absetzen. Hier als Beispiel für den Port 6514:



Abbildung 27

Für TLS-Syslog verwendet QRadar standardmäßig den Port 6514. Allerdings ist der Port meistens nicht offen. Dafür muss eine Logquelle angelegt werden, die an diesem Port lauscht. Definieren Sie unter „maximum connections“ die maximale Anzahl von Verbindungen, die QRadar an diesem Port erlauben soll.

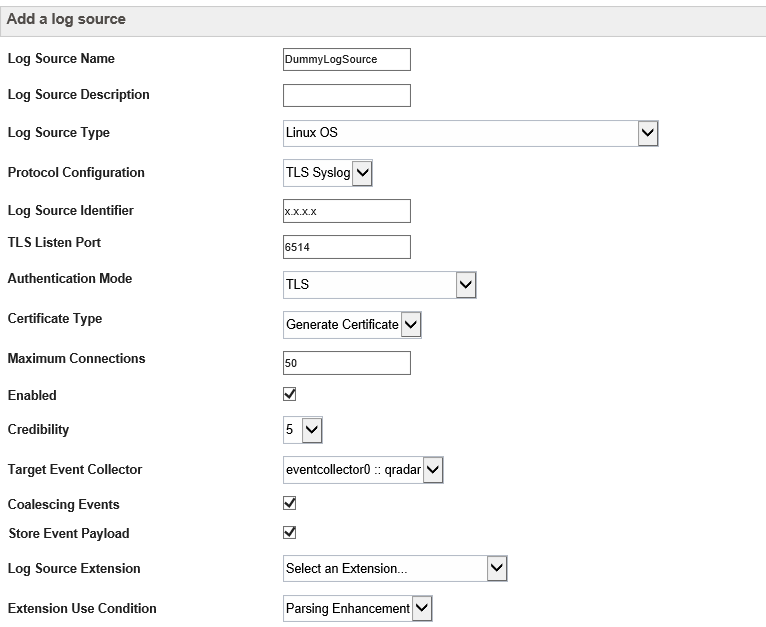


Abbildung 28

Vergessen Sie nicht, die Änderungen vorzunehmen, indem Sie „Deploy Changes“ anstoßen.

Anschließend sollen Sie sehen, dass QRadar den Port geöffnet hat.



Abbildung 29

## Wincollect Configuration Console - Installation

Damit Wincollect Events von anderen Logquellen holen kann, muss man die Wincollect Configuration Console installieren. Allerdings kann man sie zurzeit nur in der Version 7.2.5 installieren. Um die Installation der Configuration Console unter Wincollect 7.2.6 muss man die Installationsdatei der Version 7.2.5 benutzen.

1. Führen Sie die Installationsdatei der Version 7.2.5 aus und klicken Sie auf Next.
2. Stimmen Sie den AGBs zu und klicken Sie auf Next zweimal.
3. Klicken Sie auf erneut auf Next und beachten Sie, dass sowohl Wincollect Configuration Console als auch Wincollect Standalone Patch installiert werden.

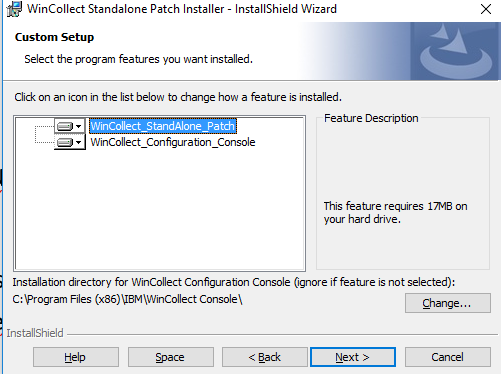


Abbildung 30

1. Klicken Sie auf Install.
2. Ein Fehler wird auftreten: Da die Installationsdatei mit dem Patch die Version 7.2.5 voraussetzt, kann die Version 7.2.5 nicht aktualisiert werden, denn sie ist nicht vorhanden, sondern die Version 7.2.6. Dies erlaubt nur die Installation von der Wincollect Configuration Console, was unser Ziel ist.

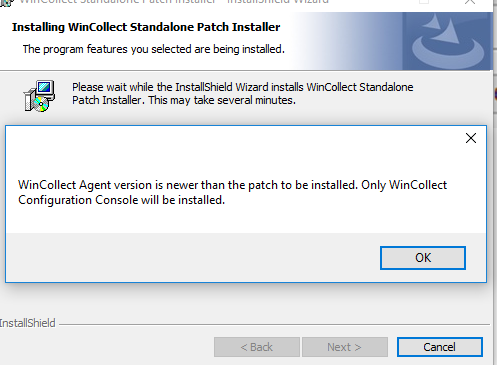


Abbildung 31

1. Klicken Sie auf Finish.

## Wincollect Configuration Console - Konfiguration

Damit der Wincollect Agent Events von anderen Windows-Servern holen kann, benutzt man die Wincollect Configuration Console. Die Wincollect Configuration Console holt Events von anderen Windows Servern und kann sie zwischenspeichern für den Fall, dass die Kommunikation zwischen QRadar und Wincollect vorübergehend unterbrochen wurde. Unter Disk Manager kann man die Größe des Puffers definieren. Standardmäßig reserviert die Console 6GB Platz auf der Festplatte.

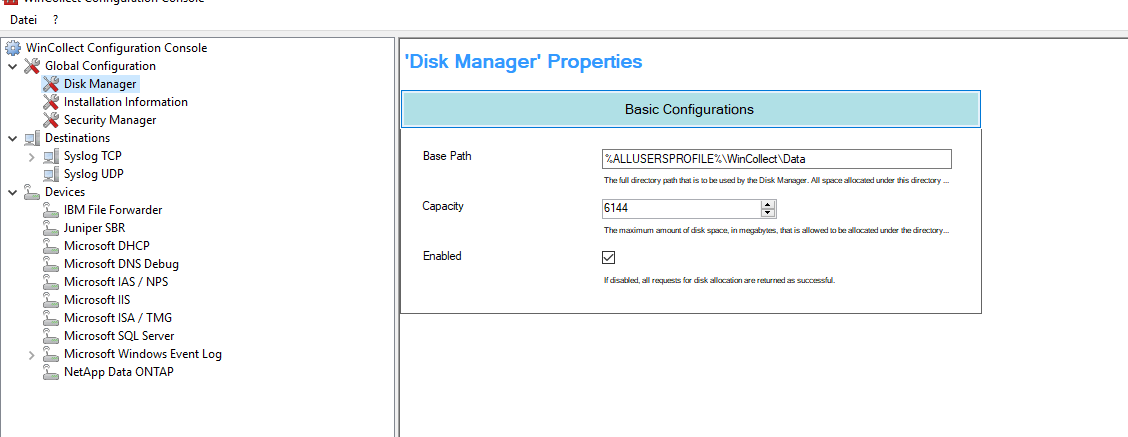


Abbildung 32

Unter „Security Manager“ kann man Credentials verwalten, die für das Auslesen der Events auf einer anderen Maschine notwendig ist. Diese Credentials benötigen keine besondere Rechte, müssen aber Mitglieder der Gruppe „Event Log Readers“ auf der Zielmaschine sein.

Unter „Destinations“ konfiguriert man wie der Agent mit QRadar kommunizieren soll. Hier soll man zum Beispiel das Ziel sehen können, das man in der Installationsphase definiert hat. Die Console unterstützt sowohl TCP als auch UDP. Die Kommunikation kann zusätzlich verschlüsselt werden.

Unter „Devices“ wählt man verschiedene Art von Systemen, deren Logs von Wincollect ausgelesen werden. Typischerweise wählt man „Microsoft Windows Event Logs“. Dort kann man neue Devices anlegen und festlegen, welche Logtypen (Security, System, Application) ausgelesen werden. Außerdem kann man dort die Credentials für dieses Device sowie das Ziel (TCP,UDP) auswählen. Wenn man alle benötigten Änderungen vorgenommen hat, kann man rechts auf „Deploy Changes“ klicken.

## Wincollect Debug

Wincollect selbst erzeugt Logs, die sich standardmäßig unter C:\Program Files\IBM\WinCollect\logs befinden. Um mehr Information zu bekommen, muss man die Debug-Logs aktivieren. Dies geschieht unter C:\Program Files\IBM\WinCollect\config. Dort befindet sich die Datei logconfig.xml, wo man den Wert von dem Key „Priority Value“ wie auf dem Bild ändern kann.  
  


Abbildung 33