IBM® Technical Support Appliance Leitfaden zum Konfigurationsassistenten

Version 2.8.0.0

Inhaltsverzeichnis

Einführung

IBM Technical Support Appliance (TSA) ist ein benutzerfreundliches Tool, mit dem Sie mehr Nutzen aus Ihren IBM Support-Verträgen ziehen können. TSA erkennt wichtige IT-Elemente und deren Beziehungen innerhalb Ihrer IT-Infrastruktur und überträgt die Daten zur Analyse sicher an den IBM Support. Diese Daten geben dem IBM Support Einblick in die komplexen Beziehungen zwischen den Servern und Netzkomponenten in Ihrem Rechenzentrum.

Ziel dieses Dokuments ist es, Informationen und Anleitungen zu liefern, die bei der Installation, Planung und Konfiguration der TSA helfen.

Netzüberlegungen bei der Offlineerkennung

Bevor Sie die TSA für die Ersterkennung und Übertragung konfigurieren, stellen Sie sicher, dass die folgenden Punkte angesprochen wurden. Es wird davon ausgegangen, dass die TSA bereits installiert wurde, die Webschnittstelle zugänglich und die TSA auf dem aktuellen Stand ist. Falls nicht, ziehen Sie das Technical Support Appliance-Installationshandbuch zu Rate (im weiteren Verlauf dieses Dokuments als Installationshandbuch bezeichnet).

TSA-spezifische Netzüberlegungen bei der Offlineerkennung	
Netzbetrieb	
	Öffnen Sie den Firewallzugriff von der TSA zu IBM. Siehe den Abschnitt **Konfigurationsanforderungen für Verbindungen zum IBM Support** im Installationshandbuch.
	Wenn ein SSL-Proxy für die Rückverbindung zu IBM verwendet wird, stellen Sie sicher, dass er in der TSA konfiguriert ist. Siehe den Abschnitt **IBM Konnektivität einrichten** im Installationshandbuch. - Die SSL-Prüfung wird nicht unterstützt. Wenn Sie die SSL-Prüfung auf dem Proxy verwenden, inaktivieren Sie sie für diese Abläufe.
	Wenn sich zwischen der TSA und den zu scannenden Zielgeräten Firewalls befinden, stellen Sie sicher, dass die erforderlichen Ports offen sind. Weitere Informationen siehe Abschnitt „Überlegungen zu Firewalls“ auf Seite 43.

Hilfreiche Dokumentation

Über den folgenden Link gelangen Sie direkt zur Website mit Informationen zur Technical Support Appliance. Dort finden Sie alles, was Sie für den Einstieg in die IBM Technical Support Appliance brauchen. Sie können auf Installationshandbücher und sicherheitsspezifische Dokumentation zugreifen, Beispielberichte anzeigen und den Installationscode der Technical Support Appliance von ibm.com herunterladen.

Weitere Informationen zur Technical Support Appliance: https://ibm.biz/TSAdemo

Überblick

Die TSA kann Informationen über Ihre IT-Infrastruktur, einschließlich der eingesetzten Betriebssystemkomponenten, Firmwarekomponenten, physischen Server, Netzgeräte, virtuellen LANs usw. erkennen. Um die Breite und Tiefe der gesammelten Informationen zu optimieren, sind Konfigurationsaufgaben innerhalb der TSA erforderlich, um die Erkennungsgeräte zu identifizieren.

Dabei versucht die TSA, die Auswirkungen auf die Netzumgebung des Kunden zu minimieren. Der Erkennungsprozess verwendet also einen iterativen und gemessenen Ansatz. Dies kann dazu führen, dass eine vollständige Erkennung bis zu 72 Stunden dauert. Der Status des Erkennungsjobs kann überwacht werden, indem Sie den Abschnitt **Jobzusammenfassung** in der **Zusammenfassungsanzeige** aufrufen.

Als Teil des Erkennungsprozesses versucht die TSA zunächst, Geräte innerhalb des definierten Bereichs ohne Verwendung von Berechtigungsnachweisen zu erkennen. Dazu gehört der Einsatz von Nmap, um Geräte über geringfügig intrusives IP-Scannen, Stack-Fingerprinting und Portzuordnung zu erkennen und klassifizieren. Im Allgemeinen ist diese Aktivität nicht signifikant genug, um ein Intrusion Detection System (IDS) auszulösen. Dies kann aber der Fall sein, wenn es strenge lokale Einstellungen gibt.

Damit die TSA Informationen über Ihre IT-Infrastruktur sammeln kann, müssen Sie Folgendes angeben:

- Bereiche
- Zugriffsberechtigungsnachweise

Bereichsgruppen definieren

Eine Bereichsgruppe ist eine logische Gruppierung von einzelnen Bereichen. Bereiche verwenden IP-Adressen, um der TSA mitzuteilen, wo mit der Erkennung der Umgebung begonnen werden soll. Eine Bereichsgruppe setzt sich aus einem oder mehreren Bereichen zusammen. Es lassen sich drei Arten von Bereichseinträgen unterscheiden:

- Teilnetz – Die Definition erfolgt über eine IP-Adresse und eine Teilnetzmaske.

  Teilnetze sind auf Teilnetze der Klasse C beschränkt.
- IP-Bereich – Umfasst alle IP-Adressen zwischen Anfangsadresse und Endadresse.
- IP-Adresse/Host – Eine individuelle IP-Adresse oder ein Hostname.

> Der Hostname wird zum Eingabezeitpunkt und nicht zur Erkennungszeit aufgelöst. Einzelheiten dazu finden Sie im Abschnitt „Zu berücksichtigende Faktoren bei der Bereichserstellung“ auf Seite 6.

Falls gewünscht, können Bereichsausschlüsse für einen Bereich durch Angabe einer Host-, Bereichs- oder Teilnetzdefinition definiert werden. Die daraus resultierenden IP-Adressen werden nicht als Teil des Bereichs betrachtet und nicht gescannt.

Die TSA unterstützt drei Arten von Bereichsgruppen:

1. **Allgemeine Bereichsgruppen**: Ermöglicht die Erkennung einzelner IT-Netzelemente. Die Bereichsgruppe enthält einen oder mehrere Bereiche, die den Standort dieser Netzelemente anhand einer IP-Adresse, eines Bereichs von IP-Adressen oder eines Netzes oder Teilnetzes identifizieren.
2. **Dynamische HMC-Bereichsgruppen**: Ermöglicht die Angabe der IP-Adresse eines oder mehrerer IBM POWER Systems HMCs zusammen mit den zugehörigen Berechtigungsnachweisen. Darüber hinaus können auch Informationen über alle LPARs, die die HMCs verwalten, gesammelt werden, ohne dass die IP-Adressen für die LPARs identifiziert werden müssen. Die dynamische Bereichsgruppe verwendet die von Ihnen bereitgestellten Berechtigungsnachweisinformationen, um fehlerfrei auf diese LPARs zuzugreifen.
3. **Dynamische VMware-Bereichsgruppen**: Ermöglicht die Angabe der IP-Adresse einer oder mehrerer VMware vCenter-Server- oder ESXi-Instanzen zusammen mit den zugehörigen Berechtigungsnachweisen. Darüber hinaus können auch Informationen über alle von VMware verwalteten virtuellen Maschinen gesammelt werden, ohne dass die IP-Adressen für die virtuelle Maschine identifiziert werden müssen. Die dynamische Bereichsgruppe verwendet die von Ihnen bereitgestellten Berechtigungsnachweisinformationen, um erfolgreich auf diese virtuellen Maschinen zuzugreifen.

Für HMCs und VMware vCenter-Server/ESXi wird die Verwendung dynamischer Bereichsgruppen empfohlen. Dynamische Bereichsgruppen erfordern in der TSA weitaus weniger Konfigurationsaufwand als die Erstellung und Verwaltung von Erkennungsbereichen für einzelne LPARs/virtuelle Maschinen. Auch für Umgebungen, in denen LPARs oder virtuelle Maschinen im Laufe der Zeit hinzugefügt oder gelöscht werden, können dynamische Bereichsgruppen diese Aufgabe übernehmen, ohne dass die Bereichsgruppen geändert werden müssen.

Detaillierte Anweisungen zur Definition von Erkennungsbereichen auf der TSA finden Sie im Abschnitt **Erkennungsbereiche einrichten** im Installationshandbuch.

Zu berücksichtigende Faktoren bei der Bereichserstellung

Es gibt keine definierten Standards für die Einrichtung von Bereichen. Es gibt jedoch einige praktische Überlegungen, durch die Sie Zeit und Aufwand sparen können:

- Wo dies praktisch möglich ist, verwenden Sie dynamische Bereichsgruppen, um die Erkennung von HMCs und ihren verwalteten LPARs bzw. von VMware vCenter-

Servern/ESXi und ihren verwalteten virtuellen Maschinen zu definieren. Bei Verwendung dynamischer Bereichsgruppen ist es nicht erforderlich, Bereiche für die LPARs oder virtuellen Maschinen zu definieren.

- Dynamische HMC-Bereichsgruppen erlauben den Import einer oder mehrerer IP-Adressen/Hostnamen für die HMCs, die Sie erkennen wollen. Weitere Informationen finden Sie im Abschnitt **Dynamische HMC-Bereiche** im Installationshandbuch.
- Dynamische VMware-Bereichsgruppen erlauben den Import einer oder mehrerer IP-Adressen/Hostnamen für die VMware vCenter Server- und ESXi-Instanzen, die Sie erkennen wollen. Weitere Informationen finden Sie im Abschnitt **Dynamische VMware-Bereiche** im Installationshandbuch.
- Verwenden Sie IP-Bereichs- oder Teilnetzbereiche, um mehrere Geräte statt einzelne IP-Adressen oder Hostnamen zu erkennen. Dadurch wird die Anzahl der Bereichsdefinitionen begrenzt und die Verwaltung erleichtert.
- Wenn Sie Teilnetzbereichsdefinitionen verwenden, beziehen Sie nur eine Definition pro Bereichsgruppe ein. Stellen Sie sicher, dass die Definition des Teilnetzbereichs auf ein Netz der Klasse C (256 IP-Adressen) oder weniger aufgelöst wird.
- Verwenden Sie die Funktion **Allgemeine Bereichsgruppe importieren**, um eine neue Bereichsgruppe basierend auf dem angegebenen Namen und der Liste der IP-Adressen aus einer Eingabetextdatei zu erstellen. Weitere Informationen finden Sie im Abschnitt **Erkennungsbereiche→ Allgemeine Bereichsgruppe importieren** im Installationshandbuch.
- Die TSA löst Hostnamen einmal zum Zeitpunkt der Eingabe auf. Wenn sich die IP-Adresse für ein System ändert, während derselbe Hostname beibehalten wird, muss der Bereich für dieses System gelöscht und neu erstellt werden, um die Auflösung zur neuen IP-Adresse zu ermöglichen.
- Je mehr IP-Adressen sich in der Bereichsgruppe befinden, desto länger dauert die Erkennung. Um die Erkennungszeit zu minimieren, richten Sie die Bereiche so ein, dass nur die Elemente, die Sie erkennen wollen, erfasst werden.

Beschränken Sie bei Verwendung von allgemeinen Bereichsgruppen die kumulative Anzahl der IP-Adressen, auf die eine Bereichsgruppe (nach der Erweiterung der Bereichs- oder Teilnetzdefinitionen) aufgelöst wird, auf maximal 400 IP-Adressen. Leistungs-, Server- oder Netzprobleme können während des Erkennungsprozesses auftreten, wenn mehr als 400 IP-

Adressen für eine einzige Bereichsgruppe gescannt werden. Bei Anzeige der Bereichsgruppe wird angezeigt, wie viele IP-Adressen eine bestimmte Bereichsgruppe zu erkennen versucht.

- TSA verhindert nicht, dass IP-Adressen in mehreren Bereichsgruppen definiert werden können. Generell sollte diese Praxis vermieden werden, da sie die Erkennungszeit verlängert, ohne dass zusätzliche Informationen gesammelt werden.
- Gruppieren Sie Bereiche in Bereichsgruppen, die eine logische Gruppierung von Geräten darstellen:
  - Gruppieren Sie gleiche Gerätetypen innerhalb einer Bereichsgruppe. Erstellen Sie zum Beispiel eine Bereichsgruppe für alle IBM FlashSystem-Speichersubsysteme.
  - Gruppieren Sie Geräte, die sich in der gleichen Region befinden.
  - Gruppieren Sie Geräte auf Basis von Geschäftsanwendungen oder Services.

Erkennungsberechtigungsnachweise

Bis auf wenige Ausnahmen erfordern Erkennungen einen gewissen Grad an Zugriffsmöglichkeiten, um die detaillierten Informationen zu erhalten, die für ein vollständiges Verständnis Ihrer Umgebung erforderlich sind.

Normalerweise sollten Servicekonten auf den Erkennungsgeräten für die Nutzung durch die TSA erstellt werden. In den folgenden Abschnitten finden Sie die spezifischen Zugriffsrechte, die für jeden Plattformtyp erforderlich sind. Um die Verwaltung dieser Servicekonten zu vereinfachen, verwenden Sie für alle Geräte einer bestimmten Produktfamilie den gleichen Benutzernamen.

Die Verwaltung der Servicekonten, über die die TSA die Verbindung zu den Geräten herstellt, kann durch eine der folgenden Strategien vereinfacht werden:

- Erstellen von Servicekonten mit nicht ablaufenden Kennwörtern
- Verwenden von SSH-Schlüsseln für Geräteproduktfamilien, die deren Verwendung unterstützen

Detaillierte Anweisungen zur Definition von Zugriffsberechtigungsnachweisen auf der Appliance finden Sie im Abschnitt **Erkennungsbereiche einrichten** im Installationshandbuch.

Zu berücksichtigende Faktoren beim Einrichten von Erkennungsberechtigungsnachweisen

Die Appliance versucht, die Anmeldedaten in der Reihenfolge zu verwenden, in der sie in der Zugriffsliste erscheinen. Um die Erkennung zu beschleunigen, stellen Sie sicher, dass Sie die Anmeldedaten in der Reihenfolge vorliegen haben, die am besten zu Ihrer Umgebung passt. Einige der Überlegungen stellen sich wie folgt dar:

- Beschränken Sie die Berechtigungsnachweise gegebenenfalls auf bestimmte Bereichsgruppen. Dadurch werden unnötige Anmeldeversuche eingeschränkt, und die Erkennungsleistung wird verbessert.
- Für diese Geräteerkennungen können SSH-Schlüssel verwendet werden:
  - AIX
  - Check Point
  - Cisco
  - Dell iDRAC
  - F5 Big IP
  - Fortinet
  - HMC
  - HP-UX
  - IBM FlashSystem
  - IBM i
  - IVM
  - Linux
  - Sun SPARC (Solaris)
  - SVC/V7000
  - VIOS

Es kann jeweils nur ein SSH-Schlüssel-Berechtigungsnachweis mit einer Bereichsgruppe verknüpft werden.

- Es hat sich bewährt, getrennte Servicekonten zu erstellen, die ausschließlich von der TSA mit der geringsten erforderlichen Berechtigungsstufe verwendet werden.

Erste Schritte

In diesem Abschnitt werden einige Best Practices und Empfehlungen für die Konfiguration der TSA behandelt.

Ersteinrichtung und -konfiguration der TSA

Führen Sie die Anweisungen in den folgenden Abschnitten des Installationshandbuchs aus:

- Technical Support Appliance installieren
- Bei der Technical Support Appliance anmelden
- Lizenzvereinbarung akzeptieren
- Die Technical Support Appliance mit dem Installationsassistenten einrichten

Vorbereitende Maßnahmen für Erkennungen

Es wird ein iterativer Prozess empfohlen, bei dem zunächst ein kleiner Teil des Netzes für die Erkennung erstkonfiguriert wird. Mit jeder Iteration werden dann weitere Netzabschnitte hinzugefügt, bis das gesamte gewünschte Netz abgedeckt ist.

> Es ist ein bewährtes Verfahren, eine Sicherungskopie Ihrer TSA-Konfiguration nach signifikanten Ergänzungen/Änderungen bei Bereichen und/oder Berechtigungsnachweisen zu speichern. Weitere Informationen finden Sie im Abschnitt zu „Sicherung und Wiederherstellung“ im IBM Technical Support Appliance-Installationshandbuch.

Schritte bei der Erkennung

Führen Sie für jede Erkennungsiteration die folgenden Schritte durch:

1. Bereiten Sie die Geräte für die Erkennung vor. Erforderliche Geräte- und Berechtigungsnachweiskonfigurationen finden Sie im Abschnitt „Geräteerkennungskonfiguration“ auf Seite 12.
2. Führen Sie bei dynamischen HMC-Bereichsgruppen die folgenden Schritte aus:
   a. Fügen Sie auf der Seite **Dynamische HMC-Bereichsgruppe** die IP-Adressen der HMCs hinzu.
   b. Fügen Sie auf der Seite **Dynamische HMC-Bereichsgruppe** die Berechtigungsnachweise für die HMCs hinzu.
   c. Wählen Sie die zu erkennenden LPAR-Typen aus. Geben Sie für jeden Typ die Berechtigungsnachweise an.

> Sie können die LPAR-Typen auswählen, die beim Erstellen der dynamischen Bereichsgruppe ermittelt werden sollen. Sie können aber auch die LPAR-Typen in einer späteren Iteration durch Ändern der dynamischen Bereichsgruppe hinzufügen.

d. (Optional) Nutzen Sie die Testfunktion auf der Seite **Dynamische HMC-Bereichsgruppe**, um zu überprüfen, ob die Berechtigungsnachweise richtig definiert sind und zur Herstellung einer Verbindung mit den HMCs oder deren LPARs verwendet werden können.

3. Führen Sie bei dynamischen VMware-Bereichsgruppen die folgenden Schritte aus:
   a. Fügen Sie die IP-Adressen der VMware vCenter-Server hinzu.
   b. Fügen Sie die IP-Adressen aller VMware ESXi-Hosts hinzu, die nicht von einem VMware vCenter-Server verwaltet werden.
   c. Fügen Sie die Berechtigungsnachweise für die VMware vCenter-Server- und ESXi-Instanzen auf der Seite **Dynamische VMware-Bereichsgruppe** hinzu.
   d. Wählen Sie die zu erkennenden VM-Typen aus. Geben Sie für jeden Typ die Berechtigungsnachweise an.

      Sie können die VM-Typen auswählen, die beim Erstellen der dynamischen Bereichsgruppe ermittelt werden sollen. Sie können aber auch die VM-Typen in einer späteren Iteration durch Bearbeiten der dynamischen Bereichsgruppe hinzufügen.

   e. (Optional) Nutzen Sie die Testfunktion auf der Seite **Dynamische VMware-Bereichsgruppe**, um zu überprüfen, ob die Berechtigungsnachweise richtig definiert sind und zur Herstellung einer Verbindung mit den VMware vCenter-Server- und ESXi-Instanzen sowie deren virtuellen Maschinen verwendet werden können.
4. Führen Sie bei allgemeinen Erkennungsbereichen die folgenden Schritte aus:
   a. Fügen Sie die gewünschten IP-Adressen in die entsprechenden Bereichsgruppen/Bereiche ein. Wenn Firewalls zwischen der TSA-Instanz und den Erkennungsgeräten bestehen, stellen Sie sicher, dass die entsprechenden Ports in der Firewall geöffnet sind, damit die Erkennung erfolgreich durchgeführt werden kann. Informationen darüber, welche Ports für jeden Plattformtyp geöffnet sein müssen, finden Sie im Abschnitt „Überlegungen zu Firewalls“ auf Seite 43.
   b. Erstellen Sie die erforderlichen Berechtigungsnachweise.
   c. (Optional) Nutzen Sie die Testfunktion in der Anzeige **Neue Erkennungsberechtigungsnachweise**, um zu überprüfen, ob der Berechtigungsnachweis richtig definiert ist und zur Herstellung einer Verbindung mit einem Zielgerät verwendet werden kann.
5. Führen Sie eine vollständige Erkennung aus, um die für diese Iteration hinzugefügten IP-Adressen zu scannen.
6. Führen Sie eine Übertragung zum Hochladen der Daten zu IBM aus.

Geräteerkennungskonfiguration

Zusätzlich zur Bereitstellung von Berechtigungsnachweisen können bestimmte Voraussetzungen für die Konfiguration des Erkennungsgeräts erforderlich sein, damit die TSA nützliche Komponenteninformationen effektiv erkennen und erfassen kann. In diesem Abschnitt können Sie Erkennungsgeräte in Ihrer Umgebung identifizieren, die spezielle Konfigurationen erfordern. Es wird empfohlen, Servicekonten mit den erforderlichen Mindestberechtigungen anzulegen. Siehe hierzu auch den Abschnitt „Überlegungen zu Firewalls“ mit Port- und Protokollinformationen.

- Bei Geräten, bei denen sowohl die SSH- als auch Telnet-Ports offen sind, versucht die TSA (aus Sicherheitsgründen) zunächst eine Verbindung per SSH herzustellen. Wenn diese SSH-Verbindung fehlschlägt, versucht die TSA die Verbindung über Telnet.

Betriebssysteme und Hosts

Plattform
IBM Power Systems • Hardware Management Console (HMC) • Integrated Virtualization Manager (IVM) • Virtual I/O Server (VIOS)-Partitionen • AIX • Linux on Power
IBM i
UNIX-Systeme • Solaris • Solaris über iLOM • Linux • HP-UX
VMware vCenter-Server und VMware ESXi
Windows
Bankautomaten

Managementmodul

- Flex System Manager (FSM)
- Chassis Management Module (CMM)
- Advanced Management Module (AMM)
- HP ProLiant Blade Server über HP OnBoard Administrator
- Integrated Management Module (IMM und IMM2)
- HP Integrity & HP9000 Server über iLO
- Dell Server über Integrated Dell Remote Access Controller (iDRAC)

Detaillierte Informationen erhalten Sie durch Klicken auf den jeweiligen Link.

IBM Power Systems

Bei IBM Power Systems, bei denen die Konfiguration der LPARs über die HMC oder den IVM verwaltet wird, verwenden Sie die dynamischen HMC-Bereichsgruppen. Mit den dynamischen HMC-Bereichsgruppen erstellen Sie eine Bereichsdefinition für die HMCs und stellen die zugehörigen HMC- und LPAR-Anmeldeinformationen zur Verfügung. Sie müssen hier keine Bereiche für jede verwaltete LPAR erstellen. Sobald die HMC erkannt wurde, ermittelt die TSA, welche LPARs zu diesem Zeitpunkt existieren, und scannt automatisch jede LPAR.

Bei IBM Power Systems, bei denen die Konfiguration von LPARs im Allgemeinen statisch ist, hat es sich bewährt, die Iteration durch Hinzufügen von Bereichen und Berechtigungsnachweisen für Entitäten in der folgenden Reihenfolge vorzunehmen:

1. **HMC- oder IVM-Instanzen**: Die HMC gibt aussagekräftige Informationen zu allen von ihr verwalteten Power Systems und den darin enthaltenen logischen Partitionen zurück. Das IVM gibt vergleichbare Informationen zu dem von ihm verwalteten Einzelsystem zurück.
2. **VIOS-Partitionen**: Hier werden Informationen über die physischen Adapter und Ressourcen zurückgegeben, deren Eigner diese Partitionen sind.
3. **Individuelle Partitionen**: Es gibt Fälle, in denen eine Nicht-VIOS-Partition Eigner physischer Adapter ist.

Hardware Management Console (HMC)

Zur Erkennung von HMC-Instanzen führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Damit die TSA Informationen zur Verwaltung der LPARs über die HMC erfassen kann, muss die HMC mit den LPARs über RMC-Tools kommunizieren können. Stellen Sie sicher, dass die HMC und die LPARs so konfiguriert sind, dass diese Kommunikation möglich ist. Weitere Informationen zu RMC-Tools für Linux finden Sie unter https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html
- Um eine sichere Datenerfassung zu ermöglichen, muss auf der HMC die Funktion für die Fernbefehlsausführung aktiviert werden. Informationen hierzu finden Sie im Thema „HMC-Fernbefehle aktivieren und inaktivieren“ unter der folgenden Adresse: https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablingandd isablinghmcremotecommands.htm

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen HMC-Bereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das HMC-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das HMC-Servicekonto.
- Der HMC-Benutzer muss die folgenden Rollen haben:
  - Rolle für spezifischen Ressourcenzugriff: AllSystemResources
  - Taskrolle (auf Basis von **hmcoperator** mit Befehlszeilentasks):
    - ManagedSystem (lshwres, lssyscfg)
    - Logische Partition (lshwres, lssyscfg, viosvrcmd)
    - HMC-Konfiguration (lshmc)
- Ein Benutzer (Servicekonto) mit **hmcviewer**-Berechtigung kann bei Bedarf ebenfalls verwendet werden. Dies führt jedoch zu einer partiellen Datenerfassung.

> Bei der Ausführung mit **hmcviewer**-Berechtigung können Informationen über Adapter, deren Eigner VIOS-Partitionen sind, nicht abgerufen werden. Um diese Informationen zu erhalten, müssen Sie sicherstellen, dass das Servicekonto mindestens über **hmcoperator**-Berechtigung verfügt. Wenn das nicht möglich

ist, fügen Sie Bereiche und Berechtigungsnachweise hinzu, um neben der HMC auch die VIOS-Partitionen direkt erkennen zu können.

Integrated Virtualization Manager (IVM)

Zur Erkennung von IVM-Instanzen führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das IVM-Servicekonto.
- Das Servicekonto darf nur Anzeigeberechtigung haben.

Virtual I/O Server (VIOS)-Partitionen

Zur Erkennung von VIOS-Instanzen führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen HMC-Bereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das VIOS-Partitions-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das VIOS-Partitions-Servicekonto.
- Das Servicekonto muss ein Administratorkonto (wie **padmin**) sein.
- Das Servicekonto muss das Benutzerattribut **rlogin=true** aufweisen. Sie können dieses Attribut mithilfe von SMIT oder durch Bearbeiten der **/etc/security/user**-Datei festlegen.
- Der Parameter **PermitUserEnvironment** in der **/etc/ssh/sshd_config**-Datei muss auf **yes** festgelegt sein.

AIX

Zur Erkennung von AIX-Instanzen führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass die Pakete bos.perf.tools und openSSH/openSSL installiert sind.
- Inaktivieren Sie die ungültigen Anmeldeversuche für das Servicekonto.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen HMC-Bereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das AIX-Partitions-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das AIX-Servicekonto.
- Das Servicekonto kann das Rootkonto oder ein Konto mit sudo-Berechtigung sein.
- Das Servicekonto muss das Benutzerattribut **rlogin=true** aufweisen. Sie können dieses Attribut mithilfe von SMIT oder durch Bearbeiten der **/etc/security/user**-Datei festlegen.
- So aktivieren Sie ein Servicekonto ohne Rootberechtigung für sudo-Berechtigung unter AIX:
  - Installieren Sie das sudo-RPM (sudo-1.6.9p15-2noldap) und die SSH-Dateigruppen (openssh.base.server, openssh.base.client) auf der AIX-Instanz).
  - Erstellen Sie eine ID für den Benutzer ohne Rootberechtigung auf der AIX-Zielinstanz, die von der TSA für den Zugriff auf das System verwendet werden kann.
  - Ändern Sie **/etc/sudoers** auf jeder AIX-Instanz, um der TSA zu erlauben, die angegebenen Befehle mit sudo-Berechtigung auszuführen.

    # Cmnd alias specification

    ```
    Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no,
    /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo,
    /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo,
    /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
    /usr/bin/sissasraidmgr, /usr/sbin/lswpar,
    /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso,
    /usr/sbin/bosdebug, /usr/sbin/chedition,
    /usr/esa/bin/esacli, /usr/sbin/bootinfo,
    /usr/bin/mpio_get_config, /usr/bin/cat /etc/objrepos/CuData,
    /usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat
    /var/adm/ras/bootlog, /usr/bin/cat
    /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
    /usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr
    view, /usr/sbin/powermt version, /usr/sbin/powermt display,
    /usr/bin/pcmpath query, /usr/sbin/datapath query
    ```

    # User privilege specification

    ```
    <User Name> ALL = NOPASSWD: TSA_CMDS
    ```

    - <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von AIX-Informationen verwendet. Dieser <User Name> ist ein Benutzer auf jeder AIX-Instanz. Die **/etc/sudoers**-Datei

auf jeder AIX-Instanz muss mit der obigen Spezifikation aktualisiert werden.

Oder

Eine Alternative zu den obigen Änderungen an der **/etc/sudoers**-Datei ist die Angabe der folgenden Benutzerberechtigung:

```
<User Name> ALL = NOPASSWD: ALL
```

- <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von AIX-Informationen verwendet. Diese Benutzerspezifikation erlaubt es dem Servicekonto, die sudo-Berechtigung für jeden AIX-Befehl zu verwenden.

Linux on Power

Zur Erkennung von Linux on Power-Instanzen führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Inaktivieren Sie die ungültigen Anmeldeversuche für das Servicekonto.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen HMC-Bereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Linux-Partitions-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Linux-Servicekonto.
- So aktivieren Sie ein Servicekonto ohne Rootberechtigung für sudo-Berechtigung unter Linux:
  - Erstellen Sie eine ID für den Benutzer ohne Rootberechtigung auf der Linux-Zielinstanz, die von der TSA für den Zugriff auf das System verwendet werden kann.
  - Ändern Sie **/etc/sudoers** auf jeder Linux-Instanz, um der TSA zu erlauben, die angegebenen Befehle mit sudo-Berechtigung auszuführen.

    # Cmnd alias specification

    ```
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,
    /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,
    /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,
    /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
    /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*,
    /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,
    /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-
    bound, /bin/cat /proc/sys/kernel/random/entropy_avail
    ```

User privilege specification

```
<User Name> ALL = NOPASSWD: TSA_CMDS
```

> <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von Linux-Informationen verwendet. Dieser <User Name> ist ein Benutzer auf jeder Linux-Instanz. Die **/etc/sudoers**-Datei auf jeder Linux-Instanz muss mit der obigen Spezifikation aktualisiert werden.

Oder

Eine Alternative zu den obigen Änderungen an der **/etc/sudoers**-Datei ist die Angabe der folgenden Benutzerberechtigung:

```
<User Name> ALL = NOPASSWD: ALL
```

> <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von Linux-Informationen verwendet. Diese Benutzerspezifikation erlaubt es dem Servicekonto, die sudo-Berechtigung für jeden Linux-Befehl zu verwenden.

- Wenn Sie das IBM Proweb-Portal für AIX als Teil Ihres Unterstützungsangebots mit IBM verwenden, wird empfohlen, dass Sie die TSA mit dynamischen HMC-Bereichsgruppen konfigurieren. Alternativ können Sie die TSA so konfigurieren, dass die HMCs und die logischen Partitionen (einschließlich VIOS) auf den Power-Systemen erkannt werden.
- Beim Scannen mithilfe von dynamischen HMC-Bereichsgruppen erhalten Sie detailliertere Informationen zur Betriebssystemkonfiguration für jede LPAR, die von ProWeb abgerufen und analysiert werden können.

> Informationen zum Hinzufügen von Bereichen und Berechtigungsnachweisen für HMC-Umgebungen finden Sie im Abschnitt **Dynamische HMC-Bereiche** im IBM Technical Support Appliance-Installationshandbuch.

- Ebene der für den Bericht erfassten Daten durch Scannen verschiedener Power Systems-Entitäten:
  - Wenn Sie nur HMCs scannen, erhalten Sie alle wichtigen Informationen auf den Registerkarten „Identifiziert“, „HMC-Topologie“, „Power Systems Firmware“, „IBM i-Empfehlungen“, „Linux-Empfehlungen“, „HMC/VIOS/AIX“ und „Vertrag“ sowie einige Adapterinformationen.

- Darüber hinaus erhalten Sie durch direktes Scannen von VIOS-Partitionen zusätzliche Informationen zur Adapterfirmware und zu verbundenem Speicher.
- Durch direktes Scannen der LPARs erhalten Sie weitere Informationen zu LPARs sowie zu Betriebssystemdetails und zu Instanzen spezieller Software wie PowerHA, GPFS und PowerSC.

IBM i

IBM i-Instanzen werden über eine SSH-Verbindung erkannt. Wenn auf der IBM i-Instanz kein SSH installiert und konfiguriert ist, befolgen Sie die folgenden Schritte:

Bereiten Sie die Umgebung vor:

Stellen Sie sicher, dass die folgenden Produkte/Optionen für IBM i 7.2 installiert und konfiguriert sind:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, Option 30
- Portable App Solutions Environment, 5770-SS1, Option 33
- IBM Developer Kit for Java, 5770-JV1

Stellen Sie sicher, dass die folgenden Produkte/Optionen für IBM i 7.3 installiert und konfiguriert sind:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, Option 30
- Portable App Solutions Environment, 5770-SS1, Option 33
- IBM Developer Kit for Java, 5770-JV1 Option 16
- Java SE 8 32 Bit

Stellen Sie sicher, dass die folgenden Produkte/Optionen für IBM i 7.4 installiert und konfiguriert sind:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, Option 30
- Portable App Solutions Environment, 5770-SS1, Option 33
- IBM Developer Kit for Java, 5770-JV1 Option 16
- Java SE 8 32 Bit

Starten Sie den SSH-Dämon mit dem folgenden Befehl:

```
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))
```

Starten Sie den SSHD-Service auf IBM i mit dem folgenden Befehl:

```
STRTCPSVR SERVER(*SSHD)
```

Weitere Informationen zum Konfigurieren von SSH auf IBM i finden Sie in den Kapiteln 21-23 in diesem Redbook – http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann eine beliebige Benutzerklasse haben wie ***USER**, auch wenn zusätzliche Anforderungen an die Objektberechtigung zu erfüllen sind, um PTF-Informationen zu erfassen (über den Befehl **DSPPTF**).
- **DSPPTF** wird mit den folgenden Einschränkungen bei den Objektberechtigungen geliefert:
  - Der Befehl wird mit der allgemeinen Berechtigung ***EXCLUDE** bereitgestellt.
  - **Die Benutzerprofile QPGMR**, **QSYSOPR**, **QSRV** und **QSRVBAS** werden mit persönlichen Berechtigungen zur Verwendung dieses Befehls bereitgestellt.
  - Wie immer kann dieser Befehl mit dem Benutzerprofil **QSECOFR** oder einem anderen Benutzerprofil mit der Benutzerklasse ***SECOFR** ausgeführt werden.
- Beim Objekt **QSYS/DSPPTF** des Objekttyps ***CMD** können die Berechtigungen bearbeitet werden, damit auch andere Benutzer diesen Befehl ausführen können.
- Wenn ein neues Servicekonto für die TSA erstellt wird, gelten die folgenden Empfehlungen:
  - Erstellen Sie das Benutzerprofil mit der Benutzerklasse ***USER**.
  - Verwenden Sie den Befehl **GRTOBJAUT**, damit über dieses Benutzerprofil der Befehl **DSPPTF** ausgeführt werden kann; das Objekt ist **QSYS/DSPPTF** mit dem Objekttyp ***CMD**.

UNIX-Systeme

Solaris

Zur Erkennung von Solaris-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie auf Solaris-Systemen sicher, dass das Paket SUNWscpu (Source Compatibility) installiert ist.
- Auf einigen Solaris-Systemen muss SNEEP installiert und konfiguriert sein, um Seriennummern abrufen zu können.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Das Servicekonto kann auch ein Servicekonto ohne Rootberechtigung sein.

Solaris über Oracle iLOM

Zur Erkennung von Solaris-Geräten über Oracle iLOM führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann entweder **Operator**- oder **Administrator**-Berechtigungen haben.

Linux

Wenn die Linux-Instanz auf einem IBM Power System läuft, lesen Sie die Anweisungen im Abschnitt Linux on Power auf Seite 17 unter IBM Power Systems.

Zur Erkennung von Linux on x86-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass das Paket pciutils installiert ist. Über den darin enthaltenen Befehl `lspci` werden Informationen über Adapter und Verbindungen zu externen Speichergeräten erfasst.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen VMware-Bereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Linux-VM-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Linux-Servicekonto.
- Legen Sie `/bin/sh` als Shell für dieses Konto fest.
- Für Linux (x86) kann das Servicekonto das Rootkonto oder ein Konto mit `sudo`-Berechtigung sein.
- Um Erkennungen mit einem Servicekonto ohne Rootberechtigung durchzuführen, fügen Sie der **/etc/sudoers**-Datei auf dem Linux-System Folgendes hinzu:

  # Cmnd alias specification

  ```
  Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode
  ```

User privilege specification

```
<User Name> ALL = NOPASSWD: TSA_CMDS
```

- <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von Linux-Informationen verwendet. Dieser <User Name> ist ein Benutzer auf jeder Linux-Instanz. Die **/etc/sudoers**-Datei auf jeder Linux-Instanz muss mit der obigen Spezifikation aktualisiert werden.

Oder

Eine Alternative zu den obigen Änderungen an der **/etc/sudoers**-Datei ist die Angabe der folgenden Benutzerberechtigung:

```
<User Name> ALL = NOPASSWD: ALL
```

- <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von Linux-Informationen verwendet. Diese Benutzerspezifikation erlaubt es dem Servicekonto, die sudo-Berechtigung für jeden Linux-Befehl zu verwenden.

HP-UX

Zur Erkennung von HP-UX-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- So aktivieren Sie ein Servicekonto ohne Rootberechtigung für sudo-Berechtigung unter HP-UX:
  - Ändern Sie **/usr/local/etc/sudoers** auf jedem HP-UX-Gerät, um der TSA zu erlauben, die angegebenen Befehle mit sudo-Berechtigung auszuführen.

    # Cmnd alias specification

    ```
    Cmnd_Alias TSA_CMDS
    =/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus
    ```

    # User privilege specification

    ```
    <User Name> ALL=(ALL) NOPASSWD:TSA_CMDS
    ```

- <User Name> gibt das Servicekonto ohne Rootberechtigung an, den die TSA zum Erfassen von HP-UX-Informationen verwendet.

VMware vCenter-Server und VMware ESXi

Verwenden Sie für VMware-Umgebungen dynamische VMware-Bereichsgruppen. Mit den dynamischen VMware-Bereichsgruppen erstellen Sie eine Bereichsdefinition für VMware vCenter-Server/ESXi und stellen die zugehörigen VMware- und VM-Berechtigungsnachweise zur Verfügung. Sie müssen hier keine Bereiche für jede verwaltete virtuelle Maschine erstellen. Sobald der VMware vCenter-Server/ESXi erkannt wurde, ermittelt die TSA, welche virtuellen Maschinen zu diesem Zeitpunkt existieren, und scannt automatisch jede virtuelle Maschine.

Bei VMware-Umgebungen, bei denen die Konfiguration von virtuellen Maschinen im Allgemeinen statisch ist, hat es sich als Alternative für dynamische VMware-Bereichsgruppenn bewährt, die Iteration durch Hinzufügen von Bereichen und Berechtigungsnachweisen für Entitäten in der folgenden Reihenfolge vorzunehmen:

1. **vCenter Server-Instanzen**: Hier werden aussagekräftige Informationen zu den von den Instanzen verwalteten ESXi-Hosts und den darin enthaltenen VM-Gästen zurückgegeben.
2. **ESXi-Hosts**: Fügen Sie ESXi-Hosts hinzu, die nicht von einem vCenter-Server verwaltet werden.
3. **Individuelle VM-Gäste**: Hier können detailliertere Informationen über das Betriebssystem erfasst werden.

Bei der Konfiguration der TSA für VMware-Umgebungen werden die folgenden Aktionen empfohlen:

1. Konfigurieren Sie die TSA so, dass VMware vCenter-Server, wo verfügbar, erkannt werden. Die automatische Erkennung eines VMware vCenter-Servers bewirkt, dass die TSA Informationen zu allen VMware ESXi-Hosts sammelt, die der vCenter-Server verwaltet. Konfigurationsdaten zu den ESXi-Hosts sind nicht erforderlich.
2. Konfigurieren Sie die TSA so, um VMware ESXi-Hosts nur dann zu erkennen, wenn der ESXi-Host nicht von einem VMware vCenter-Server verwaltet wird.
3. Installieren Sie VMware Tools auf jeder virtuellen Maschine, die auf den ESXi-Hosts gehostet wird. Wenn diese Tools nicht installiert sind, sind einige Bestandsdaten wie IP-Adresse oder Betriebssystem nicht zugänglich.
4. Konfigurieren Sie jeden VMware ESXi-Host so, dass die CIM-Schnittstelle aktiv ist. Über die CIM-Schnittstelle kann die TSA detaillierte Informationen über die Adapter innerhalb des ESXi-Hosts erfassen. Weitere Informationen zum CIM-Provider finden Sie in „Anhang C“ auf Seite 44.

Führen Sie die folgenden Schritte aus, um vCenter-Serverinstanzen sowie Informationen zu den von den Instanzen verwalteten ESXi-Servern zu erkennen:

Bereiten Sie die Umgebung vor:

- Installieren Sie VMware Tools auf jeder virtuellen Maschine, die auf den ESXi-Hosts gehostet wird.
- Konfigurieren Sie jeden VMware ESXi-Host so, dass die CIM-Schnittstelle aktiv ist.
- Der CIM-Port (5989) muss über die TSA erreichbar sein (und nicht durch Firewalls blockiert werden). Nur so ist eine vollständige Erkennung gewährleistet.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen VMware-Bereichsgruppen: Benutzername/Kennwort für das VMware vCenter-Server-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Computersystem: Benutzername/Kennwort für das VMware vCenter-Server-Servicekonto.
- Das Servicekonto muss die Rollenberechtigung **Administrator** oder zumindest Berechtigungen für eine benutzerdefinierte R/O-Rolle mit den folgenden zusätzlichen Berechtigungen haben:
  - Global → Lizenzen
  - Global → Einstellungen
  - Host → CIM
  - Host → Konfiguration → Einstellungen ändern
  - Host → CIM→ CIM-Interaktion

Zur direkten Erkennung von ESXi-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Installieren Sie VMware Tools auf jeder virtuellen Maschine, die auf den ESXi-Hosts gehostet wird.
- Konfigurieren Sie jeden VMware ESXi-Host so, dass die CIM-Schnittstelle aktiv ist.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen VMware-Bereichsgruppen: Benutzername/Kennwort für das VMware ESXi-Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Computersystem: Benutzername/Kennwort für das VMware ESXi-Servicekonto.
- Das Servicekonto muss die Rollenberechtigung **Administrator** haben.

Windows

Die TSA unterstützt die Erkennung von Windows-Instanzen mit den folgenden Methoden:

- WINRM

- SMB1

Windows über WINRM wird bevorzugt, da dies die sicherere Schnittstelle ist.

Windows über WINRM

Zur Erkennung von Windows-Geräten über WINRM führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

Die gängigste Art, die Umgebung vorzubereiten, ist die Verwendung eines Serverzertifikats, das von einer Zertifizierungsstelle generiert wird, die auf dem Windows-Zielserver installiert ist. Das Zertifikat muss die folgenden Bedingungen erfüllen:

- Die Root- und Zwischenzertifikate von der Zertifizierungsstelle müssen sich in den Trusted Root Certification Authorities-Zertifikaten befinden.
- Das Serverzertifikat muss sich in den Personal-Zertifikaten befinden.
- Das Serverzertifikat muss belegen, dass es auf den vollständig qualifizierten Hostnamen des Servers ausgestellt ist.
- Das Serverzertifikat muss den privaten Schlüssel für diesen Server enthalten.

Über den folgenden Befehl wird WINRM für remote angebundene HTTPS-Verbindungen konfiguriert:

```
winrm quickconfig -transport:https
```

Dieser Befehl bewirkt Folgendes:

- Aktivierung von WINRM, falls noch nicht aktiv
- Änderung des WINRM-Service, sodass WINRM bei Neustarts automatisch gestartet wird
- Konfiguration des WINRM HTTPS-Listeners
- Änderung der Windows-Firewall-Regeln, um remote angebundene HTTPS-Verbindungen zu ermöglichen

Der Befehl liefert die folgende Ausgabe. Geben Sie **y** ein, um die Änderungen zu bestätigen.

```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for
management.
The following changes must be made:

Create a WinRM listener on HTTPS://* to accept WS-Man requests to
any IP on this machine.
Configure CertificateThumbprint setting for the service, to be
used for CredSSP authentication.
Configure LocalAccountTokenFilterPolicy to grant administrative
rights remotely to local users.
```

```
Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTPS://* to accept WS-Man requests
to any IP on this machine.
Configured required settings for the service.
Configured LocalAccountTokenFilterPolicy to grant administrative
rights remotely to local users.
```

Um schließlich die Authentifizierung von Benutzer-ID/Kennwort über HTTPS zu ermöglichen, führen Sie den folgenden Befehl aus:

```
winrm set winrm/config/service/auth @{Basic="true"}
```

Als Alternative kann ein selbst signiertes Zertifikat verwendet werden. Die Anweisungen für diese Konfiguration befinden sich in Anhang D: Windows mit WINRM auf Seite 53.

Berechtigungsnachweise für die Zugriffsliste:

- Bei dynamischen VMware-Bereichsgruppen: Benutzername/Kennwort für das Servicekonto.
- Bei allgemeinen Erkennungsbereichsgruppen: Computersystem (Windows): Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Mitglied einer der folgenden Gruppen sein:
  - Administratoren
  - WinRMRemoteWMIUsers__

Mit dem folgenden Befehl können Sie einen Benutzer der Gruppe „WinRMRemoteWMIUsers__“ hinzufügen:

```
net localgroup WinRMRemoteWMIUsers__ [user_id] /add
```

Windows über SMB1

Zur Erkennung von Windows-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass der Windows-Scripting-Host (WSH) oder der Windows Management Instrumentation (WMI)-Service und VBScript auf dem Zielgerät aktiviert sind.
- Achten Sie darauf, dass Port 445 nicht durch eine Firewall oder IP-Sicherheitsrichtlinien geblockt ist, da die TSA das Server Message Block (SMBv1)-Protokoll über TCP/IP benötigt.
- Zum Anwenden von Sicherheitsrichtlinien gehen Sie zu **Start → Control Panel → Administrative Tools**. Wählen Sie dann die folgende Navigation aus, je nachdem, ob Ihre Richtlinien lokal oder in einem Active Directory gespeichert sind:

- Lokal gespeicherte Richtlinie: Administrative Tools → Local Security Policy → IP Security Policies on Local Computer
- In Active Directory gespeicherte Richtlinien: Administrative Tools → Default Domain Security Settings → IP Security Policies on Active Directory or Administrative Tools → Default Domain Controller Security Settings → IP Security Policies on Active Directory

- Die TSA erfordert Zugriff auf die verdeckte Remote Administration Disk Share für den Zugriff auf das systemseitige %TEMP%-Verzeichnis und andere Verzeichnisse. Der Zugriff auf die Interprocess Communications Share (IPC$) ist ebenfalls erforderlich, damit die TSA auf Remote-Registrys zugreifen kann. Achten Sie darauf, dass der Interprocess Communication Share Server-Service gestartet wurde. Den Server-Service starten Sie über **Control Panel → Administrative Tools → Services → Server**.
- Stellen Sie sicher, dass der Remote Registry-Service aktiv ist. Dies ist erforderlich, damit die TSA eine Sitzung mit dem Windows-Gerät aufbauen kann.

Berechtigungsnachweise für die Zugriffsliste:

Windows Release 2012 R2 und höher:

- Bei dynamischen VMware-Bereichsgruppen: Basisadministratorkonto/-kennwort. Dieses Konto funktioniert unabhängig von den Einstellungen der Benutzerkontosteuerung (UAC).
- Bei allgemeinen Erkennungsbereichsgruppen: Computersystem (Windows): Basisadministratorkonto/-kennwort. Dieses Konto funktioniert unabhängig von den Einstellungen der Benutzerkontosteuerung (UAC).

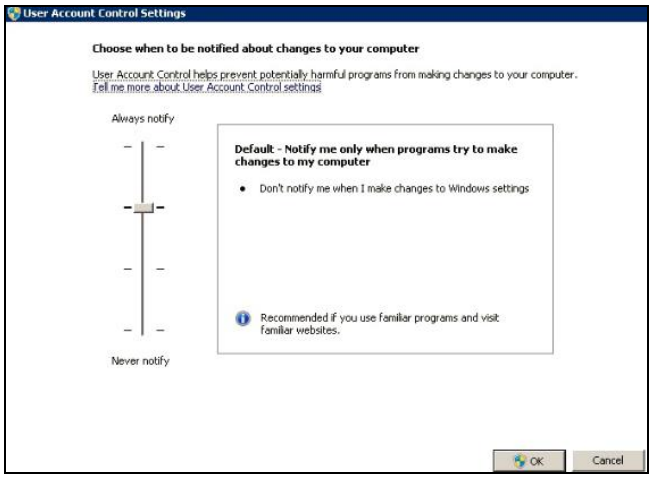
Es ist möglich, ein anderes Konto als das Basisadministratorkonto zu verwenden, wenn bestimmte Bedingungen erfüllt sind. Das Konto muss ein lokales Konto oder Domänenadministratorkonto sein, und die Einstellungen der Benutzerkontensteuerung (UAC) müssen bestimmte Anforderungen erfüllen. In der folgenden Tabelle finden Sie die unterstützten Kombinationen aus Kontotyp und UAC-Einstellung. Weitere Informationen zu UAC finden Sie in der Microsoft Windows-Dokumentation.

	Einstellungen für die Benutzerkontosteuerung			
	Always	**Notify me only**	**Notify me only**	**Never**

	Notify	when programs try to make changes to my computer (Standardeinstellung)	when programs try to make changes to my computer (do not dim my desktop)	Notify
Base Administrator	**Yes**	**Yes**	**Yes**	**Yes**
Benutzer in Domänenadministratorgruppe	**No**	**Yes**	**Yes**	**Yes**
Benutzer in lokaler Administratorgruppe	**No**	**Yes**	**Yes**	**Yes**
Konto für Benutzer ohne Administratorberechtigung (Domäne oder lokal)	**No**	**No**	**No**	**No**

- Für den Zugriff auf die UAC-Einstellungen klicken Sie auf die Schaltfläche **Start** und dann auf **Control Panel**. Geben Sie **uac** im Suchfeld ein, und klicken Sie auf **Change User Account Control settings**.

Nachfolgend finden Sie die Standardeinstellung:



Bankautomaten

Es können bestimmte Bankautomatenmodelle erkannt werden. Führen Sie die folgenden Schritte aus, um die Bankautomaten sowie grundlegende Informationen zu deren Komponenten zu erkennen:

Bereiten Sie die Umgebung vor:

- Wincor Nixdorf-Modelle – Befolgen Sie die Anweisungen für Windows über SMB.

Managementmodul

Bei IBM Flex System ist es am besten, die Iteration durch Hinzufügen von Bereichen und Berechtigungsnachweisen für Entitäten in der folgenden Reihenfolge vorzunehmen:

1. **Flex System Manager (FSM):** Hier werden aussagekräftige Informationen über die Flex System Manager und die von diesen verwalteten Chassis sowie die zugehörigen Rechenknoten zurückgegeben.

   > Wenn keine FSMs vorhanden sind, wird empfohlen, die CMMs und alle HMCs zu scannen, die POWER-Rechenknoten auf Flex-Systemen verwalten.

2. **Chassis Management Module (CMM):** Bei Chassis, die nicht von einem FSM verwaltet werden, zeigen Sie auf jedes CMM, um detaillierte Informationen über jedes Chassis und die zugehörigen Knoten abzurufen.

3. **Rechenknoten:** Hier werden aussagekräftige Informationen über das Betriebssystem zurückgegeben.

Flex System Manager (FSM)-Geräte

Zur Erkennung von FSM-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss die Berechtigung **SMAdmin** haben.

Chassis Management Module (CMM)-Geräte

Zur Erkennung von CMM-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss mindestens die Berechtigung **Operator** haben.

Advanced Management Module (AMM)-Geräte

Zur Erkennung von AMM-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss mindestens die Berechtigung **Operator** haben.

HP Proliant Blade Server über HP OnBoard Administrator

Bei Hewlett Packard (HP) ProLiant Servern ist es am besten, Bereiche und Berechtigungsnachweise für Entitäten von HP OnBoard Administrator (HP OBA) hinzuzufügen. HP OBA gibt aussagekräftige Informationen zu HP OnBoard Administrator, dem von ihm verwalteten Gehäuse und den im Gehäuse enthaltenen Rechenknoten zurück.

Um einen HP Proliant Blade-Server über HP OnBoard Administrator (OBA) zu erkennen, führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- HP OBA muss sich im aktiven Modus befinden.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss die Berechtigung **OA administrator**, **OA operator** oder **OA user** auf dem HP Onboard Administrator aufweisen. Empfohlen wird die Berechtigung **OA user**.

> Die TSA erfasst Informationen nur von HP OnBoard Administratoren, die sich im aktiven Modus befinden. Die TSA erfasst keine Informationen von HP OnBoard Administratoren, die sich im Standby-Modus befinden.

Integrated Management Module (IMM)- & Integrated Management Module II (IMM2)-Geräte

Zur Erkennung von IMM- und IMM2-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.

- Das Servicekonto kann jede gültige Berechtigung aufweisen.

HP Integrity & HP9000 Servers über iLO

iLO ist eine separate Prozessorkarte im HP Integrity & HP9000 Server, die grundlegende Hardware-Informationen über den Server liefert. iLO ist aktiv, sobald der Server aktiviert wird, auch wenn der Server selbst noch nicht eingeschaltet ist.

Zur Erkennung der zusammengefassten Bestandsdaten über iLO für HP Integrity und HP9000 Server führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Berechtigungsstufe haben. Empfohlen wird die Berechtigung „User“.

Dell Server über Integrated Dell Remote Access Controller (iDRAC)

iDRAC ist eine separate Prozessorkarte im Dell Server, die grundlegende Hardware-Informationen über den Server liefert. iDRAC ist standardmäßig inaktiviert und muss aktiviert und konfiguriert werden, um verwendet werden zu können.

Folgende Voraussetzungen müssen erfüllt sein:

- iDRAC muss aktiviert und konfiguriert werden, um verwendet werden zu können.
- Ein iDRAC-Servicemodul muss im Betriebssystem installiert sein, damit die Betriebssysteminformationen erkannt werden können.

Zur Erkennung der zusammengefassten Bestandsdaten über iDRAC für Dell Server führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss mindestens Administratorberechtigung haben.
- Der Berechtigungsnachweis muss SSH-Zugriffsberechtigung zur Ausführung von CLI-Befehlen haben.

Netzgeräte

Dieser Abschnitt enthält detaillierte Informationen zu den folgenden Typen von Netzgeräten:

Plattform
BNT-Switches
Brocade-Switches

Check Point
Cisco-Switches
F5 Big-IP (TMOS)
Fortinet (FortiOS)
IBM Storage Area Network (SAN) Typ B-Switches
Juniper-Switches
Palo Alto Networks (PAN-OS)
QLogic-Switches

Detaillierte Informationen erhalten Sie durch Klicken auf den jeweiligen Link.

BNT-Switches

Zur Erkennung von BNT-Switches führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss die Berechtigung **admin** haben.

Brocade

Zur Erkennung von Brocade-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Virtual Fabric-Modus inaktiviert: Das Servicekonto kann jede gültige Berechtigungsstufe haben. Empfohlen wird die Berechtigung **User**.
- Virtual Fabric-Modus aktiviert: Das Servicekonto benötigt die Berechtigung **Admin** für Fabric OS.

Check Point

Zur Erkennung von Check Point-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung (**adminRole**) haben.

- Das Servicekonto muss SSH-Zugriffsberechtigung zur Ausführung von CLI-Befehlen haben.

Cisco

Zur Erkennung von Cisco-Geräten können Sie die folgenden Computersystem-Berechtigungsnachweise oder SNMP-Berechtigungsnachweise verwenden.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Andere (Cisco Device): Benutzername/Kennwort oder Kennwort und optional Aktivierung der Kennwortauthentifizierung für das Servicekonto.
- Andere (Cisco Works): Benutzername/Kennwortauthentifizierung für das Servicekonto.
- Das Servicekonto erfordert Rollenberechtigungen für **Netzadministratoren**.
- SNMP: Community-Zeichenfolge eingeben (für SNMPv1 und SNMPv2).
- SNMP (SNMPv3):
  - Geben Sie Folgendes ein:
    - Benutzername
    - Kennwort
    - Privates Kennwort (optional)
  - Wählen Sie das Authentifizierungsprotokoll aus: kein, MD5, SHA.

Es ist wichtig, dass der TSA eine einzige Community-Zeichenfolge zur Verfügung gestellt wird, die nur Lesezugriff auf ALLE infrage kommenden Netzgeräte hat.

F5 Big-IP (TMOS)

Zur Erkennung von F5 Big-IP-Systemen, auf denen TMOS läuft, führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Das Servicekonto muss F5-Administratorberechtigung haben.
- Das Servicekonto muss SSH-Zugriffsberechtigung zur Ausführung von TMSH CLI-Befehlen haben.

Fortinet (FortiOS)

Zur Erkennung von Fortinet-Geräten, auf denen FortiOS läuft, führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass die Systemkonsole so konfiguriert ist, dass die gesamte Befehlsausgabe angezeigt wird:

```
config system console
set output standard
end
```

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Das Servicekonto muss mindestens die Berechtigung „Read-only“ haben.

IBM Storage Area Network (SAN) Typ B-Switches

Zur Erkennung von IBM SAN Typ B-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Virtual Fabric-Modus inaktiviert: Das Servicekonto kann jede gültige Berechtigungsstufe haben. Empfohlen wird die Berechtigung **User**.
- Virtual Fabric-Modus aktiviert: Das Servicekonto benötigt die Berechtigung **Admin** für Fabric OS.

Juniper

Zur Erkennung von Juniper-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto
- Das Servicekonto muss Administratorberechtigung haben.

> **Hinweis**: Die Erkennung von Hauptspeichergrößeninformationen erfordert die Installation von Junos® Version 12.1 oder höher auf dem Gerät.

Palo Alto Networks (PAN-OS)

Zur Erkennung von Palo Alto Networks-Systemen, auf denen PAN-OS läuft, führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Superuser- oder Superuser (Lesezugriff)-Berechtigung haben.

- Das Servicekonto muss REST-API-Zugriff (Port 443) haben.

QLogic-Switches

Zur Erkennung von QLogic-Switches führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung haben.

Speichergeräte

Dieser Abschnitt enthält detaillierte Informationen zu den folgenden Typen von Speicher- und Bandgeräten:

Plattform
EMC Corporation-Speicher
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx, DS4xxx oder DS5xxx
IBM DS6xxx oder DS8xxx
IBM FlashSystem, v9000
IBM ProtecTier
IBM SVC oder V7000/V3700
IBM TS3100-Bandarchiv
IBM TS3200-Bandarchiv
IBM TS3310-Bandarchiv
IBM TS3494, TS3953-Bandarchive
IBM TS3500, TS3584-Bandarchive
IBM TS4300-Bandarchiv
IBM TS4500-Bandarchiv
IBM TS7700-Bandarchiv
IBM V7000 Unified
IBM XIV

Plattform
nSeries oder NetApp

- Detaillierte Informationen erhalten Sie durch Klicken auf den jeweiligen Link.

EMC Corporation-Speicher

EMC CLARiiON/VNX/VMAX

Zur Erkennung von EMC CLARiiON-, VNX-, VMAX-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass eine Instanz des EMC SMI-S-Provider-Produkts auf einem Windows- oder Linux-System installiert ist. Standardmäßig folgt die TSA der Empfehlung von EMC SMI-S, den Standort des Providers mithilfe von SLP zu ermitteln. Wenn Ihre Netzsicherheitsrichtlinie den SLP-Netzverkehr blockiert, kann die TSA so konfiguriert werden, dass der direkte Zugriff auf den EMC SMI-S-Provider ohne die Verwendung von SLP möglich ist.
- Wenn Ihre Netzsicherheit keinen SLP-Netzverkehr zulässt, stellen Sie mithilfe der Seite **Erkennungseinstellungen → Verbindungseinstellungen** Informationen dazu bereit, welche Ports die EMC SMI-S-Provider bei Abfrageanforderungen überwachen.
- Stellen Sie sicher, dass mindestens eine der IP-Adressen, die der SMI-S-Provider verwendet, in einer Bereichsgruppe definiert ist. Die TSA stellt eine Verbindung zum SMI-S-Provider her, um Informationen zu den von ihr verwalteten EMC-Geräten abzurufen. Die IP-Adressen der einzelnen EMC-Geräte müssen nicht in einer Bereichsgruppe hinterlegt werden. Die TSA versucht, eine Verbindung zum SMI-S-Provider über HTTPS (falls verfügbar) oder andernfalls über HTTP herzustellen.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Rolle haben. Empfohlen wird die Rolle **monitor**.

- In der TSA müssen nur die Berechtigungsnachweise für den SMI-S-Provider eingegeben werden. Es müssen keine Berechtigungsnachweise für die EMC-Geräte eingegeben werden.

EMC Data Domain

Zur Erkennung von EMC Data Domain-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Berechtigung aufweisen. Es wird empfohlen, die niedrigste Berechtigungsstufe zu verwenden.

HP StorageWorks P2000 Modular Smart Array

Zur Erkennung von HP Speichersystemen führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Berechtigung aufweisen. Es wird empfohlen, die niedrigste Berechtigungsstufe zu verwenden.

IBM DS3xxx-, DS4xxx- oder DS5xxx-Speicher

Zur Erkennung von IBM DS3xxx-, DS4xxx- oder DS5xxx-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass der Speichermanager die Verwendung von **smcli**-Remotebefehlen erlaubt.

Berechtigungsnachweise für die Zugriffsliste:

- Für nicht gesicherte Speichergeräte sind keine Berechtigungsnachweise erforderlich.
- Führen Sie für gesicherte Speichergeräte die folgenden Schritte durch:
  - Computersystem: Benutzername/Kennwort für das Servicekonto.
  - Das Servicekonto kann entweder **admin**- oder **monitor**-Berechtigungen haben. Empfohlen wird **monitor**.

IBM DS6xxx-/DS8xxx-Speicher

Zur Erkennung von IBM DS6xxx-/DS8xxx-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass der Speichermanager die Verwendung von **dscli**-Remotebefehlen erlaubt.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss die Rollenberechtigung **monitor** haben.

IBM FlashSystem, v9000

Zur Erkennung von IBM FlashSystem-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Bei alten Modellen muss sich der MCP (Management Control Port) im aktiven Status befinden, um das System erfolgreich erkennen zu können.
  - Um zu überprüfen, ob sich ein System im aktiven Status befindet, führen Sie den folgenden Befehl aus: `system status`.
  - Wenn eine der beiden IP-Adressen ausfällt, geht das System in den passiven Status über. Um den anderen Ethernet-Port in den aktiven Status zu setzen, führen Sie den Befehl `sync activate` aus.
  - Bei dem erkannten System muss es sich um die Management-IP-Adresse und/oder den Konfigurationsknoten handeln.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüsselauthentifizierung für das Servicekonto.
- Das Servicekonto kann jede gültige Rolle haben. Empfohlen wird die Rolle **monitor**.

IBM ProtecTIER

Zur Erkennung von ProtecTIER-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung haben.

IBM SVC, V7000/V3700-Speicher

Zur Erkennung von SVC- und V7000-/V3700-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort oder Benutzername/SSH-Schlüssel für die Authentifizierung.
- Das Servicekonto kann jede gültige Rolle haben. Empfohlen wird die Rolle **monitor**.

IBM TS3100-Bandarchiv

Zur Erkennung von TS3100-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.

- Das Servicekonto muss Administratorberechtigung haben.

IBM TS3200-Bandarchiv

Zur Erkennung von TS3200-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung haben.

IBM TS3310-Bandarchiv

Zur Erkennung von TS3310-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Der Web-Service wird immer im sicheren Modus konfiguriert.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung haben.

IBM TS3494-, TS3953-Bandarchive

Zur Erkennung von TS3494-, TS3953-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Für das Servicekonto reicht die erforderliche Mindestberechtigung aus.

IBM TS3500-, TS3584-Bandarchive

Folgende Voraussetzungen müssen erfüllt sein:

- Das TS3500-Bandarchiv muss Firmwareversion 8xxx (oder höher) aufweisen.
- Das Advanced Library Management System (ALMS) muss installiert und aktiviert sein.

> Sowohl SSL- als auch andere Verbindungen werden unterstützt.

Zur Erkennung von TS35xx-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Die TS3500-Webschnittstelle kann für **Kein Kennwortschutz** oder **Kennwortschutz** konfiguriert werden.
  - Wenn der **Kennwortschutz** aktiviert ist, erstellen Sie einen Berechtigungsnachweis wie in **Berechtigungsnachweise für die Zugriffsliste** unten beschrieben.

- Wenn der **Kennwortschutz** inaktiviert ist, sind keine Berechtigungsnachweise erforderlich.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss Administratorberechtigung haben.

IBM TS4300-Bandarchiv

Folgende Voraussetzungen müssen erfüllt sein:

- Beim TS4300-Bandarchiv muss die Rest-API an Port 3031 über HTTPS aktiviert werden.

Zur Erkennung von TS43000-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss mindestens die Berechtigungsstufe **Service** aufweisen.
- Der Berechtigungsnachweis muss Zugriff auf die REST-API an Port 3031 über HTTPS haben.

IBM TS4500-Bandarchiv

Folgende Voraussetzungen müssen erfüllt sein:

- Das TS4500-Bandarchiv muss Firmwareversion 1.4.1.2 oder höher (bis zu 1.7.0.0) aufweisen.
- Das Advanced Library Management System (ALMS) muss installiert und aktiviert sein.

Sowohl SSL- als auch andere Verbindungen werden unterstützt.

Zur Erkennung von TS4500-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Die TS4500-Webschnittstelle kann so konfiguriert werden, dass Benutzername/Kennwort erforderlich ist. Sie kann auch so konfiguriert werden, dass keine Benutzername-/Kennwortkombination erforderlich ist.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto ist nur erforderlich, wenn das TS4500-Bandarchiv so konfiguriert ist, dass Anmeldeberechtigungsnachweise erforderlich sind.

- Dem Servicekonto muss die Rolle **Service** zugeordnet sein.

IBM TS7700-Bandarchiv

Zur Erkennung von TS7700-Bandarchivgeräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto benötigt nur die Berechtigung **Read-Only** (Lesezugriff).

IBM V7000 Unified-Speicher

Zur Erkennung von V7000 Unified-Geräten führen Sie die folgenden Schritte durch:

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Rolle haben. Empfohlen wird die Rolle **monitor**.

IBM XIV-Speicher

Zur Erkennung von XIV-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Stellen Sie sicher, dass der Speichermanager die Verwendung von **xcli**-Remotebefehlen erlaubt.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto muss die Rollenberechtigung **read-only** (Lesezugriff) haben.
- Beachten Sie, dass XIV-Systeme einen niedrigeren unteren Schwellenwert für ungültige Anmeldeversuche haben können, bevor sie Alerts generieren. Wenn Sie einen großen Berechtigungsnachweissatz verwenden, überschreiten Sie möglicherweise diesen Grenzwert und verursachen so unnötige Probleme, die gemeldet werden müssen. Versuchen Sie, die XIV-Geräte in einer einzigen Bereichsgruppe zu gruppieren und ihre Servicekontoberechtigungsnachweise auf diese Bereichsgruppe zu beschränken.

nSeries- oder NetApp-Speicher

Zur Erkennung von nSeries- oder NetApp-Geräten führen Sie die folgenden Schritte durch:

Bereiten Sie die Umgebung vor:

- Die Datenerfassung wird für Systeme unterstützt, die mit der datenspezifischen ONTAP CLI, RLM CLI und SP CLI konfiguriert wurden. Die BMC CLI wird nicht unterstützt.

- Die Option **telnet.distinct.enable** muss aktiviert sein.

Berechtigungsnachweise für die Zugriffsliste:

- Computersystem: Benutzername/Kennwort für das Servicekonto.
- Das Servicekonto kann jede gültige Berechtigung aufweisen. Es wird empfohlen, die niedrigste Berechtigungsstufe zu verwenden.

Überlegungen zu Firewalls

Firewall(s) zwischen der Appliance und den Erkennungsgeräten können eine vollständige und erfolgreiche Erkennung verhindern.

In Fällen, in denen eine Firewall überwunden werden muss, müssen eventuell Ports in der Firewall geöffnet werden, je nach Art des Geräts, das der Benutzer erkennen will. Typischerweise sollten die Ports 22 (SSH) und 161 (SNMP) geöffnet werden, gefolgt von den entsprechenden Ports in der folgenden Tabelle basierend auf den unterstützten Geräten.

Erkennungsendpunkt	**Ports**	**Schnittstelle/Protokoll**
Mehrere	161	SNMP
Speichergeräte		
DS6000/DS8000	1750 (HTTP) oder 1751 (HTTPS)	DSCLI
DS3000/DS4000/DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries oder NetApp	22/23	SSH oder Telnet
SVC oder V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3100/TS3200	80	HTTP
IBM TS3310	80	HTTP
IBM TS3500	443/80	HTTPS oder HTTP
IBM TS4300	3031	HTTPS (an Port 3031)
IBM TS4500	443/80	HTTPS oder HTTP
IBM TS7700	443/80	HTTPS oder HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Speicher	22/23	SSH oder Telnet
IBM Flash System, v9000	22	SSH

Erkennungsendpunkt	Ports	Schnittstelle/Protokoll
EMC Corporation-Speicher – CLARiion/VNX/VMAX	427 – (Standard), wenn die SLP-Erkennung zulässig ist; andernfalls wird dieser Port nicht verwendet, wenn die SLP-Erkennung inaktiviert ist. Vom EMC SMI-S-Provider konfigurierte HTTPS-/HTTP-Ports; die Standardwerte sind 5989/5988.	SLP, HTTPS/HTTP
	Sie können die SLP-Erkennungsoption aktivieren oder inaktivieren, um EMC-Speichergeräte über EMC SMI-S-Provider zu erkennen.	
EMC Corporation-Speicher – EMC Data Domain	22	SSH*
Betriebssysteme und Hosts		
FSM	22/23	SSH oder Telnet
CMM	22/23	SSH oder Telnet
AMM	22/23	SSH oder Telnet
HP Proliant Blade-Server über HP OnBoard Administrator	22/23	SSH oder Telnet
IMM und IMM2	22/23	SSH oder Telnet
HP iLO für die HP Integrity/HP 9000 Server	22/23	SSH* oder Telnet
Dell iDRAC	22/23	SSH oder Telnet
Netzgeräte		
Brocade	161/22/23	SNMP, SSH, Telnet
IBM Storage Area Network (SAN) Typ B-Switches	22/23	SSH, Telnet
Cisco	161/22/23	SNMP, SSH, Telnet
BNT	22/23	SSH oder Telnet
Juniper	22/23	SSH oder Telnet

Erkennungsendpunkt	Ports	Schnittstelle/Protokoll
QLogic	22/23	SSH* oder Telnet
Fortinet (FortiOS)	22/23	SSH oder Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22/23	SSH oder Telnet
Check Point	22/23	SSH oder Telnet
Betriebssysteme/Serverplattformen		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443, 5989	HTTPS
IVM	22/23	SSH oder Telnet
IBM i	22	SSH
SUN	22	SSH

- Die TSA unterstützt nur SSH v1 für die Geräte, die mit SSH* gekennzeichnet sind.

Erkennungsprobleme

Die meisten Erkennungsprobleme sind auf Zugriffs- oder Berechtigungsprobleme zurückzuführen.

Die häufigsten Zugriffsprobleme sind auf Firewalls zurückzuführen, die den Zugang zu den notwendigen Ports auf dem Gerät blockieren. Die Ports, die offen und erreichbar sein müssen, variieren je nach Gerätetyp. Im Abschnitt „Überlegungen zu Firewalls“ auf Seite 43 können Sie bestimmen, welche Ports anwendbar sind.

Zu den häufigsten Berechtigungsproblemen gehören die folgenden:

- **Keine Berechtigungsnachweise definiert**. Stellen Sie sicher, dass die Berechtigungsnachweise für die Geräte in der TSA definiert sind und die entsprechenden Servicekonten auf den Geräten erstellt wurden.
- **Benutzername oder Kennwort für den Berechtigungsnachweis falsch**. Verwenden Sie beim Erstellen oder Bearbeiten eines Berechtigungsnachweises die **Testfunktion**, um zu überprüfen, ob der Berechtigungsnachweis gültig ist.
- **Berechtigungsnachweiskennwort abgelaufen**.
- **Für den Berechtigungsnachweis fehlen die erforderlichen Berechtigungen auf dem Gerät**. Die Berechtigungsnachweisanforderungen für ein Zielgerät können Sie im Abschnitt Geräteerkennungskonfiguration auf Seite 12 ermitteln.
- **Verwendung eines gültigen Berechtigungsnachweistyps**. Erstellen Sie für Windows-Geräte einen „Computersystem (Windows)“-Berechtigungsnachweis und keinen „Computersystem“-Berechtigungsnachweis.

Überprüfen Sie die Seite **Authentifizierungsstatus (Tools → Authentifizierungsstatus)**, um zu sehen, ob bei Berechtigungsnachweisen für ein Servicekonto Kennwörter abgelaufen sind oder ob sie nicht mehr funktionieren.

Überlegungen zu fortlaufenden Aktivitäten

Nachdem die gewünschten Netzbereiche in der TSA definiert und erfolgreich gescannt wurden, kann die TSA periodische Erkennungen und Übertragungen nach den gewünschten Zeitplänen durchführen.

Im Folgenden sind einige erwartete laufende Aktivitäten aufgeführt:

- Überprüfen Sie die von der TSA erstellten Berichte in regelmäßigen Abständen zusammen mit Ihrem IBM Ansprechpartner.
- Führen Sie regelmäßig eine Sicherung über die TSA-Benutzerschnittstelle durch, um eine Kopie der TSA-Konfiguration zu speichern.

Bei diesem Vorgang werden keine von der TSA erfassten Daten gespeichert. Es werden nur die Konfigurationsdaten gespeichert.

- Überprüfen Sie in regelmäßigen Abständen die Seite **Authentifizierungsstatus (Tools → Authentifizierungsstatus)**, um zu sehen, ob bei Berechtigungsnachweisen für ein Servicekonto Kennwörter abgelaufen sind oder ob sie nicht mehr funktionieren.
- Wenn die Kennwörter für die Servicekonten auf den Geräten aktualisiert werden, stellen Sie sicher, dass auch die Kennwörter in der TSA aktualisiert werden, um die Berechtigungsnachweisdefinition in der TSA mit dem Berechtigungsnachweis auf dem Zielgerät synchron zu halten.
- Wenn Ihre Sicherheitsrichtlinie es zulässt, sollten Sie die Einrichtung von Servicekonten mit nicht ablaufenden Kennwörtern in Betracht ziehen oder SSH-Schlüssel verwenden. Dadurch entfällt die Notwendigkeit, die Kennwörter in der TSA-Benutzerschnittstelle und auf den Geräten periodisch zu aktualisieren.

Fehlerbehebung

Aktive Sitzung für AMM-Erkennung

AMM-Geräte haben eine Einstellung, die die Anzahl der gleichzeitig aktiven Sitzungen begrenzt (maximal 20). Wenn diese Einstellung nicht hoch genug ist, damit die TSA eine Sitzung erstellen kann, kann das AMM-Gerät nicht erkannt werden.

Um die Begrenzung der aktiven Sitzungen für ein AMM-Geräts zu ändern, führen Sie folgende Schritte aus:

1. Melden Sie sich bei der AMM-Webschnittstelle an, indem Sie die IP-Adresse des AMM-Geräts in einem Web-Browser eingeben.
2. Gehen Sie zu **MM Control → Login Profiles**.
3. Klicken Sie auf die von der TSA verwendete Anmelde-ID, um das Gerät zu erkennen.
4. Erhöhen Sie den Einstellungswert für **Maximum simultaneous active sessions**.
5. Klicken Sie auf **Save** in der rechten unteren Ecke der Seite.

Anhang A: Begriffe und Definitionen

Es wird davon ausgegangen, dass die Leser über ein umfassendes Verständnis der Internet Protocol (IP)-Netze und -Protokolle verfügen.

Begriff	**Definition**
Erkennungsgerät	Dieser Begriff bezieht sich auf implementierte IT-Infrastrukturkomponenten, die von der TSA erkannt werden können. Typische Geräte sind Server, Computersysteme (z. B. IBM, Dell und HP), Speicherelemente und Netzelemente (z. B. Switches, Bridges, Router).

Anhang B: Sonstiges

Downloadfunktionen der Benutzerschnittstelle

Wenn ein Web-Browser verwendet wird, werden in einigen Fällen die Option „Alle Protokolle herunterladen“ (auf der Seite **Aktivitätenprotokoll**) oder die Dateidownloads (über die Seite **Erkennungsverlauf**) nicht erfolgreich abgeschlossen. Um dieses Problem zu beheben, versuchen Sie, zu einem anderen unterstützten Web-Browser zu wechseln, wie im IBM Technical Support Appliance-Installationshandbuch beschrieben. Wenn das keine Option ist, versuchen Sie, die Eigenschaften Ihres Browsers auf die Standardeinstellungen zurückzusetzen.

Anhang C: CIM-Provider für VMware ESXi

Ein CIM-Provider setzt sich aus mehreren VMware ESXi-Plugins zusammen, die zusätzliche Hardware- und Firmwareinformationen über den Server erfassen können, auf dem VMware ESXi ausgeführt wird.Sowohl die TSA als auch VMware vCenter können von diesen zusätzlichen Informationen profitieren.

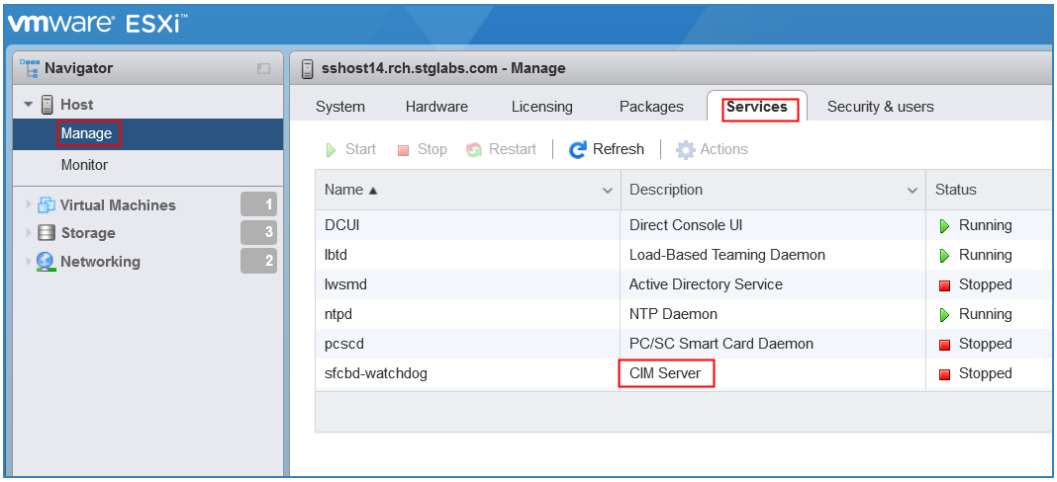
CIM-Provider-Plugins werden von den Server- und Komponentenherstellern entwickelt. Um sicherzustellen, dass CIM-Provider-Plugins in ESXi enthalten sind, verwenden Sie ein angepasstes Installationsimage, in dem die CIM-Provider-Plugins enthalten sind. Für vorhandene VMware ESXi-Instanzen, auf denen der CIM-Provider nicht installiert ist, beziehen Sie die erforderlichen Plugins von den Server- und Komponentenherstellern und installieren sie in ESXi. VMware bietet eine Liste der verschiedenen Plugins, die von den Herstellern zur Verfügung gestellt werden.

Weitere Informationen finden Sie unter https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

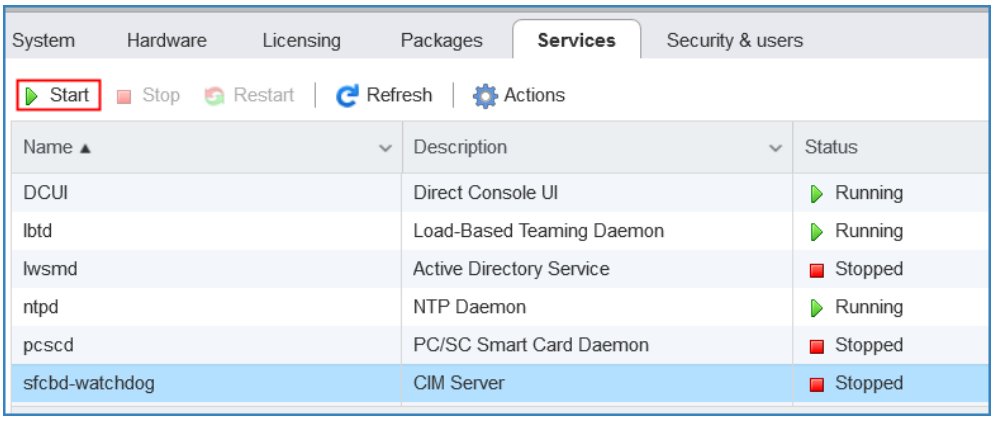
Wenn Sie feststellen wollen, ob der CIM-Provider aktiv ist, und zum Aktivieren eines inaktiven CIM-Providers führen Sie die folgenden Schritte durch.

Gehen Sie im VMware vSphere Web Client wie folgt vor:

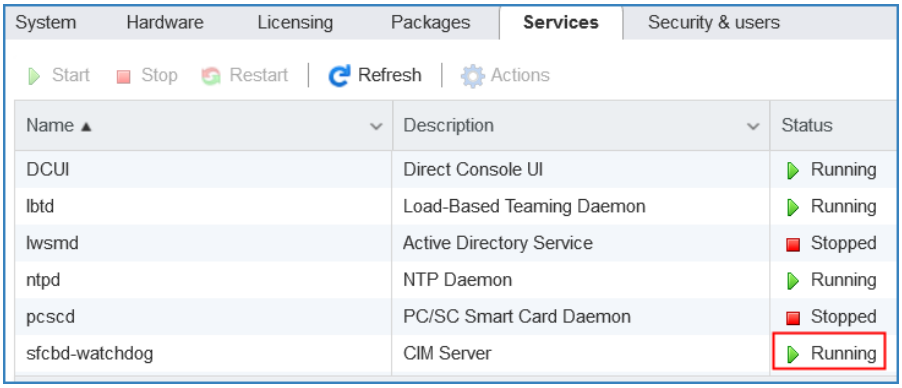
- Melden Sie sich beim VMware vSphere Web Client an.
- Klicken Sie im linken Navigationsfenster auf **Host → Manage** und wählen Sie im rechten Teilfenster die Registerkarte **Services** aus.
- Eine Reihe von Services wie **CIM Server** werden angezeigt.



- Wenn sich der **CIM-Server** im Status **Stopped** befindet, wählen Sie den Server aus und klicken auf die Schaltfläche **Start**.



- Der CIM-Server-Service wird gestartet, und der Status lautet jetzt **Running**.



Anhang D: Windows mit WINRM

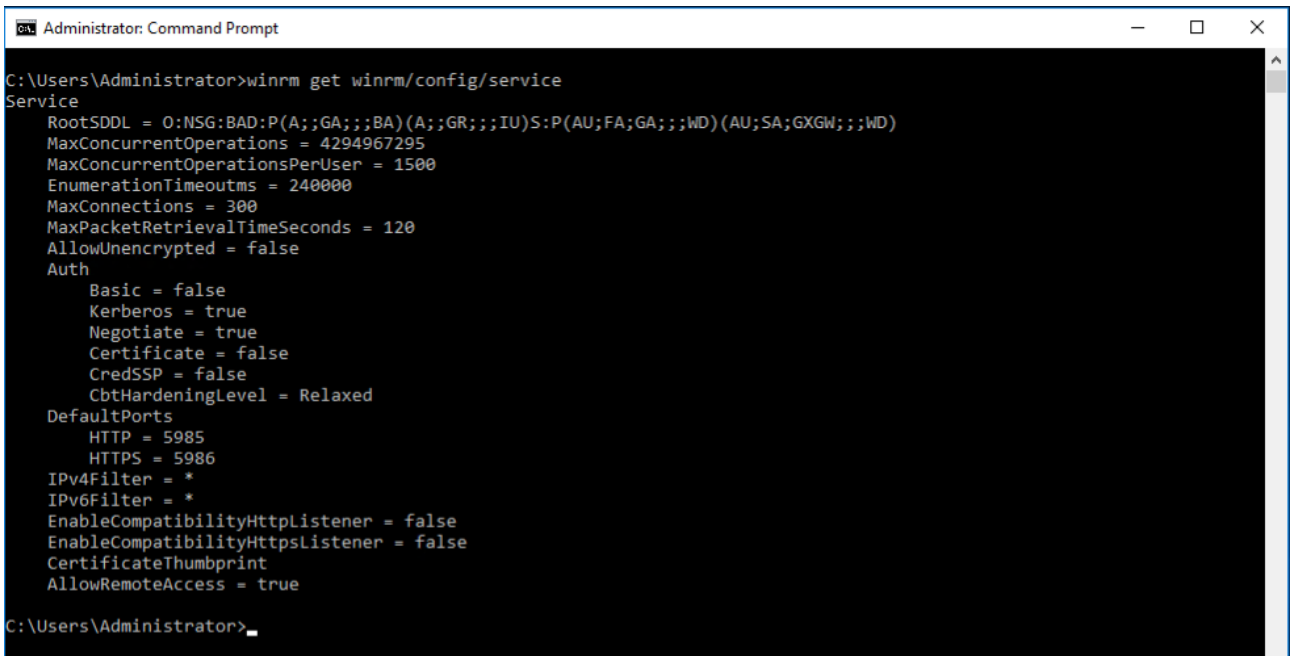
Bei Windows 2012 Server, 2016 Server und 2019 Server wird der WINRM-Service automatisch gestartet. Die Fernverwaltung ist jedoch nicht standardmäßig aktiviert. Dies ist ein kurzer Überblick über die Voraussetzungen, dass WINRM mithilfe eines selbst signierten Zertifikats Fernverbindungen zulassen kann:

- Ermöglichen Sie WINRM, HTTPS-Verbindungen zu akzeptieren, bei denen die Authentifizierung mit Benutzer-ID und Kennwort erfolgt.
- Verknüpfen Sie ein selbst signiertes Zertifikat mit dem aktivierten HTTPS-Listener für WINRM.
- Ändern Sie die Windows-Firewall, um eingehende Verbindungen über Port 5986 (den WINRM HTTPS-Standardport) zuzulassen.

Mit den folgenden Befehlen wird WINRM darauf vorbereitet, Fernverbindungen über HTTPS zuzulassen:

- Ermitteln Sie mit diesem Befehl den aktuellen Status des WINRM-Service:

  winrm get winrm/config/service



- Der Wert für **AllowUnencrypted** muss *false* lauten. Ist der Wert auf *true* festgelegt, ändern Sie ihn mit dem folgenden Befehl in *false*:

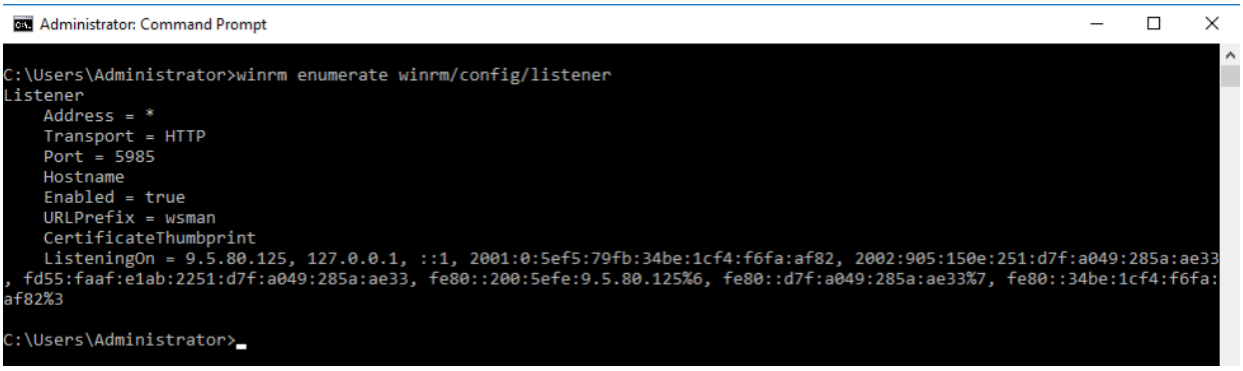
  winrm set winrm/config/service @{AllowUnencrypted="false"}

- Der Wert für **Basic** muss *true* lauten. Ist der Wert auf *false* festgelegt, ändern Sie ihn mit dem folgenden Befehl in *true*:

  winrm set winrm/config/service/auth @{Basic="true"}

- Ermitteln Sie mit diesem Befehl, ob WINRM einen HTTPS-Listener hat:

  winrm enumerate winrm/config/listener

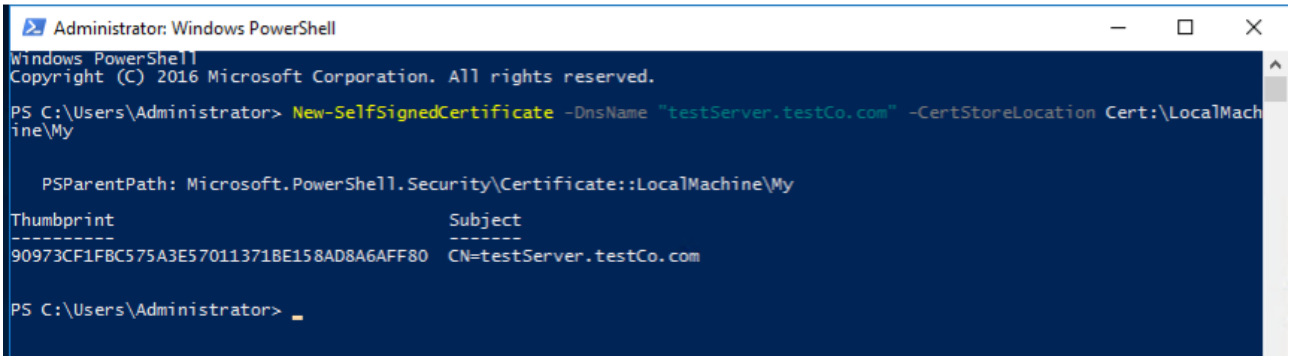


- Im Befehlsbeispiel oben existiert nur ein HTTP-Listener, sodass ein HTTPS-Listener konfiguriert werden muss. So aktivieren Sie den HTTPS-Listener, wenn er nicht konfiguriert ist:
  - Erstellen Sie mit PowerShell ein selbst signiertes Zertifikat:

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > Ersetzen Sie DnsName **(myHost@myBusiness.com)** im Beispiel durch den vollständig qualifizierten Windows-Domänennamen für den Windows-Server.

  - Speichern Sie den Zertifikatsfingerabdruck für den nächsten Schritt.



- Erstellen Sie den HTTPS-Listener:

  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}

- Überprüfen Sie, ob HTTPS nun konfiguriert ist:

  winrm enumerate winrm/config/listener

- Ändern Sie die Windows-Firewall, um eingehende Fernverbindungen zu WINRM zu ermöglichen:
  - Wechseln Sie zu Control Panel → System and Security → Windows Firewall.
  - Klicken Sie auf „Advanced Settings“. Das Fenster „Firewall with Advanced Security“ wird angezeigt.
  - Klicken Sie auf „Inbound Rules“.
  - Wählen Sie das Menü „Actions“ aus und klicken Sie auf „New Rule“. Der „New Inbound Rule Wizard“ wird angezeigt.
  - Wählen Sie **Port** aus und klicken Sie auf **Next**.
  - Wählen Sie **TCP → Specific local ports** aus und geben Sie 5986 an. Klicken Sie auf **Next.**
  - Wählen Sie die Option **Allow the connection** aus und klicken Sie auf **Next.**
  - Wählen Sie die Kontrollkästchen **Domain**, **Private** und **Public** aus, wenn diese noch nicht markiert wurden, und klicken Sie auf **Next**.
  - Geben Sie der neuen Regel einen Namen (z. B. Windows Remote Management (HTTPS-In)) und klicken Sie auf **Finish.**

Bemerkungen

IBM Deutschland GmbH IBM-Allee
1 71139 Ehningen ibm.com/de
IBM Österreich Obere Donaustrasse
95 1020 Wien ibm.com/at
IBM Schweiz Vulkanstrasse 106 8010
Zürich ibm.com/ch

Januar 2021.

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem US-amerikanischen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an.

Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich.

Jegliche Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

IBM, das IBM Logo, POWER, System i, System p, i5/OS sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter http://www.ibm.com/legal/copytrade.shtml.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

IBM Hardwareprodukte sind aus fabrikneuen Teilen oder aus neuen und gebrauchten Teilen hergestellt. Unabhängig davon gelten die jeweiligen Bestimmungen zum Herstellerservice von IBM.

Dieses Produkt unterliegt den FCC-Vorschriften. Das Produkt wird auf die Einhaltung der entsprechenden FCC-Vorschriften geprüft, bevor es endgültig an den Käufer ausgeliefert wird.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte.

Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die IBM Homepage finden Sie im Internet unter http://www.ibm.com.

Die IBM System p-Homepage finden Sie im Internet unter http://www.ibm.com/systems/p.

Die IBM System i-Homepage finden Sie im Internet unter http://www.ibm.com/systems/i.

PSW03007-DEDE-00