Version 2.8.0.0

Technical Support Appliance Installationshandbuch

Hinweis

Lesen Sie vor der Verwendung dieser Informationen und des darin beschriebenen Produkts die Informationen unter „Bemerkungen” auf Seite 143.

24. Ausgabe (Januar 2021)

Diese Ausgabe bezieht sich auf Version 2, Release 8, Modifikation 0 der IBM® Technical Support Appliance und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1. Einführung

Die Technical Support Appliance (TSA) ist ein benutzerfreundliches Tool, das Ihnen hilft, den Nutzen Ihrer IBM Supportverträge zu steigern. Die TSA erkennt wichtige IT-Elemente und deren Beziehungen innerhalb Ihrer IT-Infrastruktur und überträgt die Daten sicher an den IBM Support zur Analyse. Diese Daten geben dem IBM Support Einblick in die komplexen Beziehungen zwischen Anwendungen, Middleware, Servern und Netzkomponenten in Ihrem Rechenzentrum.

Die TSA beinhaltet eine webbasierte Benutzerschnittstelle (UI) zum Einrichten und Anpassen des Zugriffs auf Ihr System und Ihre Daten. Über diese Schnittstelle können Sie auch Zeitpläne für die Datenerkennung und -übertragung ändern.

Im Rahmen des Erkennungsprozesses versucht die TSA zunächst, Endpunkte innerhalb des definierten Bereichs ohne Verwendung von Berechtigungsnachweisen zu erkennen. Mithilfe von Nmap wird versucht, Geräte durch minimal intrusives Scannen von IP-Adressen, durch Stack-Fingerprinting und durch Portzuordnung zu erkennen und zu klassifizieren. Im Allgemeinen ist diese Aktivität nicht signifikant genug, um ein Intrusion Detection System (IDS) auszulösen. Bei sehr strikten lokalen Einstellungen kann dies gelegentlich dennoch geschehen.

Mit den allgemeinen Bereichsgruppen können Sie einzelne IT-Netzelemente erkennen. Die Bereichsgruppe enthält einen oder mehrere Bereiche, die den Standort dieser Netzelemente unter Verwendung einer IP-Adresse oder eines Hostnamens, eines Bereichs von IP-Adressen oder eines Netzes oder Teilnetzes identifiziert.

Für HMCs und VMware vCenter-Server/ESXi wird die Verwendung dynamischer Bereichsgruppen empfohlen. Dynamische Bereichsgruppen erfordern weit weniger Konfigurationsaufwand in TSA als das Erstellen und Verwalten von Erkennungsbereichen für einzelne LPARs/virtuelle Maschinen. Auch für Umgebungen, in denen die LPARs oder virtuellen Maschinen im Lauf der Zeit hinzugefügt und gelöscht werden, können dynamische Bereichsgruppen dies ohne die Notwendigkeit, Bereichsgruppen zu ändern, handhaben.

Benutzerkonten und Benutzergruppen

Die Ausführung einer TSA-Funktion setzt eine bestimmte Berechtigungsstufe voraus. Wenn ein authentifizierter Benutzer versucht, eine Funktion auszuführen, ohne über die erforderliche Berechtigungsstufe zu verfügen, wird ein Fehler angezeigt und die Ausführung der Funktion verhindert.

In einem Unternehmen können Rollen für diverse Jobfunktionen angelegt werden. Die Berechtigung zur Ausführung bestimmter Operationen wird rollenspezifisch erteilt. TSA-Benutzern werden spezifische Rollen zugewiesen, und durch diese Rollenzuweisung erhalten sie die erforderlichen Berechtigungen zur Ausführung einzelner Systemfunktionen. Somit besitzt jeder Benutzer, dem eine Rolle zugewiesen ist, die Berechtigungsstufen, die zu dieser Rolle gehören. Auf diese Weise wird es sehr einfach, einem Benutzer eine Rolle zuzuordnen sowie Rollenzuweisungen zu ändern oder aufzuheben.

In der TSA werden Rollen als Benutzergruppen mit bestimmten Berechtigungsstufen verwaltet. Benutzer werden dagegen mithilfe von Benutzerkonten verwaltet. Benutzerkonten kann die Mitgliedschaft in einer oder mehreren Benutzergruppen zugeordnet werden, wodurch sie die Berechtigungsstufe zur Ausführung bestimmter Funktionen erhalten.

Benutzergruppen können auch auf ausgewählte Bereichsgruppen beschränkt werden. Eine Bereichsgruppe ist eine Gruppe von IP-Adressen oder Hostnamen, Adressbereichen oder Teilnetzen, durch die festgelegt wird, welche IT-Elemente die TSA erkennen kann. Durch Festlegung von Bereichsgruppenbeschränkungen für eine Benutzergruppe kann der Zugriff für die Mitglieder dieser Benutzergruppe weiter eingeschränkt werden. Beispielsweise lassen sich durch eine Kombination aus Berechtigungsstufe und Bereichsgruppenbeschränkungen für eine bestimmte Benutzergruppe plattformspezifische Benutzergruppen erstellen, z. B. Benutzer, die für die Instandhaltung von Linux®-Systemen zuständig sind.

Erkennungsbereiche und Bereichsgruppen

Durch Erkennungsbereiche wird festgelegt, welche Ressourcen die TSA erkennen soll. Die Erkennungsbereiche sind in Erkennungsbereichsgruppen gegliedert.

Erkennungsbereiche werden durch eine IP-Adresse oder einen Hostnamen, einen IP-Adressbereich oder ein Netz bzw. Teilnetz definiert, das die Ressourcen enthält, auf die bei der Erkennung zugegriffen wird. Ein Erkennungsbereich kann auf eine einzelne IP-Adresse/einen Hostnamen oder einen Bereich von IP-Adressen begrenzt sein oder ein ganzes Netz umfassen.

Um die Erstellung einer Bereichsgruppe zu vereinfachen, können Sie eine Datei mit einer Liste von IP-Adressen und Hostnamen importieren. Weitere Informationen hierzu finden Sie im Abschnitt „Bereichsgruppe importieren” auf Seite 75.

Je mehr IP-Adressen ein Erkennungsbereich umfasst, desto länger dauert der Erkennungsprozess. Sie können die Erkennungsgröße ändern, indem Sie Erkennungsbereichsgruppen inaktivieren oder aktivieren oder indem Sie IP-Adressen, IP-Adressbereiche oder Netze bzw. Teilnetze aus einem Bereich innerhalb eines Bereichs ausschließen.

Anmerkung: Zur Optimierung des Leistungsverhaltens empfiehlt es sich, die Gesamtzahl von IP-Adressen (IP-Adressen, Bereiche, Teilnetze und Ausschlüsse) in einer Bereichsgruppe auf maximal 400 zu begrenzen.

Anmerkung: Bei Bereichen oder Importlisten, die mit Hostnamen definiert sind, wird der Hostname in eine IP-Adresse aufgelöst, wenn der Bereich erstellt oder bearbeitet wird. TSA verwendet bei der Erkennung von Netzressourcen nicht den Hostnamen.

Zugehörige Tasks

Benutzerkonten und Benutzergruppen hinzufügen
Sie können Benutzerkonten und -gruppen hinzufügen, um den Zugriff auf TSA-Funktionen zu steuern.

Erkennungsberechtigungsnachweise

Erkennungsberechtigungsnachweise sind eine Sammlung von Benutzernamen, Kennwörtern oder SSH-Schlüsseln sowie SNMP-Community-Zeichenfolgen (Simple Network Management Protocol), die die TSA für den Zugriff auf Ressourcen während der Erkennung verwendet.

Sie müssen Erkennungsberechtigungsnachweise für alle Ressourcen einrichten und verwalten, die Sie in die Erkennung einbeziehen möchten. Die anzugebenden Zugriffsinformationen sind je nach Typ des Berechtigungsnachweises unterschiedlich, beinhalten aber in der Regel zumindest Benutzernamen und Kennwort oder einen SSH-Schlüssel.

Ein Erkennungsberechtigungsnachweis kann für alle Bereichsgruppen gelten oder auf eine einzelne Bereichsgruppe beschränkt sein. Durch die Definition von Berechtigungsnachweisen, die nur für eine einzelne Bereichsgruppe gelten, können Sie das Leistungsverhalten verbessern und ungültige Anmeldeversuche verhindern, die zu einer Sperrung des Kontos führen können.

Beim Zugriff auf eine Ressource verwendet die TSA nacheinander alle Berechtigungsnachweise für einen bestimmten Bereich in der Reihenfolge, die auf der Seite **Erkennungsberechtigungsnachweise** angegeben ist, bis die Ressource der TSA die Berechtigung zum Zugriff erteilt. Ein Beispiel: Wenn Sie auf ein Computersystem zugreifen möchten, wendet die TSA zunächst die erste Benutzername/Kennwort-Kombination an, die in der Berechtigungsnachweisliste für Computersysteme angegeben ist und zu der Bereichsgruppe gehört, die das System enthält. Falls der Benutzername und das Kennwort für dieses Computersystem nicht zutreffen, verwendet die TSA automatisch die nächste Benutzername/Kennwort-Kombination, die in der Berechtigungsnachweisliste für Computersysteme angegeben ist.

Tipp: Bevor Sie neue Berechtigungsnachweise speichern, testen Sie, ob die angegebenen Berechtigungsnachweise für die jeweiligen Systemtypen gültig sind, z. B. **Computersystem**, **Computersystem (Windows)**, **SNMP** oder **SNMPv3**. Durch diesen Test können Sie sicherstellen, dass die Berechtigungsnachweise gültig definiert sind.

Tipp:

- Verwenden Sie ein gemeinsames Servicekonto mit einheitlichem Kennwort für alle Geräte eines bestimmten Typs, z. B. AIX oder Windows. Auf diese Weise müssen Sie nur einen einzelnen Berechtigungsnachweis für die Erkennung aller Instanzen dieses Gerätetyps definieren.
- Verwenden Sie Konten mit dauerhaft gültigen Kennwörtern.
- Verwenden Sie SSH-Schlüssel, wo immer nötig.

Erkennungszeitplan

Erkennungsoperationen werden planmäßig zu bestimmten Tagen und Uhrzeiten ausgeführt, um sicherzustellen, dass die erkannten Daten stets aktuell und korrekt sind. Die TSA führt nach einem Standardzeitplan vollständige Erkennungen an allen verfügbaren Bereichsgruppen aus. Dieser Standardzeitplan kann an Ihre Anforderungen angepasst werden. Sie können auch Zeitpläne erstellen, mit denen die Ermittlung von Bereichsgruppen auf verschiedene Zeit- und Datumsräume verteilt werden können. Außerdem können Sie Details, Verlaufsinformationen und den Status der zuletzt ausgeführten Erkennung anzeigen.

Sie können bei einem Erkennungszeitplan den Namen, die Bereichsgruppen, die Startzeit und Häufigkeit der Erkennungen ändern. Beim Standarderkennungszeitplan können Sie nur die Startzeit und die Häufigkeit der Erkennungen ändern. Erkennungen können auch bei Bedarf ausgeführt werden.

Die Dauer der Erkennungsoperation hängt von verschiedenen Faktoren wie der Anzahl und Komplexität der Ressourcen ab. Sie kann bis zu 72 Stunden lang dauern.

Übertragungszeitplan

Erkannte Daten werden gebündelt und zu den im Zeitplan festgelegten Tagen und Uhrzeiten sicher an den IBM Support übertragen, damit IBM stets aktuelle und korrekte Informationen zur Verfügung hat. In der TSA ist ein Standardübertragungszeitplan eingerichtet, den Sie nach Ihren Anforderungen ändern können. Übertragungen können auch bei Bedarf ausgeführt werden. Außerdem können Sie den Status der zuletzt ausgeführten Übertragung anzeigen.

Die Zeitdauer für eine Übertragung hängt von der Menge der erkannten Daten ab.

Kapitel 2. Voraussetzungen

Bevor Sie die TSA einrichten und nutzen können, müssen bestimmte Voraussetzungen erfüllt sein. Beispielsweise müssen die erforderlichen Berechtigungsnachweise für die Erkennungsumgebung vorliegen und die Verbindung zum IBM Support muss konfiguriert sein.

TSA-Image herunterladen

TSA-Images sind sowohl für Microsoft Hyper-V- [*TSA-HYPERV-<Version>*] und VMware- [*TSA-VMWARE-<Version>*] Server verfügbar.

Downloadanweisungen erhalten Sie unter https://ibm.biz/TSAdemo

Systemanforderungen der TSA

Bevor Sie die TSA einrichten und verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

x86 64-Bit-Hardware
Die TSA muss auf x86 64-Bit-Systemen installiert werden.

Hypervisor
Die TSA setzt VMware ESXi oder Microsoft Hyper-V voraus.

Anmerkung: Verwenden Sie nur Versionen von ESXi oder Hyper-V, die derzeit vom Hersteller unterstützt werden.

Prozessor
Die TSA benötigt einen Vierkern-Prozessor mit mindestens 2,26 GHz.

CPU
Die TSA erfordert vier 64-Bit-CPUs.

Hauptspeicher
Die TSA benötigt 16 GB Hauptspeicher.

Direct-Access-Speichergerät (DASD)
Die TSA benötigt 150 GB DASD.

Netz
Die TSA erfordert einen 1-Gigabit-Ethernet-Adapter.

Erforderliche Web-Browser

Die Erkennung und Übertragung wird über eine webbasierte Benutzerschnittstelle eingerichtet und überwacht.

Die TSA unterstützt folgende Internet-Browser:

- Mozilla Firefox V78.4.0 Extended Support Release (ESR)
- Microsoft Edge V86.0.622.56 for Windows 10
- Google Chrome V86.0.4240.111 (64-Bit)

Diese Browser können von folgenden Websites heruntergeladen werden:

- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Microsoft Edge (https://www.microsoft.com/en-us/edge)
- Google Chrome (https://support.google.com/chrome/answer/95346?hl=de)

Konfigurationsanforderungen für Verbindungen zum IBM Support

Die TSA kann mit dem IBM Support entweder per Direktverbindung oder über einen benutzerseitigen Proxy-Server in Verbindung treten, der für die Kommunikation mit IBM konfiguriert werden muss. Bei Verwendung eines Proxy wird die TLS/SSL-Prüfung nicht unterstützt. Alle über einen Proxy gesendeten Anforderungen müssen ohne TLS/SSL-Abschluss direkt an IBM fließen können.

Stellen Sie sicher, dass Ihre Firewall Verbindungen zu Hostnamen und IP-Adressen von IBM Servern zulässt, wie in der Tabelle Netzverbindungen erläutert. Falls Ihr Netz den Zugriff auf die IBM Server nicht erlaubt, schlagen TSA-Transaktionen mit dem IBM Support fehl.

Tabelle 1. Netzverbindungen

DNS-Name	IP-Adresse	Port	Protokoll
esupport.ibm.com	129.42.54.189	443	HTTPS (an IBM)
	129.42.56.189		
	129.42.60.189		

Die Serverumgebung ist vollständig NIST SP800-131A-konform und unterstützt das TLS 1.2-Protokoll, SHA-256 oder leistungsstärkere Hashfunktionen sowie RSA-Schlüssel mit mindestens 2048 Bit.

Anmerkung: Die SSL-Prüfung wird nicht unterstützt. Wenn Sie die SSL-Prüfung auf dem Proxy-Server verwenden, müssen Sie sie für diese Datenflüsse inaktivieren.

Wenn Sie Blue Coat-Proxys verwenden, inaktivieren Sie die Protokollerkennung für IBM Server. Fügen Sie folgende Konfigurationsregeln hinzu:

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

Berechtigungsnachweise und Softwareanforderungen für die Erkennungsumgebung

Für die Erkennung von Endpunkten oder Ressourcen in Ihrer Umgebung muss die TSA Zugriff auf diese Ressourcen haben. Es empfiehlt sich, auf jeder Ressource ein spezielles Servicekonto einzurichten, das die TSA beim Zugriff auf die Ressource nutzen kann.

Nachdem Sie ein Servicekonto auf einer Ressource erstellt haben, müssen Sie auf der TSA Berechtigungsnachweise definieren und verwalten, die mit den Berechtigungsnachweisen übereinstimmen, die auf der Ressource für dieses Servicekonto definiert sind. Die TSA benötigt diese Berechtigungsnachweise für den Zugriff auf die Ressource. Die Anforderungen an Berechtigungsnachweise sind je nach Umgebung und Typ der zu erkennenden Ressource unterschiedlich, bestehen aber normalerweise aus einem Benutzernamen mit Kennwort oder einem SSH-Schlüssel. Für manche Ressourcen gelten darüber hinaus spezielle Softwareanforderungen.

Berechtigungsnachweistyp	Zugriffsinformationen
Computersystem	**Benutzername:** Der Benutzername für den Zugriff auf das Gerät. **Kennwort/Kennphrase:** Das Kennwort oder die Kennphrase für den Zugriff auf das Gerät. **Authentifizierungstyp:** Der Typ der Authentifizierung für das Gerät. • **Kennwort** – Verwendet das angegebene Kennwort. • **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.
Computersystem (Windows)	**Benutzername:** Benutzername für den Zugriff auf das Windows-Computersystem. **Kennwort:** Kennwort für den Zugriff auf das Windows-Computersystem.
Netzelement (SNMP)	**Community-Zeichenfolge:** Die Community-Zeichenfolge für das Gerät.
Netzelement (SNMPv3)	**Benutzername:** Der Benutzername für den Zugriff auf das Gerät. **Kennwort:** Das Kennwort für den Zugriff auf das Gerät. **Privates Kennwort:** Das Kennwort, das verwendet wird, wenn Datenverschlüsselung für SNMP eingerichtet ist. **Authentifizierungsprotokoll:** Der Typ des Authentifizierungsprotokolls, das von SNMP verwendet wird. • Kein • MD5 • SHA
Andere (Cisco Device)	**Benutzername:** Der Benutzername für den Zugriff auf das Cisco-Gerät. **Kennwort:** Das Kennwort für das Cisco-Gerät. **Aktivierungskennwort:** Das Aktivierungskennwort für das Cisco-Gerät.
Andere (Cisco Works)	**Benutzername:** Der Benutzername für den Zugriff auf den CiscoWorks-Server. **Kennwort:** Das Kennwort für den Zugriff auf den CiscoWorks-Server.

Anmerkung: Weitere Informationen zu Berechtigungsnachweisen und Softwareanforderungen finden Sie im Leitfaden zum Konfigurationsassistenten.

Kapitel 3. Technical Support Appliance installieren

Die TSA wird mit vorinstallierter Software geliefert. Diese ist gebündelt und wird als Image für VMware-Installationen oder als VHDX-Image für Microsoft Hyper-V-Installationen verteilt. Bei Verwendung von VMware kann die TSA mithilfe der VMware-Webschnittstelle (für ESXi) installiert werden. Bei Hyper-V wird die TSA mithilfe des Hyper-V Manager installiert. In diesem Abschnitt werden die Schritte zur Installation der TSA mit den einzelnen Methoden beschrieben.

Installation über die VMware ESXi-Webschnittstelle

Vorbereitende Schritte

Für die Installation der TSA muss VMware ESXi 6.5. oder höher zur Steuerung der Hardware geladen sein.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte durch, um das TSA-Image zu installieren.

Vorgehensweise

1. Melden Sie sich beim ESXi-System über die VMware ESXi-Webschnittstelle an.
2. Klicken Sie auf **Create/Register VM**. Der **New Virtual Machine Wizard** wird angezeigt.

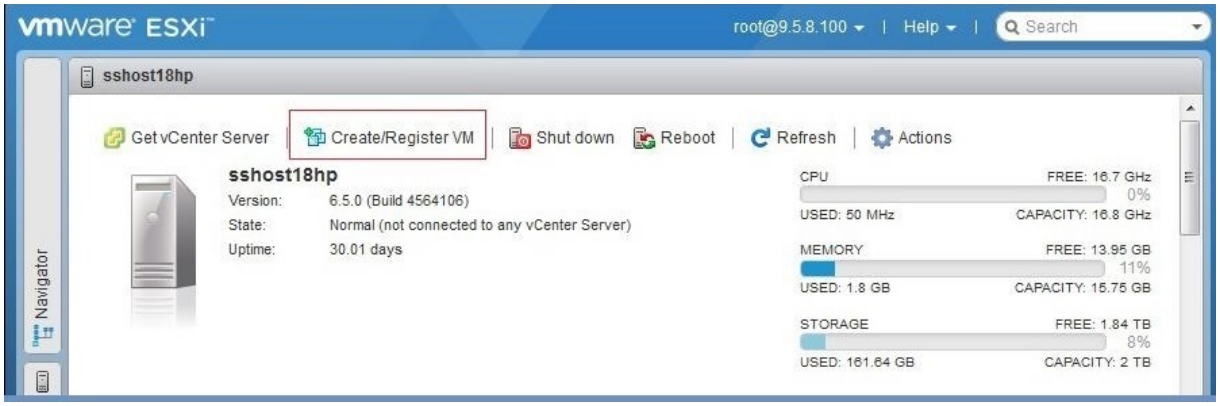

Abbildung 1. VM erstellen/registrieren

3. Wählen Sie in der Anzeige **Select creation type** die Option **Deploy a virtual machine from an OVF or OVA file** aus und klicken Sie dann auf **Next**.

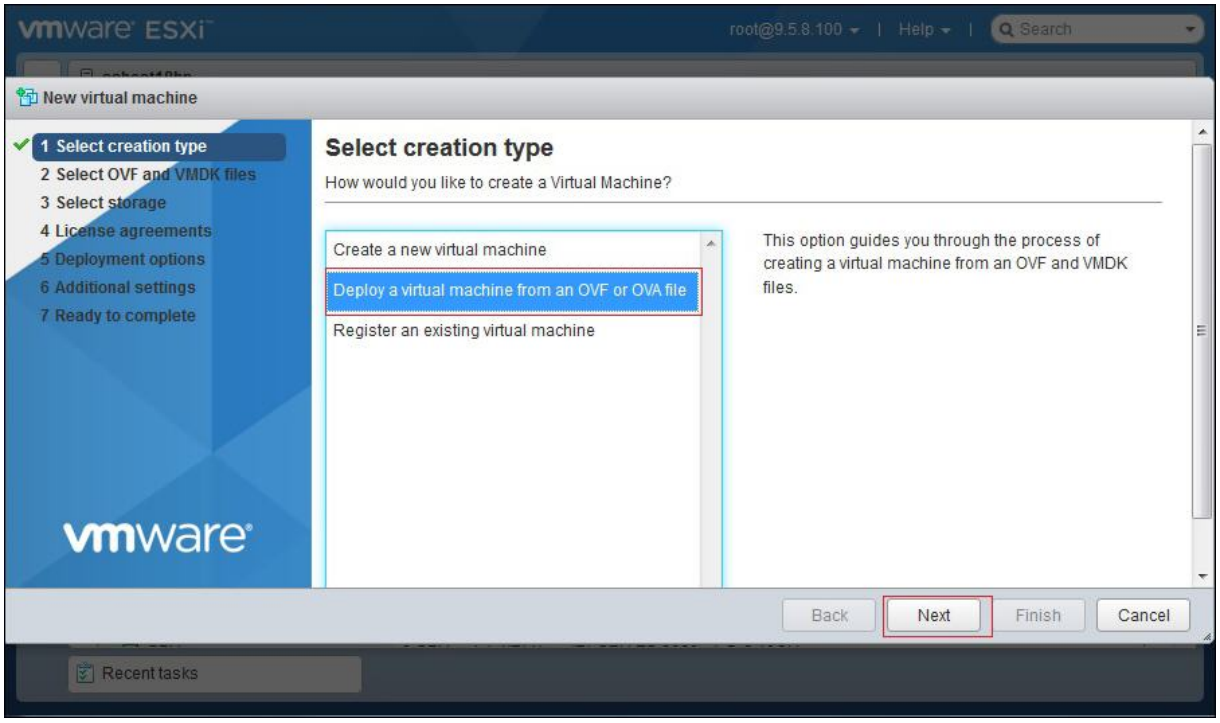

Abbildung 2. Erstellungstyp auswählen

4. Klicken Sie in der Anzeige **Select OVF and VMDK** in das Feld **Click to select files or drag/drop** und wählen Sie die Imagedatei aus, die Sie von Fix Central heruntergeladen haben. Geben Sie einen eindeutigen Namen für Ihre virtuelle Maschine ein oder belassen Sie den Standardwert. Klicken Sie anschließend auf **Next**.

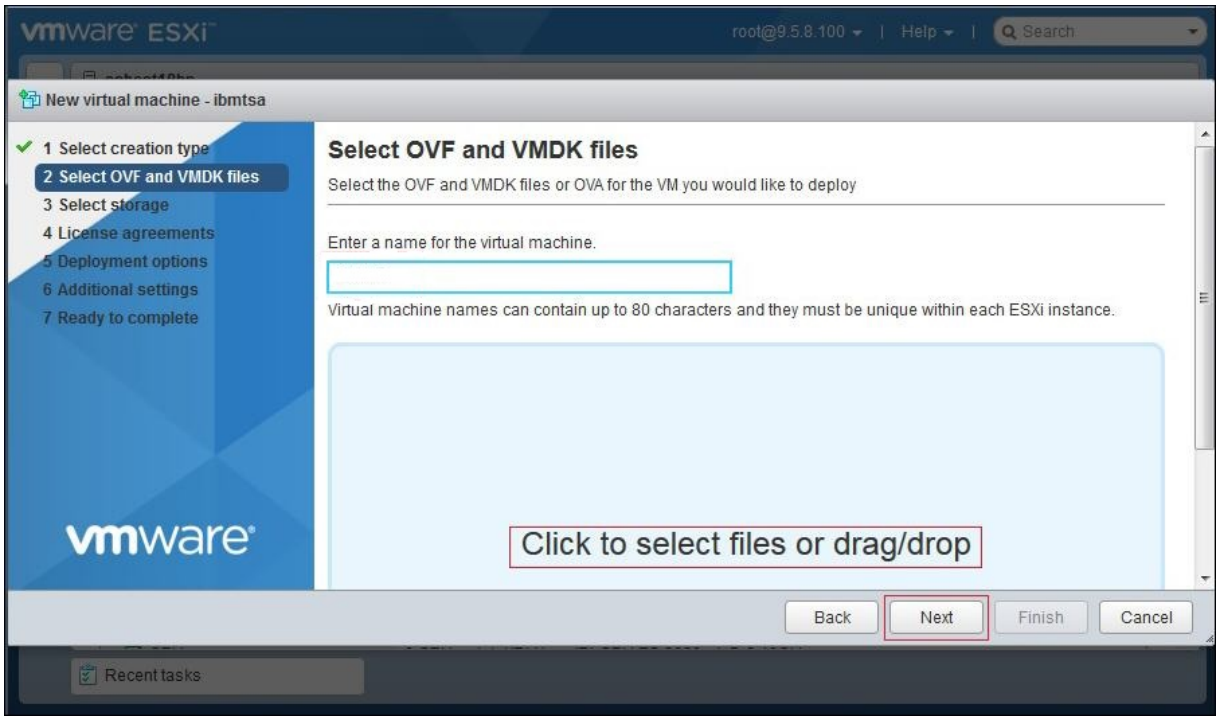

Abbildung 3. OVF- und VMDK-Dateien auswählen

5. Wählen Sie in der Anzeige **Select storage** aus der angezeigten Liste einen Datenspeicher zur Speicherung der Konfiguration und der Plattendateien aus. Klicken Sie anschließend auf **Next**.

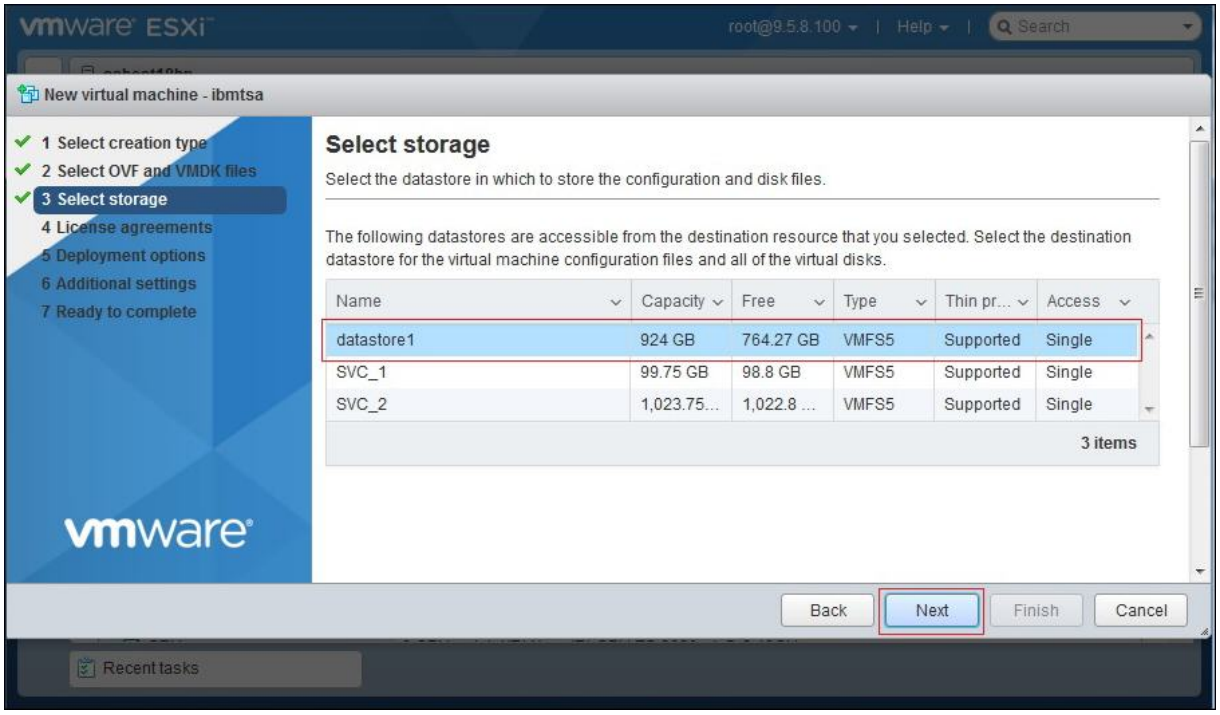

Abbildung 4. Speicherort auswählen

6. Wählen Sie in der Anzeige **Deployment options** eine Netzzuordnung aus der Dropdown-Liste **VM Network** aus.

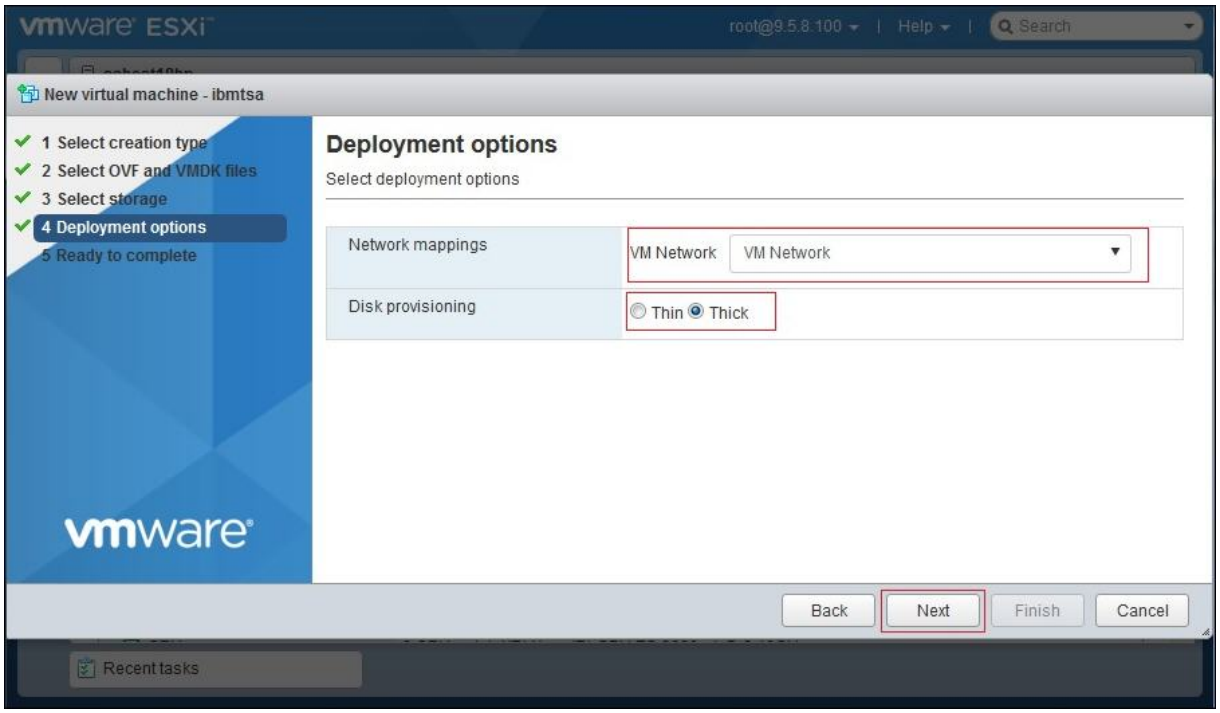

Abbildung 5. Bereitstellungsoptionen

7. Wählen Sie für die Plattenbereitstellung die Option **Thick** aus und klicken Sie dann auf **Next**.
8. Überprüfen Sie in der Anzeige **Ready to complete** alle Einstellungen, die Sie ausgewählt haben. Falls Sie etwas ändern möchten, klicken Sie auf **Back** und nehmen Sie die gewünschten Änderungen an den Optionen vor. Wenn alles in Ordnung ist, klicken Sie auf **Finish**.

   Wichtig: Aktualisieren Sie nicht die Browseransicht, während die virtuelle Maschine bereitgestellt wird.

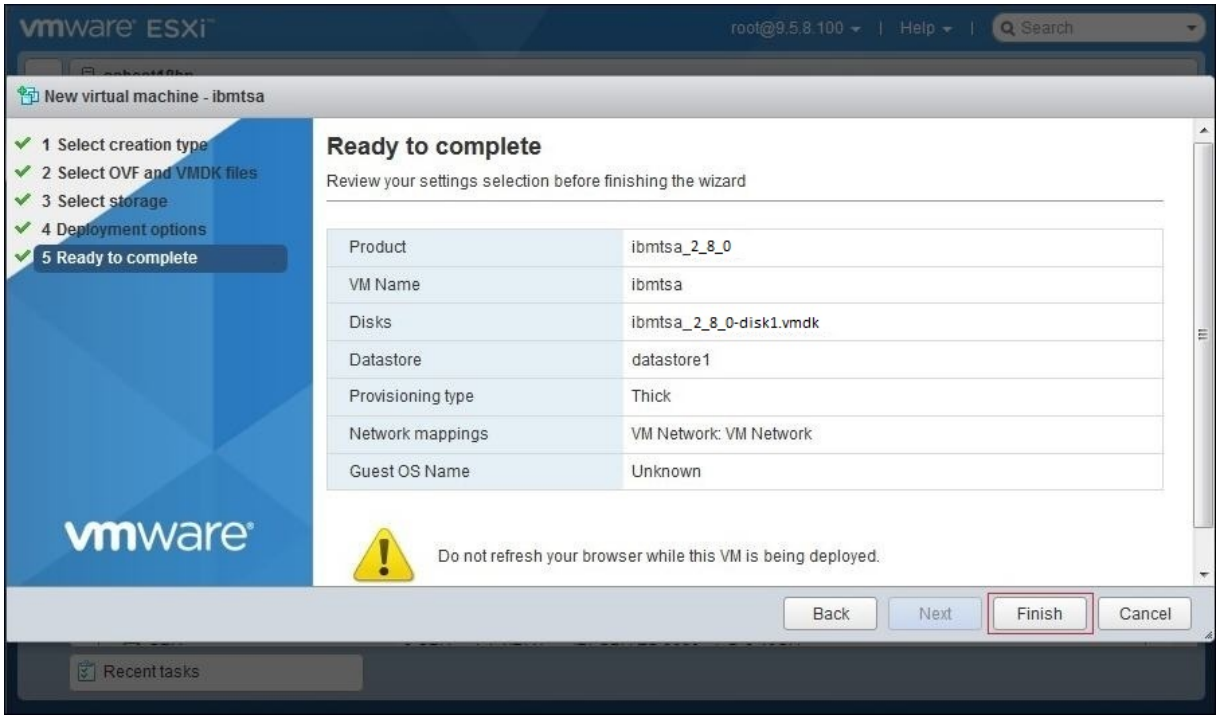

Abbildung 6. Ausgewählte Einstellungen überprüfen

Die virtuelle Maschine für die TSA wird auf Ihrem System installiert.

9. Geben Sie in der TSA-Konsole für **ibmtsa login** den Wert **`tsausr`** und für **Password** den Wert **`configTsa`** ein.
10. Erforderlich: Ändern Sie das Anmeldekennwort, wie im Abschnitt „Kennwort tsausr ändern (erforderlich)" auf Seite 19 beschrieben.
11. Um die Installation fertigzustellen, führen Sie die im Abschnitt „Netzdetails konfigurieren" auf Seite 19 beschriebenen Schritte durch.

Die TSA auf Microsoft Hyper-V installieren

Vorbereitende Schritte

Bevor Sie die TSA auf Hyper-V installieren und verwenden, müssen Sie darauf achten, dass Sie die folgenden Voraussetzungen erfüllen:

- Hyper-V Server 2016 oder 2019
- Hyper-V Manager
- Virtual Network Switch wurde durch Hyper-V Manager erstellt

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte durch, um die TSA auf Hyper-V zu installieren:

Vorgehensweise

Führen Sie zum Installieren der TSA auf Hyper-V die folgenden Schritte durch:

1. Extrahieren Sie nach dem Download des TSA-Image die Datei *ibmtsa_2800.vhdx* aus *ibmtsa_2800.zip* und verschieben Sie sie in ein Verzeichnis auf dem Hyper-V-Server.
2. Starten Sie Hyper-V Manager und stellen Sie eine Verbindung zum Hyper-V-Server über das Clientsystem her.
3. Klicken Sie auf **Browse** und wählen Sie das auf Ihrem System gespeicherte Image aus.

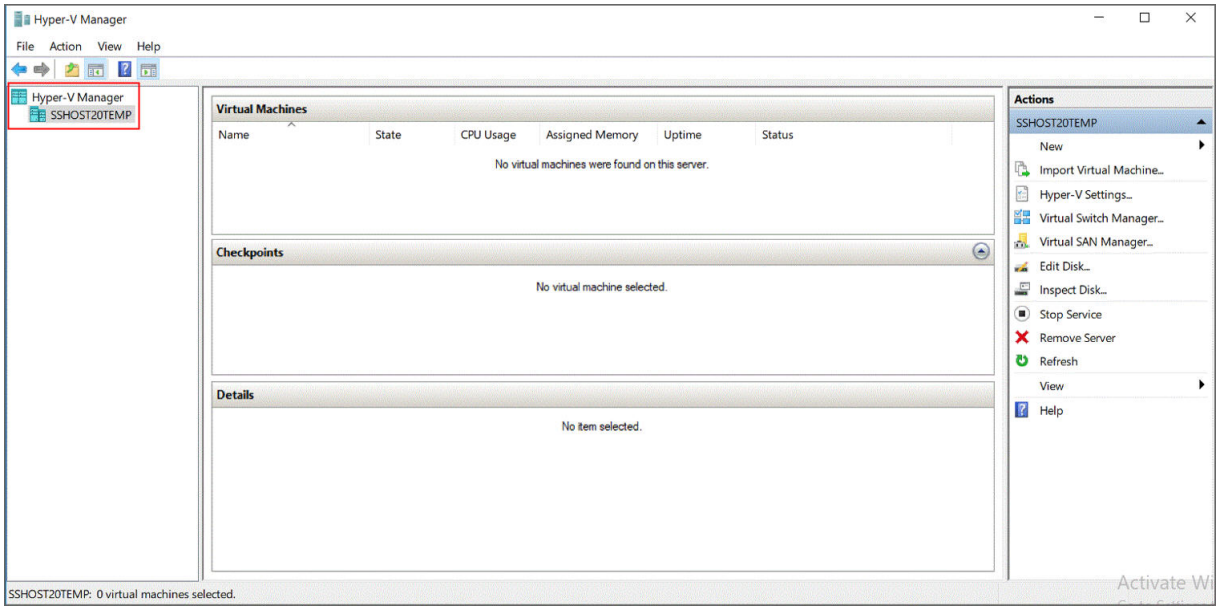

Abbildung 7. Hyper-V Manager

4. Wählen Sie im Menü **Actions** die Option **New** → **Virtual Machine** aus. Der **New Virtual Machine Wizard** wird angezeigt.
5. Geben Sie unter **Name** einen Namen für die neue virtuelle Maschine ein und klicken Sie auf **Next**.

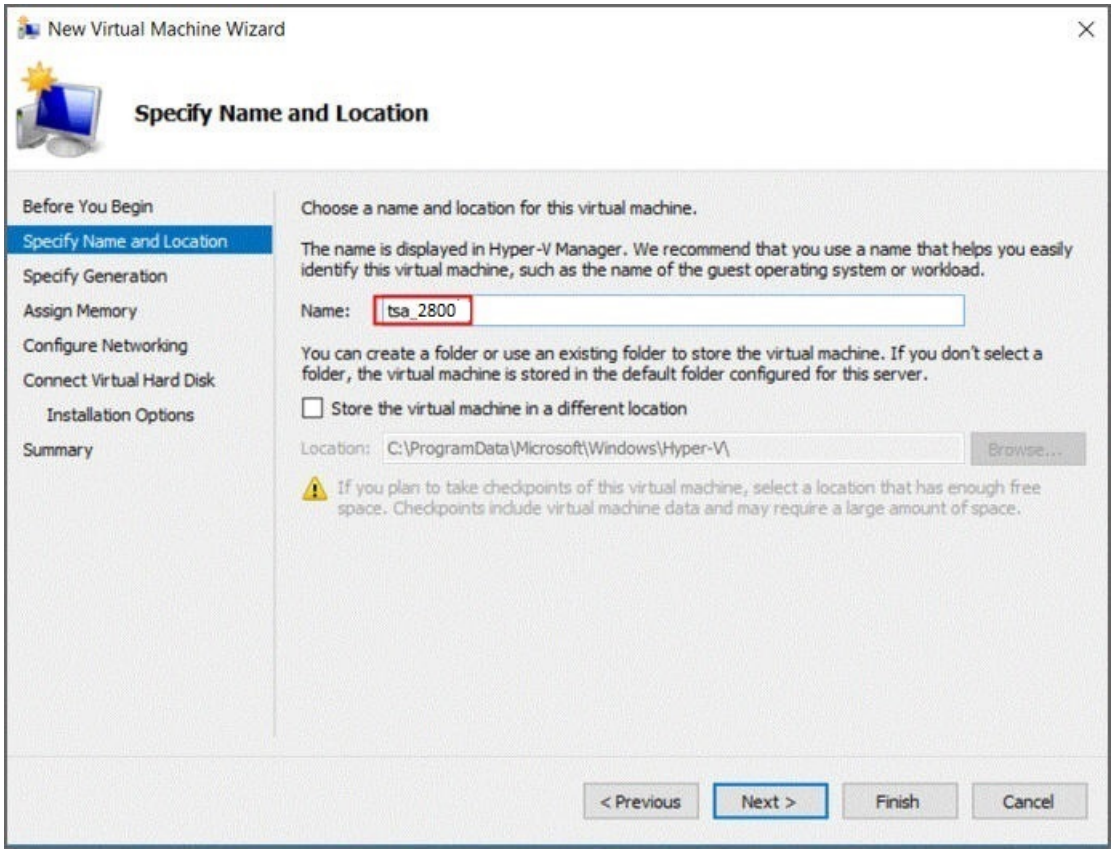

Abbildung 8. Name für virtuelle Maschine

6. Wählen Sie **Generation 1** als Generation der virtuellen Maschine aus und klicken Sie auf **Weiter**.

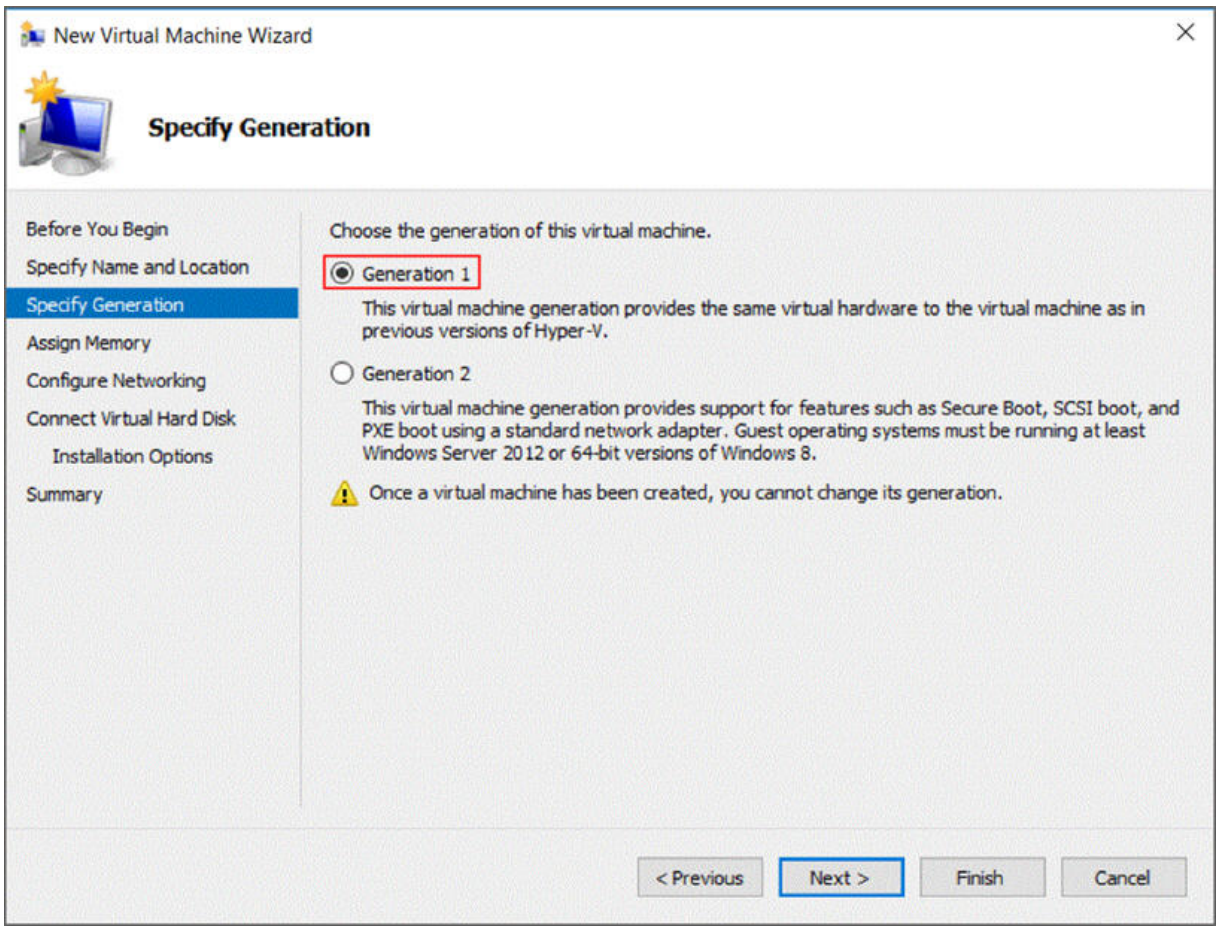

Abbildung 9. Generation angeben

7. Geben Sie unter **Startup memory** den Wert *16384* MB ein und klicken Sie auf **Next**.

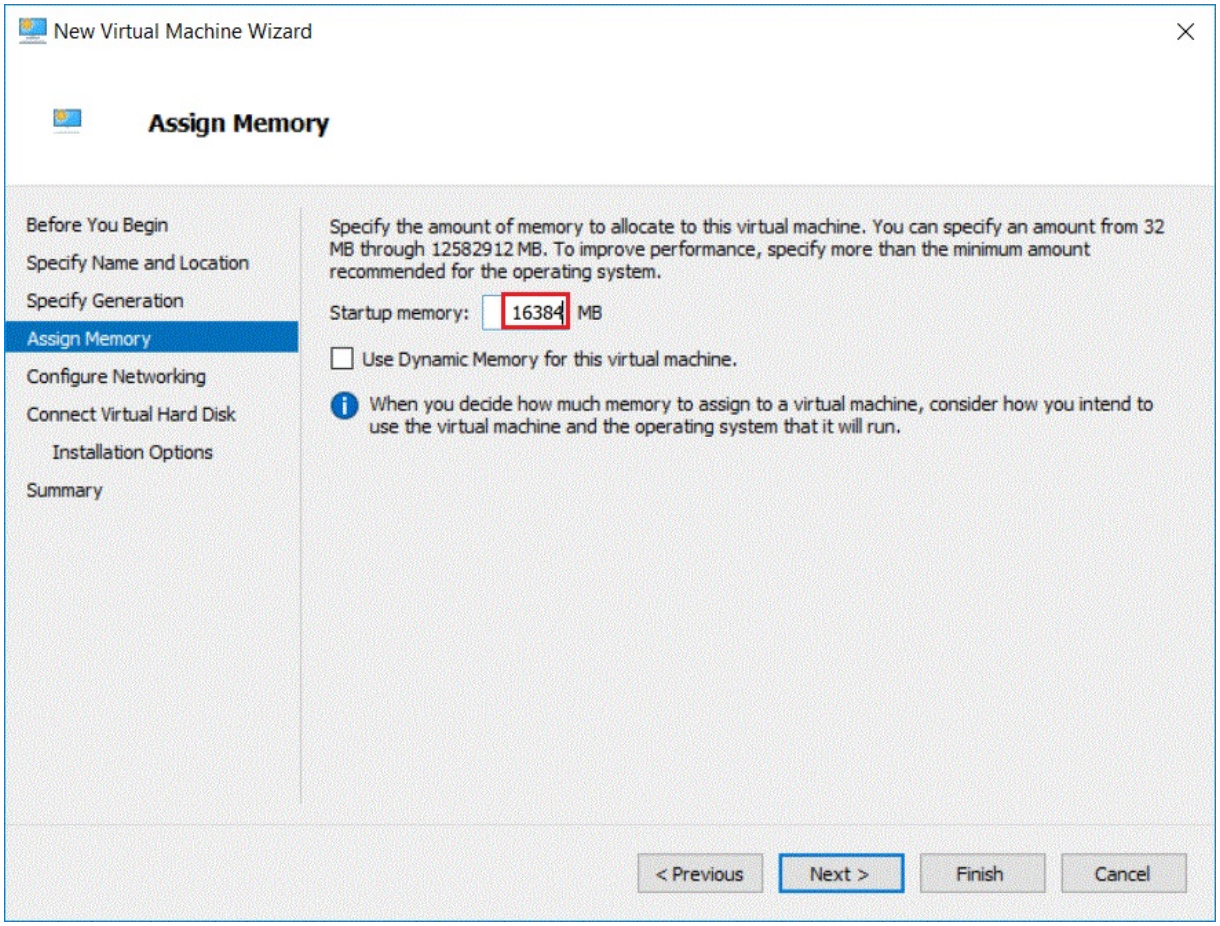

Abbildung 10. Startspeicher

8. Wählen Sie einen vorkonfigurierten virtuellen Switch aus und klicken Sie auf **Next**.

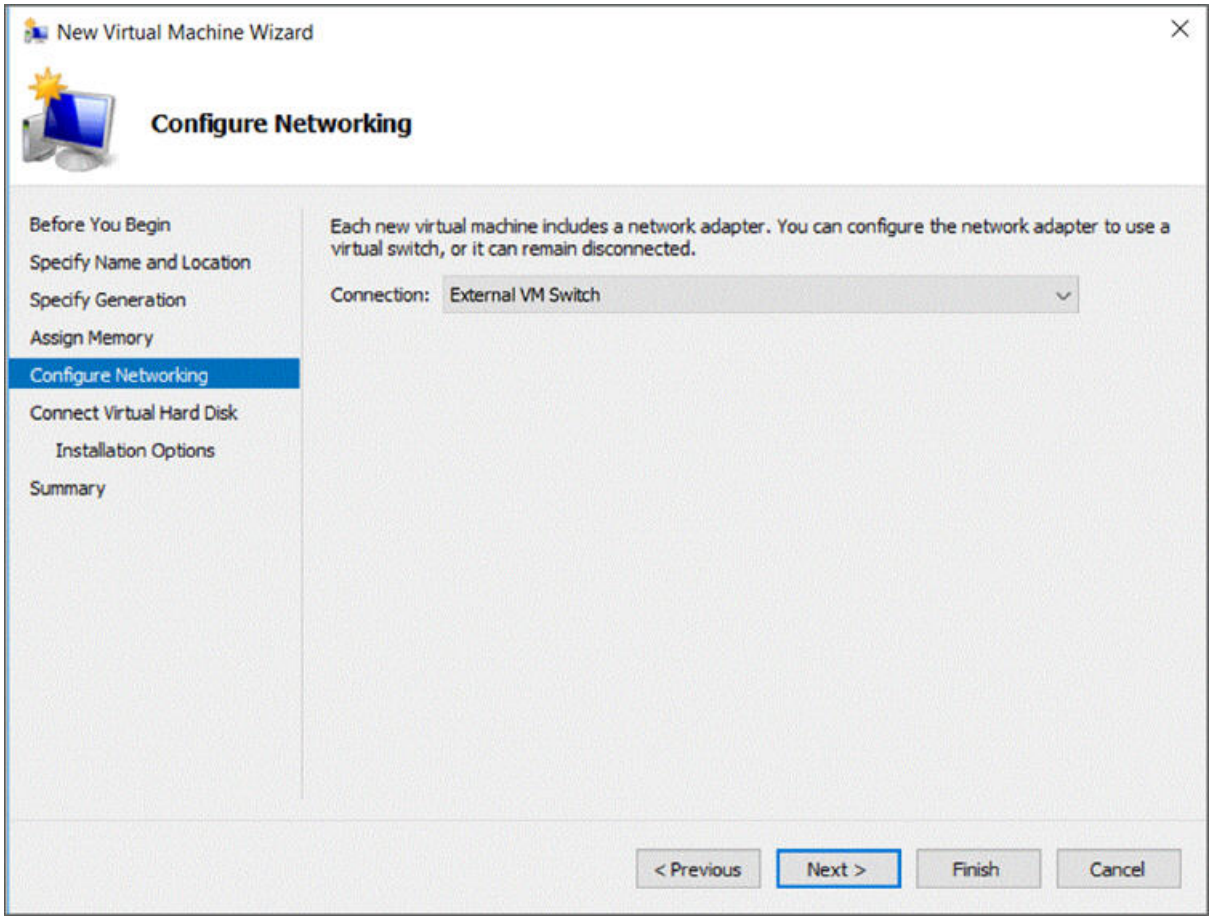

Abbildung 11. Netzbetrieb konfigurieren

9. Wählen Sie die Option **Use an existing virtual hard disk** aus und suchen Sie nach der Datei *ibmt-sa_2800.vhdx*, die Sie in Schritt 2 auf den Hyper-V-Server kopiert haben. Klicken Sie anschließend auf **Next**.

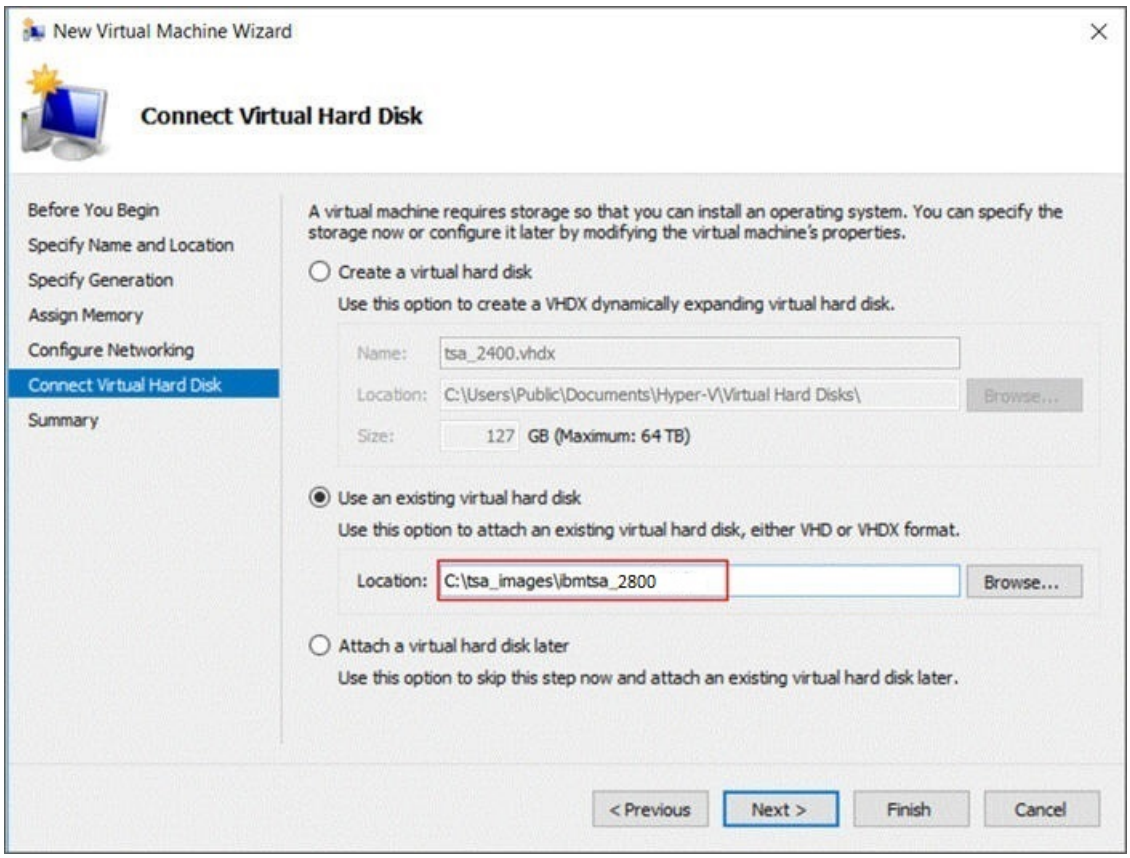

Abbildung 12. Mit virtueller Festplatte verbinden

10. Überprüfen Sie auf der Seite **Summary** die Einstellungen und klicken Sie auf **Finish**.

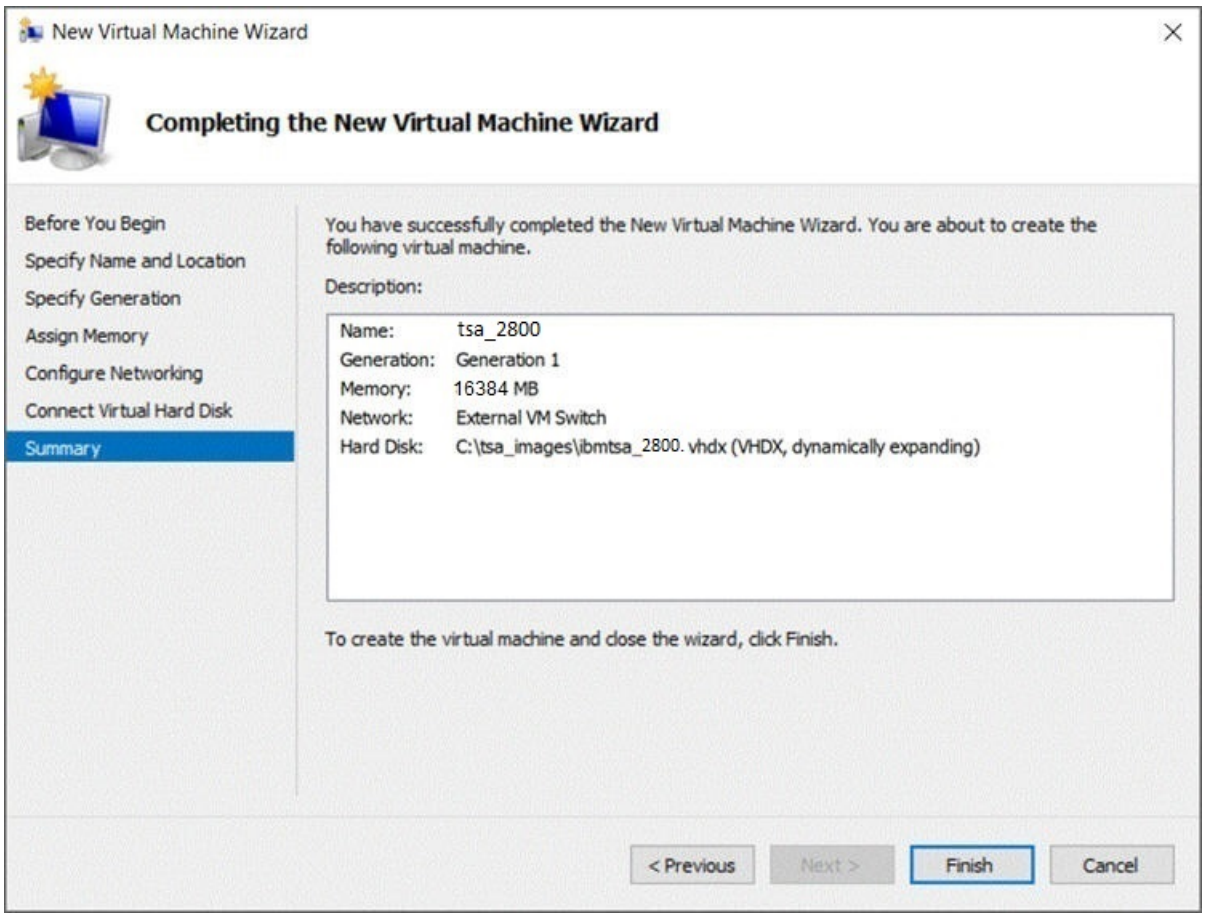

Abbildung 13. Übersicht

11. Die neue virtuelle Maschine wird zum Hyper-V Manager hinzugefügt. Wählen Sie die virtuelle Maschine aus und klicken Sie im Menü **Actions** auf **Start**.

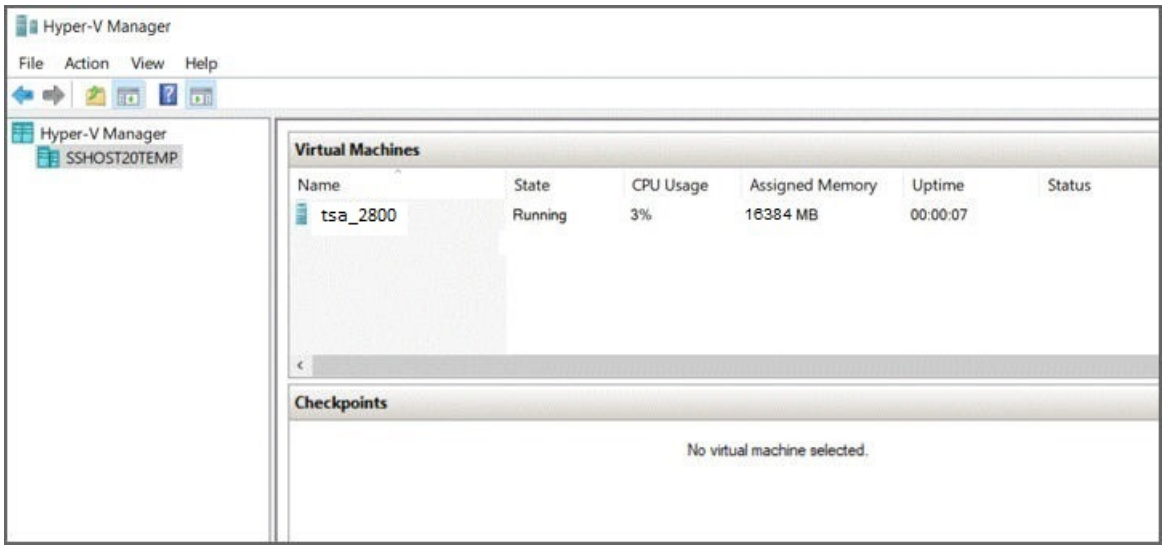

Abbildung 14. Hyper-V Manager

12. Wählen Sie im Menü **Actions** die Option **Connect** aus, um eine Konsolensitzung zu starten. Geben Sie in der TSA-Konsole für **ibmtsa login** den Wert **`tsausr`** und für **Password** den Wert **`configTsa`** ein.
13. Erforderlich: Ändern Sie das Anmeldekennwort, wie im Abschnitt „Kennwort tsausr ändern (erforderlich)" auf Seite 19 beschrieben.
14. Um die Installation fertigzustellen, führen Sie die im Abschnitt „Netzdetails konfigurieren" auf Seite 19 beschriebenen Schritte durch.

Kennwort *tsausr* ändern (erforderlich)

Aus Sicherheitsgründen wird empfohlen, das anfängliche Kennwort für *tsausr* zu ändern. Führen Sie zum Ändern des Kennworts für *tsausr* die folgenden Schritte durch.

Vorgehensweise

1. Wählen Sie im **TSA-Konfigurationsmenü** die Option **2) Change tsausr password** aus.

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: 2
```

Abbildung 15. Kennwort ändern

2. Geben Sie an der Eingabeaufforderung **New password** das neue Kennwort ein. Geben Sie dasselbe Kennwort an der Eingabeaufforderung **Retype new password** ein. Das neue Kennwort muss mindestens 7 Zeichen lang sein.

```
Changing password for user tsausr.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Returning to menu in 5 seconds...
```

Abbildung 16. Neues Kennwort

Netzdetails konfigurieren

Vorgehensweise

1. Wählen Sie im **TSA-Konfigurationsmenü** die Option **1) Setup network configuration** aus.

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: _
```

Abbildung 17. Netzkonfiguration einrichten

2. Geben Sie die folgenden Netzkonfigurationsdetails ein.

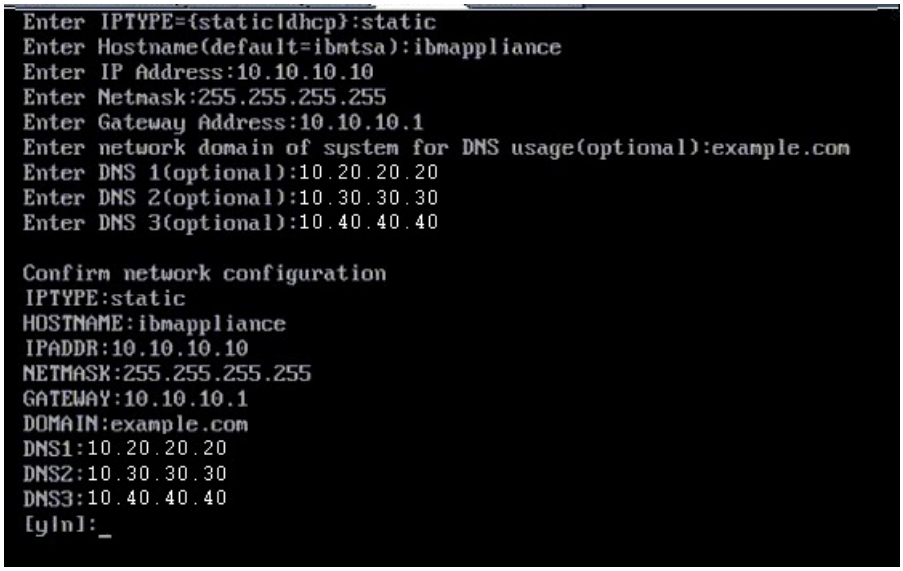

Abbildung 18. Netzkonfiguration

a) **Enter IPTYPE = {static|dhcp}**. Geben Sie `static` oder `dhcp` ein. Wenn Sie `static` eingeben, führen Sie die folgenden Schritte durch. Andernfalls führen Sie die Schritte für die `dhcp`-Konfiguration durch, beschrieben im Abschnitt Anhang B, „DHCP-Netzdetails konfigurieren", auf Seite 131

IPTYPE: static

Enter Hostname(default=ibmtsa). Sie können den Standardhostnamen ändern. Stellen Sie sicher, dass der Hostname eindeutig ist.

Enter IP Address.

Enter Netmask und **Enter Gateway**.

Enter network domain of system for DNS usage (optional).

Enter DNS 1(optional), **Enter DNS 2(optional)** und **Enter DNS 3(optional)**.

Die angegebenen Netzkonfigurationsdetails werden zur Bestätigung angezeigt.

b) Geben Sie **[y|n]** ein, um die Netzkonfiguration zu bestätigen oder zu verwerfen. Durch Eingabe von **y** wird die Netzkonfiguration gespeichert und das System automatisch neu gestartet.

Anmerkung: Falls die Konfiguration nicht korrekt ist können Sie die Details ändern. Geben Sie **n** ein, um die aktuellen Einstellungen zu ignorieren und die Konfiguration ab Schritt „2.a" auf Seite 20 neu zu starten.

c) Das System wird nach 15 Sekunden neu gestartet, damit die neue Netzkonfiguration wirksam wird.

d) Rufen Sie in Ihrem Browser die TSA mit sicherem HTTP und dem oben angegebenen Hostnamen oder der angegebenen IP-Adresse auf.
Beispiel: `https://<Hostname | IP-Adresse>.`

Anmerkung: Bei der ersten Verbindung zeigt Ihr Browser möglicherweise eine Sicherheitswarnung an. Sie müssen das Sicherheitszertifikat akzeptieren und die Anmeldung bei der TSA fortsetzen.

Anmerkung: Um die grundlegenden Netzeinstellungen für die TSA über die Benutzerschnittstelle zu ändern, führen Sie die im Abschnitt „Grundlegende Netzeinstellungen konfigurieren" auf Seite 34 beschriebenen Schritte durch. Zum Konfigurieren von erweiterten Netzeinstellungen führen Sie die Schritte im Abschnitt „Erweiterte Netzeinstellungen konfigurieren" auf Seite 36 durch.

3. Richten Sie die Technical Support Appliance anhand der Schritte in Kapitel 4, „Die Technical Support Appliance einrichten", auf Seite 21 ein.

Ergebnisse

Nachdem Sie die TSA erfolgreich eingerichtet haben, fahren Sie mit Kapitel 5, „Erkennung und Übertragung an IBM einrichten", auf Seite 49 fort.

Kapitel 4. Die Technical Support Appliance einrichten

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte durch, um die TSA schnell in Betrieb zu nehmen: Falls noch nicht geschehen, lesen Sie Kapitel 2, „Voraussetzungen", auf Seite 5.

Vorgehensweise

1. „Bei der Technical Support Appliance anmelden" auf Seite 21
2. „Lizenzvereinbarung akzeptieren" auf Seite 23
3. „Den Installationsassistenten für die Erstkonfiguration verwenden" auf Seite 25
   a) „IBM Konnektivität einrichten" auf Seite 26
   b) „Technical Support Appliance registrieren" auf Seite 27
   c) „Systemzeit einstellen" auf Seite 29
   d) „Übertragungszeitplan einrichten" auf Seite 31
   e) „Technical Support Appliance aktualisieren" auf Seite 32
4. „Netzeinstellungen konfigurieren" auf Seite 33
5. „Zertifikate einrichten" auf Seite 42.
6. Optional: Anhang C, „Benutzerkonten und Benutzergruppen", auf Seite 133

Nächste Schritte

Wenn Sie die Einrichtung der TSA abgeschlossen haben, lesen Sie in Kapitel 5, „Erkennung und Übertragung an IBM einrichten", auf Seite 49, wie Sie weitere Aufgaben durchführen können.

Bei der Technical Support Appliance anmelden

Vorgehensweise

1. Öffnen Sie einen Internet-Browser auf einem System mit Netzzugriff auf die TSA.
   Weitere Informationen hierzu unter „Erforderliche Web-Browser" auf Seite 5.
2. Geben Sie die folgende URL in die Adressleiste des Browsers ein:

   ```
   https://<Hostname oder IP-Adresse>
   ```

   Anmerkung: Wenn der `<Hostname>` nicht funktioniert, versuchen Sie es mit der zugewiesenen IP-Adresse der TSA.
3. Geben Sie in der angezeigten Eingabeaufforderung die folgende Informationen ein:

   Benutzer-ID:
   Verwenden Sie die ID `admin`

   Kennwort:
   Geben Sie das TSA-Administratorkennwort ein.

   Das Anfangskennwort lautet `passw0rd`. Dieses Anfangskennwort müssen Sie nach der Anmeldung in der TSA ändern.

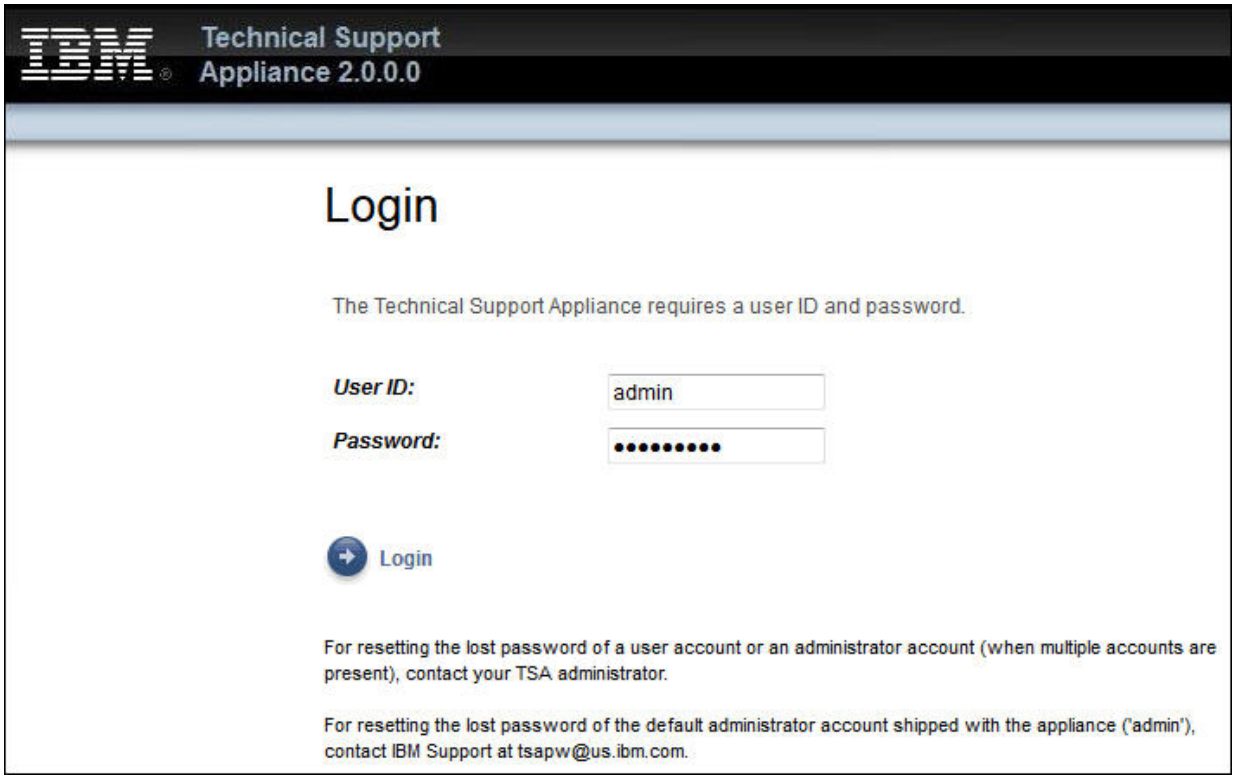

Abbildung 19. Anmeldung

Bei der erstmaligen Anmeldung wird die Seite **Kennwort ändern** angezeigt.

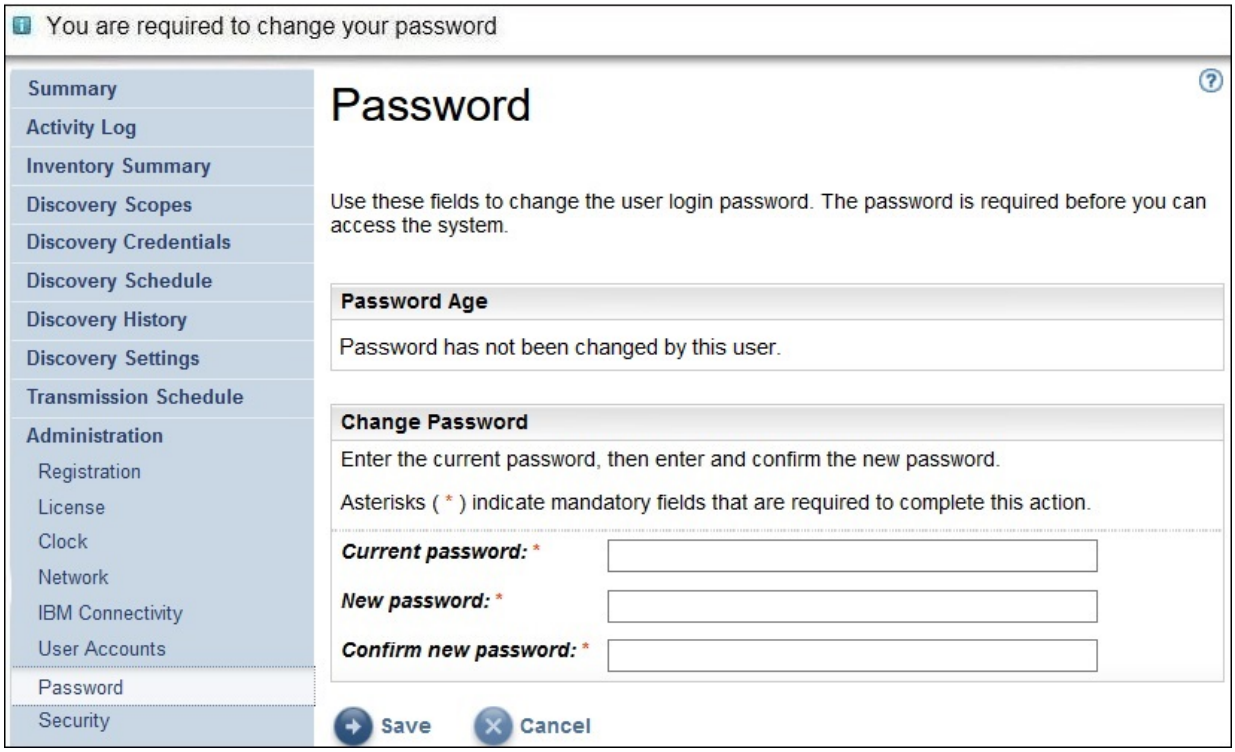

Abbildung 20. Kennwort ändern

Führen Sie zum Ändern des Anfangskennworts die folgenden Schritte durch:

a) Geben Sie ein neues Kennwort ein.

Das Kennwort muss folgenden Regeln entsprechen:

- Es muss mindestens 8 Zeichen lang sein.
- Es muss mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthalten.
- Der Benutzername darf nicht enthalten sein.
- Es darf nicht mit einem der acht vorherigen Kennwörter identisch sein.
- Es muss mindestens alle 90 Tage (Standard) geändert werden, jedoch nicht öfter als einmal pro Tag.

b) Geben Sie im Feld **Neues Kennwort bestätigen** das neue Kennwort erneut ein.

Bevor das Kennwort gespeichert wird, werden die beiden von Ihnen eingegebenen Kennwörter verglichen, um zu bestätigen, dass sie übereinstimmen.

c) Notieren Sie sich das neue Kennwort, um es später nachschlagen zu können.

Wichtig: Es ist nicht möglich, ein Kennwort wiederzuerlangen. Falls Sie Ihr Kennwort verlieren oder vergessen, können Sie sich nicht mehr in der TSA anmelden, um das Kennwort zu ändern. Bei Verlust des Kennworts für ein Benutzerkonto oder Administratorkonto (falls mehrere Konten vorhanden sind) wenden Sie sich bitte an Ihren TSA-Administrator. Bei Verlust des Kennworts für das Standardadministratorkonto (Werkseinstellung der TSA) rufen Sie den IBM Support an.

d) Klicken Sie auf **Speichern**.Bei der erstmaligen Anmeldung wird die Seite **Lizenzvereinbarung** angezeigt.

Lizenzvereinbarung akzeptieren

Lesen und akzeptieren Sie die Lizenzvereinbarung, bevor Sie fortfahren.

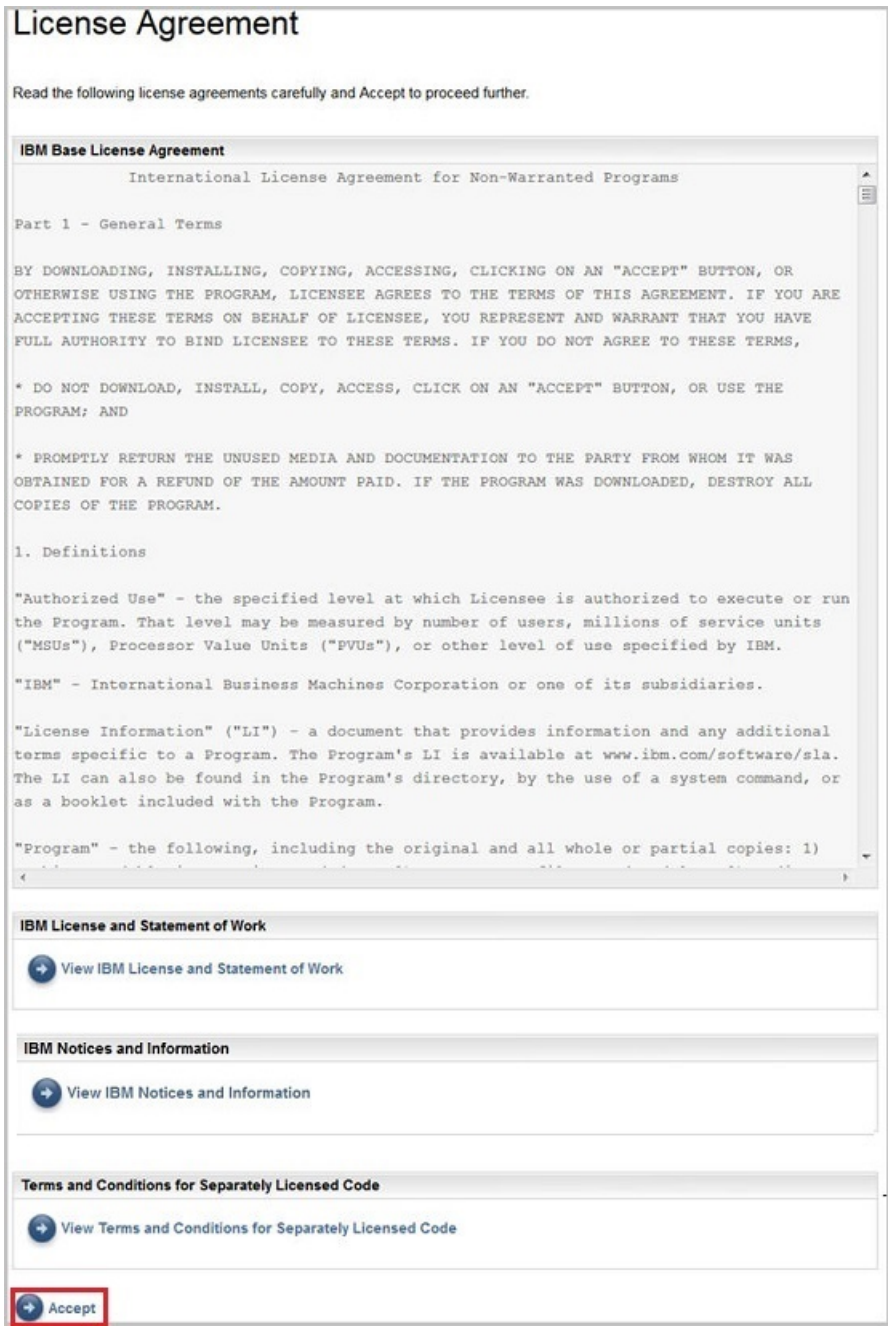

Abbildung 21. Lizenzvereinbarung

Die Lizenzvereinbarung enthält die folgenden Informationen:

- **IBM Basislizenzvereinbarung**: Zeigt die IBM Basislizenzvereinbarung an.
- **IBM Lizenz und Leistungsbeschreibung**: Klicken Sie auf **IBM Lizenz und Leistungsbeschreibung**, um die Leistungsbeschreibung zur IBM Lizenz anzuzeigen.

  Anmerkung: Die TSA entspricht den Bestimmungen der DSGVO [EU/2016/679]. Die DSGVO-Konformitätsinformationen finden Sie ebenfalls im Abschnitt **IBM Lizenz und Leistungsbeschreibung**.
- **IBM Bemerkungen und Informationen**: Klicken Sie auf **IBM Bemerkungen und Informationen anzeigen**, um Bekanntmachungen und Informationen von IBM anzuzeigen.
- **Bedingungen für separat lizenzierten Code**: Klicken Sie auf **Bedingungen für separat lizenzierten Code anzeigen**, um die Bedingungen für separat lizenzierten Code anzuzeigen.

Klicken Sie auf **Akzeptieren**, um die Vereinbarung zu akzeptieren. Sobald Sie die Lizenzvereinbarung akzeptiert haben, wird der **Installationsassistent** angezeigt, um die TSA zu konfigurieren. Sie können die TSA entweder über den **Installationsassistenten** konfigurieren oder den Assistenten beenden und TSA-Einstellung gemäß Ihren Anforderungen konfigurieren.

Anmerkung: Um die Lizenzvereinbarung nach dem Akzeptieren erneut anzuzeigen, klicken Sie im Navigationsbereich auf **Verwaltung** > **Lizenz**.

Zugehörige Konzepte

„Den Installationsassistenten für die Erstkonfiguration verwenden" auf Seite 25
Verwenden Sie den **Installationsassistenten**, um die TSA für die Erstkonfiguration einzurichten.

„Die Technical Support Appliance konfigurieren" auf Seite 121
Falls Sie die Konfiguration der Einstellungen im **Installationsassistenten** beenden oder überspringen, können Sie die Einstellungen über das Navigationsmenü der TSA auf der linken Seite manuell konfigurieren.

Den Installationsassistenten für die Erstkonfiguration verwenden

Verwenden Sie den **Installationsassistenten**, um die TSA für die Erstkonfiguration einzurichten.

Sobald Sie die Lizenzvereinbarung akzeptiert haben, wird der **Installationsassistent** automatisch angezeigt.

Anmerkung: Klicken Sie, um den **Installationsassistenten** manuell zu starten, im Navigationsfenster auf **Tools** > **Installationsassistent** > **Installationsassistent starten**.

Abbildung 22. Installationsassistent

Der **Installationsassistent** führt Sie durch die folgenden Schritte:

- „IBM Konnektivität einrichten" auf Seite 26
- „Technical Support Appliance registrieren" auf Seite 27
- „Systemzeit einstellen" auf Seite 29
- „Übertragungszeitplan einrichten" auf Seite 31
- „Technical Support Appliance aktualisieren" auf Seite 32

Anmerkung: Falls Sie die Konfiguration der Einstellungen im **Installationsassistenten** beenden oder überspringen, können Sie die Einstellungen über das Navigationsteilfenster der TSA manuell konfigurieren. Weitere Informationen zur Konfiguration dieser Einstellungen finden Sie im Abschnitt Anhang A, „Die Technical Support Appliance konfigurieren", auf Seite 121.

IBM Konnektivität einrichten

Vorgehensweise

Sie können die Konfiguration, die TSA für die Verbindung zu IBM verwendet, anzeigen, ändern und testen.

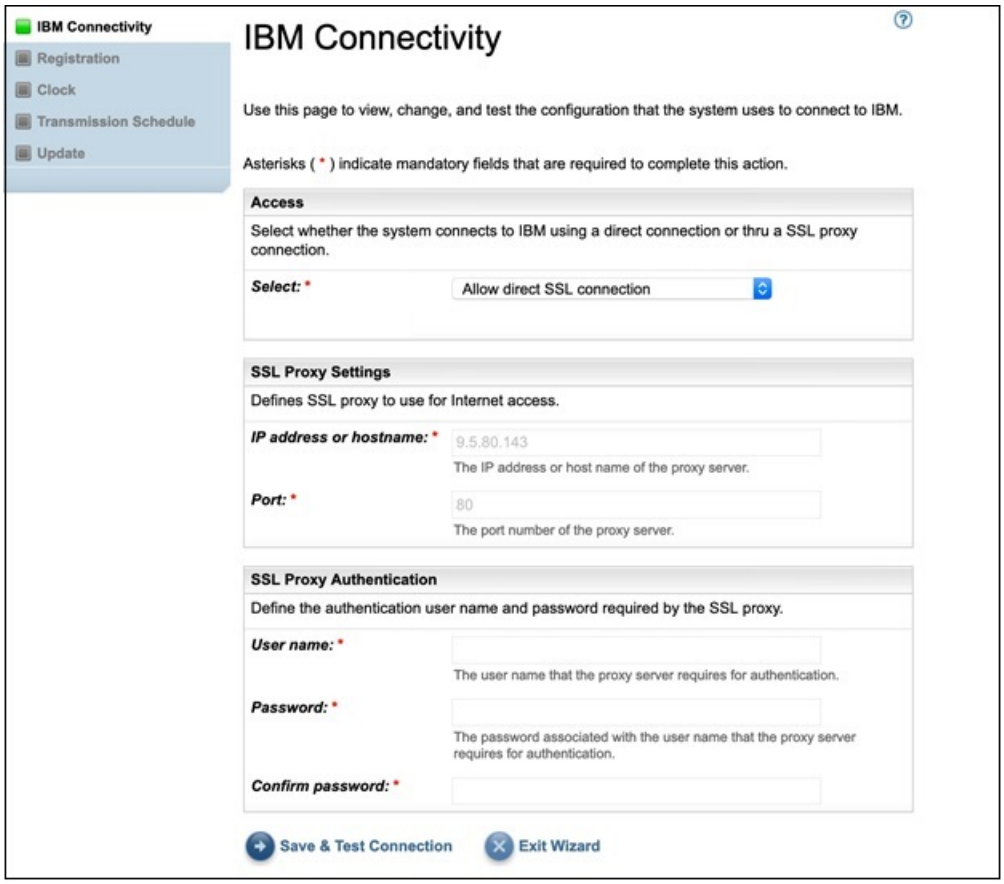

Abbildung 23. IBM Konnektivität

1. Wählen Sie im Fenster **Zugang** eine der folgenden Internetzugangsarten aus:

   SSL-Direktverbindung ermöglichen
   TSA stellt die Verbindung zu IBM über eine Direktverbindung her.

   SSL-Proxyverbindung verwenden
   TSA stellt die Verbindung zu IBM über eine SSL-Proxyverbindung her.

   SSL-Proxyverbindung mit Authentifizierung verwenden
   TSA stellt die Verbindung zu IBM über eine authentifizierende SSL-Proxyverbindung her.
2. Wenn Sie **Use SSL proxy connection** oder **Use authenticating SSL proxy connection** ausgewählt haben, geben Sie die folgenden Informationen zum Proxyserver an.

   IP-Adresse oder Hostname
   Die IP-Adresse oder der Hostname des Proxyservers.

   Anmerkung: Der eingegebene Hostname darf keinen Unterstrich ("_") enthalten.

   Port
   Die Portnummer des Proxyservers.
3. Wenn Sie **Use authenticating SSL proxy connection** ausgewählt haben, geben Sie die folgenden Informationen zum Proxyserver an:

   Benutzername
   Der Benutzername, den der Proxyserver zur Authentifizierung benötigt.

Kennwort
Das Kennwort zum Benutzernamen, das der Proxyserver zur Authentifizierung benötigt.

Kennwort bestätigen
Geben Sie das Kennwort erneut ein. Die beiden Kennwörter werden verglichen und auf Übereinstimmung geprüft, bevor das Kennwort gespeichert wird.

Nächste Schritte

- Klicken Sie auf **Verbindung speichern und testen**, um die angegebene Verbindung zu speichern und zu testen. Wenn die Verbindung erfolgreich ist, wird die Schaltfläche **Weiter** angezeigt.
- Klicken Sie auf **Weiter**, um zur Seite **Registrierung** zu gehen.

  -oder-
- Klicken Sie auf **Assistent verlassen**, um den **Installationsassistenten** zu verlassen und zur Seite **Zusammenfassung** zu gehen.

Technical Support Appliance registrieren

Sie können Ansprechpartner und physischen Standort für Systemservice anzeigen und ändern.

Vorgehensweise

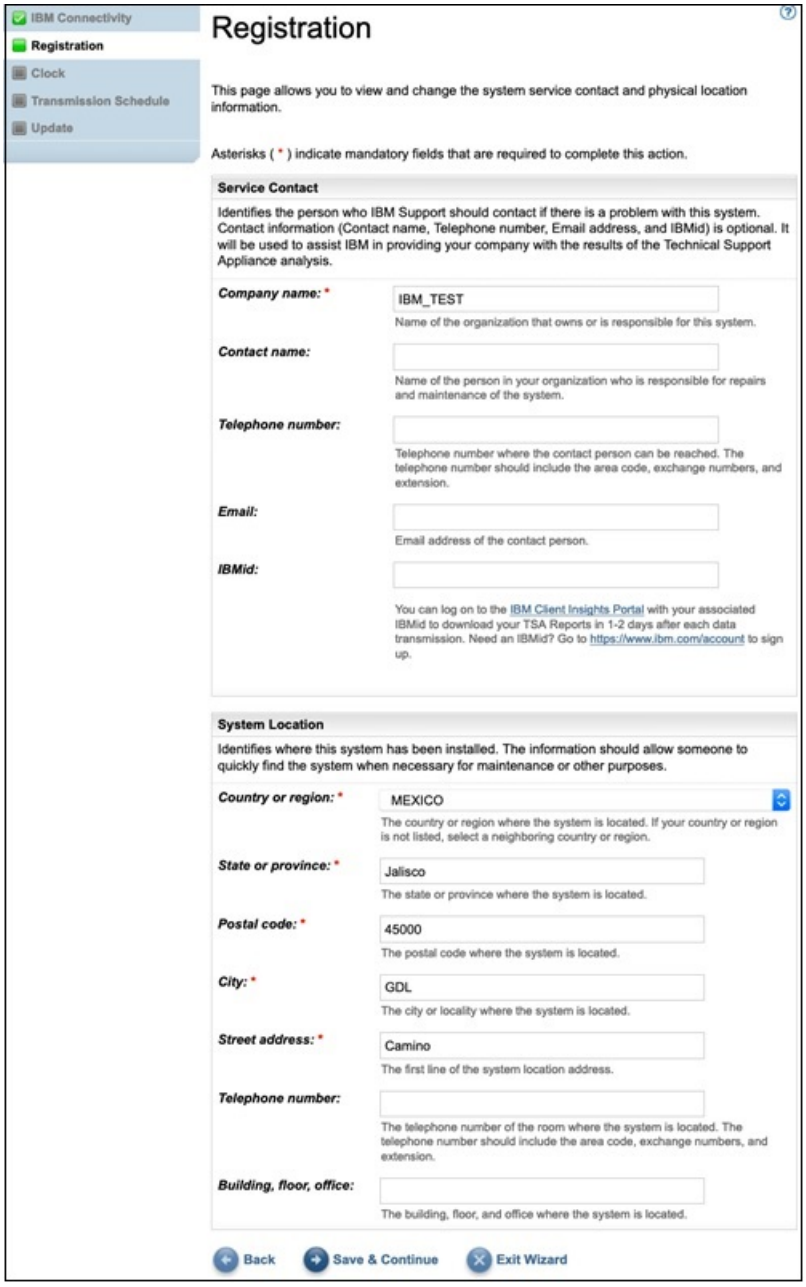

Abbildung 24. Registrierung

1. Geben Sie die Servicekontaktinformationen in folgenden Feldern an:

   Firmenname
   Der Name des Unternehmens, das die TSA verwendet.

   Kontaktname
   (Optional) Der Name der Person im Unternehmen, die für die TSA verantwortlich ist.

   Telefonnummer
   (Optional) Die Telefonnummer, unter der die Kontaktperson erreicht werden kann. Die Telefonnummer muss Vorwahl, Telefonzentrale und Durchwahlnummer enthalten. In der Telefonnummer dürfen keine Klammern enthalten sein.

   E-Mail
   (Optional) Die E-Mail-Adresse der Kontaktperson.

IBMid
(Optional) Die IBMid der Person, die Sie zum Anzeigen der Berichte im IBM Client Insights Portal autorisieren möchten.

Anmerkung: Mit Ihrer zugewiesenen IBMid können Sie sich unter https://clientinsightsportal.ibm.com/ an, um Ihre TSA-Berichte innerhalb von 1-2 Tagen nach jeder Datenübertragung herunterzuladen. Um eine IBMid zu beantragen, rufen Sie die Seite https://www.ibm.com/account auf.

Anmerkung: Der Servicekontakt ist die Person, die vom IBM Support bei einem Problem mit dem System zu kontaktieren ist. Die Kontaktinformationen werden von IBM verwendet, um Ihrem Unternehmen die Ergebnisse der Analyse der Technical Support Appliance zu übermitteln.

2. Geben Sie den Standort der TSA in folgenden Feldern an:

Land oder Region
Das Land oder die Region, wo sich die TSA befindet.

Bundesland oder Provinz
Das Bundesland oder die Provinz, wo sich die TSA befindet. Falls Ihnen das Bundesland nicht bekannt ist, geben Sie *Unbekannt* ein.

Postleitzahl
Die Postleitzahl des Standorts, an dem sich die TSA befindet.

Ort
Die Stadt oder der Ort, wo sich die TSA befindet.

Straßenadresse
Die Adresse des TSA-Standorts.

Telefonnummer
(Optional) Die Telefonnummer des Raums, in dem sich die TSA befindet. Die Telefonnummer muss Vorwahl, Telefonzentrale und Durchwahlnummer enthalten. In der Telefonnummer dürfen keine Klammern enthalten sein.

Gebäude, Stockwerk, Büro
(Optional) Das Gebäude, Stockwerk und Büro, in dem sich die TSA befindet.

Nächste Schritte

- Klicken Sie auf **Speichern und Weiter**, um Registrierungsinformationen zu speichern und auf die Seite **Systemzeit** zu gehen.
- Klicken Sie auf **Zurück**, um zur Seite **IBM Konnektivität** zurückzukehren.

  -oder-
- Klicken Sie auf **Assistent verlassen**, um den **Installationsassistenten** zu verlassen und zur Seite **Zusammenfassung** zu gehen.

Systemzeit einstellen

Während der Einrichtung können Sie die Systemzeit für die TSA, das Datum und die örtliche Zeitzone festlegen.

Vorgehensweise

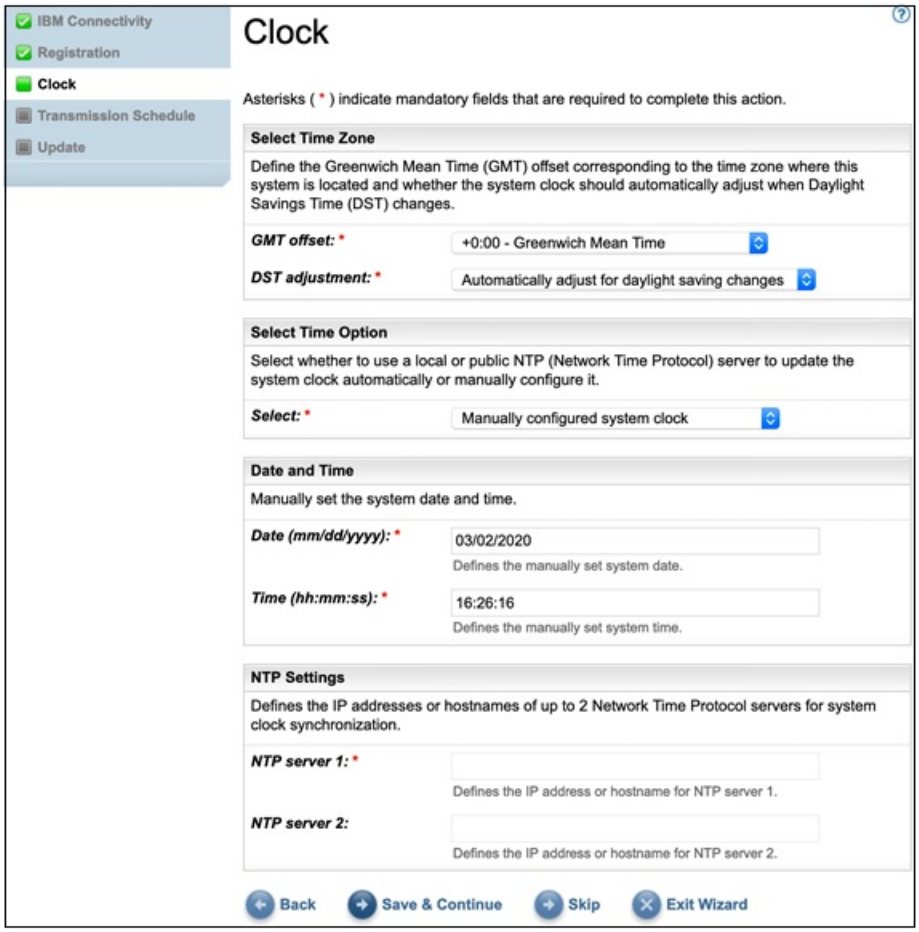

Abbildung 25. Systemzeit

1. Wählen Sie in der Dropdown-Liste **GMT-Abweichung** Ihre örtliche Zeitzone aus.
2. Wählen Sie in der Dropdown-Liste **Sommerzeitanpassung** die Anpassung für die Sommerzeit aus.

   Anmerkung: Die Sommerzeit gilt nicht in allen Zeitzonen. Wenn Sie diese Option für eine Zeitzone ohne Sommerzeit auswählen, wird eine Fehlernachricht angezeigt.
3. Wählen Sie in der Dropdown-Liste **Zeitoption auswählen** eine Methode für die Aktualisierung der Systemuhr aus.

   Die Systemuhr kann entweder automatisch durch Synchronisierung mit einem NTP-Server (Network Time Protocol) aktualisiert oder manuell eingestellt werden.

   a) Wenn Sie festgelegt haben, die Systemuhr manuell zu konfigurieren, stellen Sie das Datum und die Uhrzeit für das System ein. Geben Sie Datum und Uhrzeit in die Felder **Datum** und **Uhrzeit** ein.

   b) Wenn Sie festgelegt haben, die Systemuhr automatisch durch Synchronisierung mit einem NTP-Server zu aktualisieren, müssen Sie die IP-Adresse und den Hostnamen des NTP-Servers angeben. Tragen Sie in den **NTP-Server**-Feldern die IP-Adressen oder Hostnamen für bis zu zwei Server ein.

   Anmerkung: Vergewissern Sie sich, das der NTP-Server für die TSA über das Netz erreichbar ist.

Nächste Schritte

- Klicken Sie auf **Speichern und Weiter**, um Systemzeitinformationen zu speichern und auf die Seite **Übertragungszeitplan** zu gehen.

  -oder-
- Klicken Sie auf **Überspringen**, um zur Seite **Übertragungszeitplan** zu springen.

Einstellungen im vorherigen Schritt des Assistenten ändern

- Klicken Sie auf **Zurück**, um zur Seite **Registrierung** zurückzukehren.

Den Assistenten verlassen

- Klicken Sie auf **Assistent verlassen**, um den **Installationsassistenten** zu verlassen und zur Seite **Zusammenfassung** zu gehen.

Übertragungszeitplan einrichten

In der TSA ist ein Standardzeitplan definiert, nach dem der Übertragungsprozess zu bestimmten Zeiten ausgeführt wird. Sie können diesen Zeitplan gemäß Ihren Anforderungen ändern.

Vorgehensweise

1. Wählen Sie mithilfe der Dropdown-Listen **Stunde** und **Minute** einen neuen Zeitpunkt aus.
2. Legen Sie den **Tagauswahlmodus** fest.

Wöchentlich nach Tag(en) (So-Sa)
Um die Übertragung für einen bestimmten Tag oder mehrere Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus.

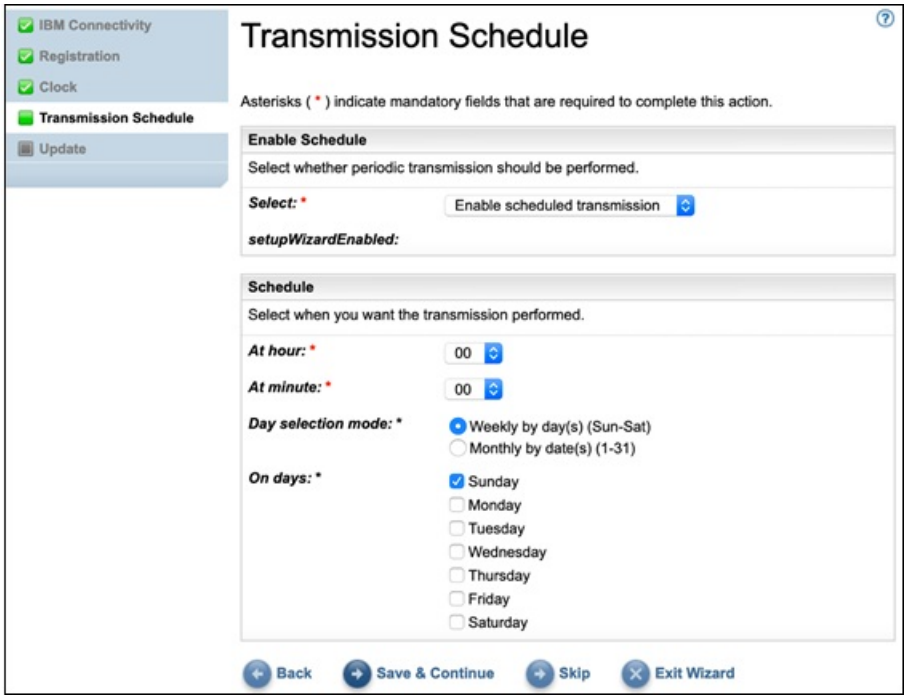

Abbildung 26. Wöchentlich nach Tag(en) (So-Sa)

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Wochentage aus.

Monatlich nach Datum (1-31)
Um die Übertragung für bestimmte Tage im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Tage im Monat aus.

Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.

Anmerkung: Stellen Sie sicher, dass die Startzeit der Erkennung vor der Übertragungszeit liegt, um lange Verzögerungen bei der Übertragung der neu erfassten Daten zu vermeiden.

Nächste Schritte

- Klicken Sie auf **Speichern und Weiter**, um den Übertragungszeitplan zu speichern und auf die Seite **Update** zu gehen.

  -oder-

- Klicken Sie auf **Überspringen**, um zur Seite **Update** zu springen.

Einstellungen im vorherigen Schritt des Assistenten ändern

- Klicken Sie auf **Zurück**, um zur Seite **Systemzeit** zurückzukehren.

Den Assistenten verlassen

- Klicken Sie auf **Assistent verlassen**, um den **Installationsassistenten** zu verlassen und zur Seite **Zusammenfassung** zu gehen.

Technical Support Appliance aktualisieren

Sie können die TSA auf die aktuellste verfügbare Version aktualisieren.

Wenn ein Update verfügbar ist, wird die folgende Seite **Update** angezeigt.

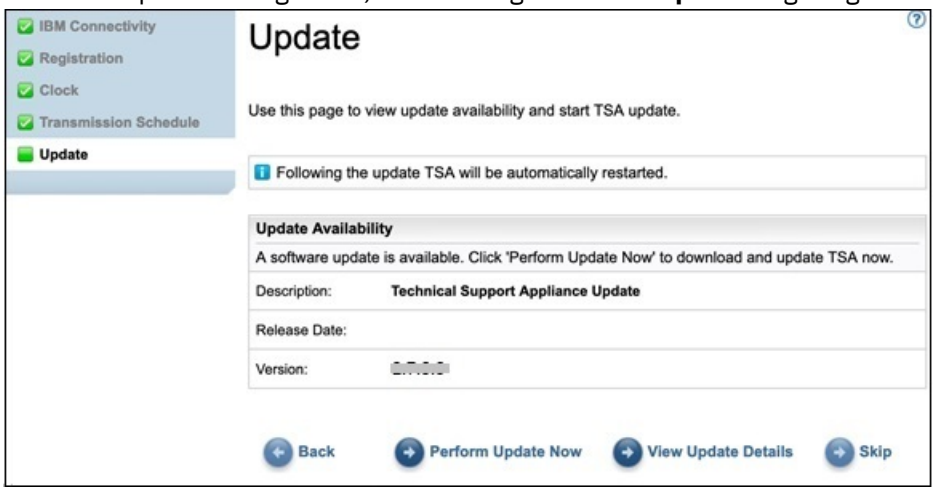

Abbildung 27. Updateverfügbarkeit

- Klicken Sie auf **Update jetzt ausführen**, um das Update zu installieren und den **Installationsassistenten** zu beenden.

  -oder-

- Klicken Sie auf **Updatedetails anzeigen**, um Informationen zum Inhalt des Updates anzuzeigen.

Einstellungen im vorherigen Schritt des Assistenten ändern

- Klicken Sie auf **Zurück**, um zur Seite **Übertragungszeitplan** zurückzukehren.

Den Assistenten beenden

- Klicken Sie auf **Überspringen**, um den **Installationsassistenten** zu beenden, ohne das Update anzuwenden.

Wenn kein Update verfügbar ist, wird die folgende Seite **Update** angezeigt.

Abbildung 28. Keine Updates verfügbar

- Klicken Sie auf **Installationsassistent beenden**, um den **Installationsassistenten** zu beenden. Die Seite **Installationsassistent beendet** wird angezeigt.

  -oder-

- Klicken Sie auf **Zurück**, um zur Seite **Übertragungszeitplan** zurückzukehren.

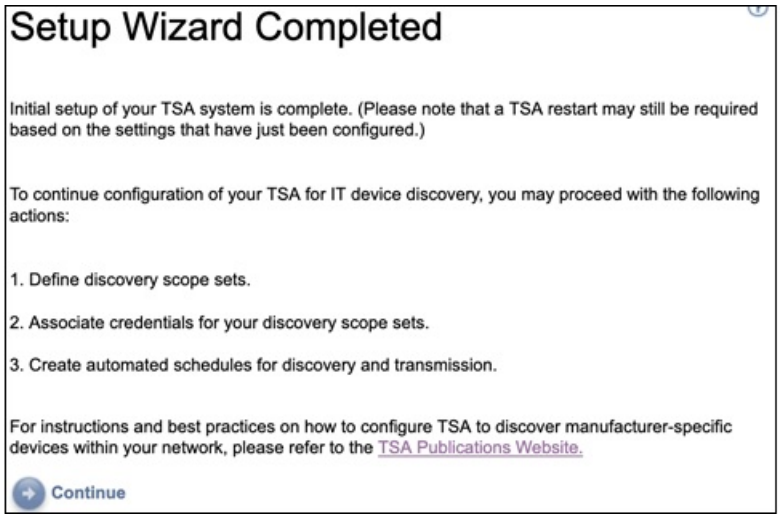

Abbildung 29. Installationsassistent beendet

- Klicken Sie auf **Weiter**, um zur Seite **Zusammenfassung** zu gehen.

  Anmerkung: Bei einigen Änderungen an der Seite **Systemzeit** ist ein Neustart erforderlich, damit die Änderungen wirksam werden. Beispielsweise werden Sie aufgefordert, das System neu zu starten, wenn Sie das Datum oder die Uhrzeit eingestellt haben oder von der manuellen Konfiguration zur NTP-Server-Konfiguration umgestiegen sind.

  – Klicken Sie auf **OK**, um den **Installationsassistenten** zu beenden und zur Seite **Zusammenfassung** zurückzukehren. Die Seite **Zusammenfassung** wird angezeigt und das System wird neu gestartet.

Anmerkung: Falls Sie die Konfiguration der Einstellungen im **Installationsassistenten** beenden oder überspringen, können Sie die Einstellungen über das Navigationsteilfenster der TSA manuell konfigurieren. Weitere Informationen zur Konfiguration dieser Einstellungen finden Sie im Abschnitt Anhang A, „Die Technical Support Appliance konfigurieren”, auf Seite 121.

Netzeinstellungen konfigurieren

Für die Installation der TSA müssen grundlegende Netzeinstellungen konfiguriert werden. Wenn diese Einstellungen für Ihr IT-Netz geeignet sind, können Sie diesen Abschnitt überspringen.

Vorbereitende Schritte

Verwenden Sie die Seite **Netz**, um folgende Aufgaben durchzuführen:

- Die ursprünglichen grundlegenden Netzeinstellungen ändern
- Die TSA für den Zugriff auf mehrere Netze konfigurieren

Führen Sie zum Konfigurieren der grundlegenden Netzeinstellungen über die Konsole die im Abschnitt „Netzdetails konfigurieren” auf Seite 19 beschriebenen Schritte durch.

Grundlegende Netzeinstellungen konfigurieren

Verwenden Sie die Seite **Netz**, um ursprüngliche Netzeinstellungen zu ändern.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Netz**.
   Die Seite **Netz** wird angezeigt.

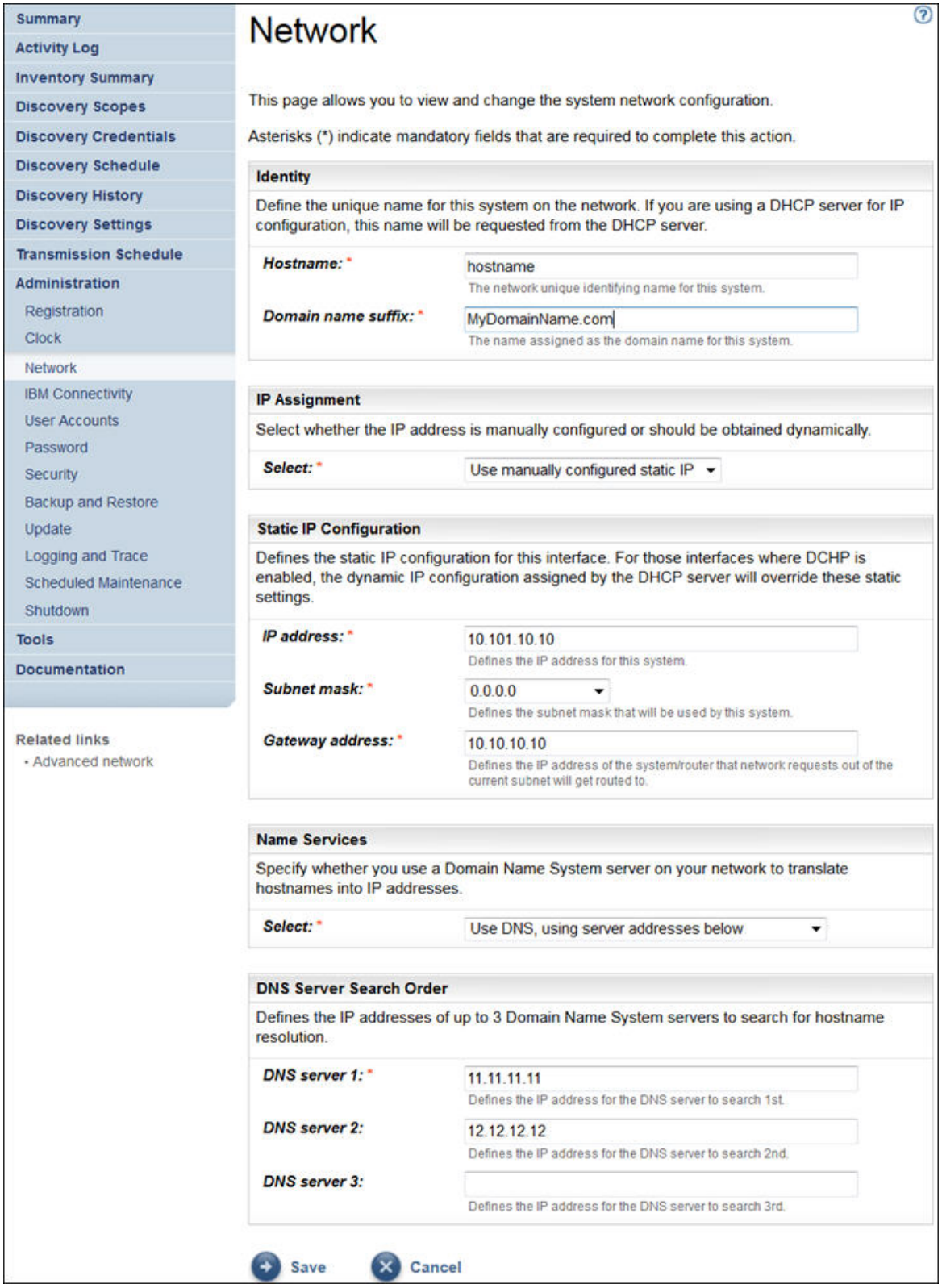

Abbildung 30. Netz

2. Geben Sie im Feld **Hostname** einen eindeutigen Namen für dieses System im lokalen Netz an.
3. Geben Sie im Feld **Domänennamenssuffix** den Namen an, der als Domänenname für dieses System im lokalen Netz verwendet wird.

4. Wählen Sie unter *IP-Adressenzuweisung* die Option **Manuell konfigurierte statische IP verwenden** aus. Weitere Informationen zur DHCP-Adressenzuweisung finden Sie im Abschnitt Anhang B, „DHCP-Netzdetails konfigurieren", auf Seite 131.
5. Konfigurieren Sie die statische IP-Adresse:
   a) Geben Sie im Feld **IP-Adresse** die IP-Adresse für dieses System ein.
   b) Wählen Sie in der Dropdown-Liste **Teilnetzmaske** die Teilnetzmaske aus, die von diesem System verwendet werden soll.
   c) Geben Sie im Feld **Gateway-Adresse** die IP-Adresse des Systems oder Routers an, das oder der Anforderungen außerhalb des aktuellen Teilnetzes abwickelt.
6. Geben Sie die **Namensservices** gemäß der IP-Zuweisung an.
   a) Wählen Sie bei manuell konfigurierten statischen IP-Adressen die Option **DNS mit den unten angegebenen Serveradressen verwenden** aus.
   b) Wählen Sie bei DHCP-IP-Adressenzuweisung die Option **DNS verwenden, aber Serveradressen über DHCP abrufen** aus.
7. Tragen Sie bis zu drei IP-Adressen für DNS-Server (Domain Name System) ein, die bei der Auflösung von Hostnamen verwendet werden sollen.

   Die TSA sucht die Server in der Reihenfolge, in der sie aufgeführt sind.
8. Klicken Sie auf **Speichern**, um die Netzeinstellungen zu speichern.

   Anschließend werden Sie aufgefordert, das System neu zu starten.

   

   Vorsicht: Gehen Sie beim Ändern von Netzeinstellungen sehr vorsichtig vor. Falls bei der Netzkonfiguration ein Fehler gemacht wird, ist die TSA-Benutzerschnittstelle womöglich nicht mehr erreichbar. In diesem Fall muss die TSA-Konsole verwendet werden, um die Netzkonfiguration zu reparieren:

   - Für VMware: Verwenden Sie die VMware ESXi-Webschnittstelle oder den VMware vSphere Client.
   - Für Microsoft Hyper-V: Verwenden Sie den Hyper-V Manager.
9. Klicken Sie auf **Abbrechen**, wenn Sie die Seite **Netz** verlassen möchten, ohne die Einstellungen zu speichern.

Erweiterte Netzeinstellungen konfigurieren

Wenn Sie die TSA für den Zugang zu mehreren Netzen konfigurieren möchten, können Sie auf der Seite **Netz (erweitert)** die entsprechenden Netzeinstellungen festlegen.

Führen Sie zum Konfigurieren von erweiterten Netzeinstellungen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Netz**.
2. Klicken Sie unterhalb des Navigationsbereichs unter **Zugehörige Links** auf **Erweitertes Netz**.

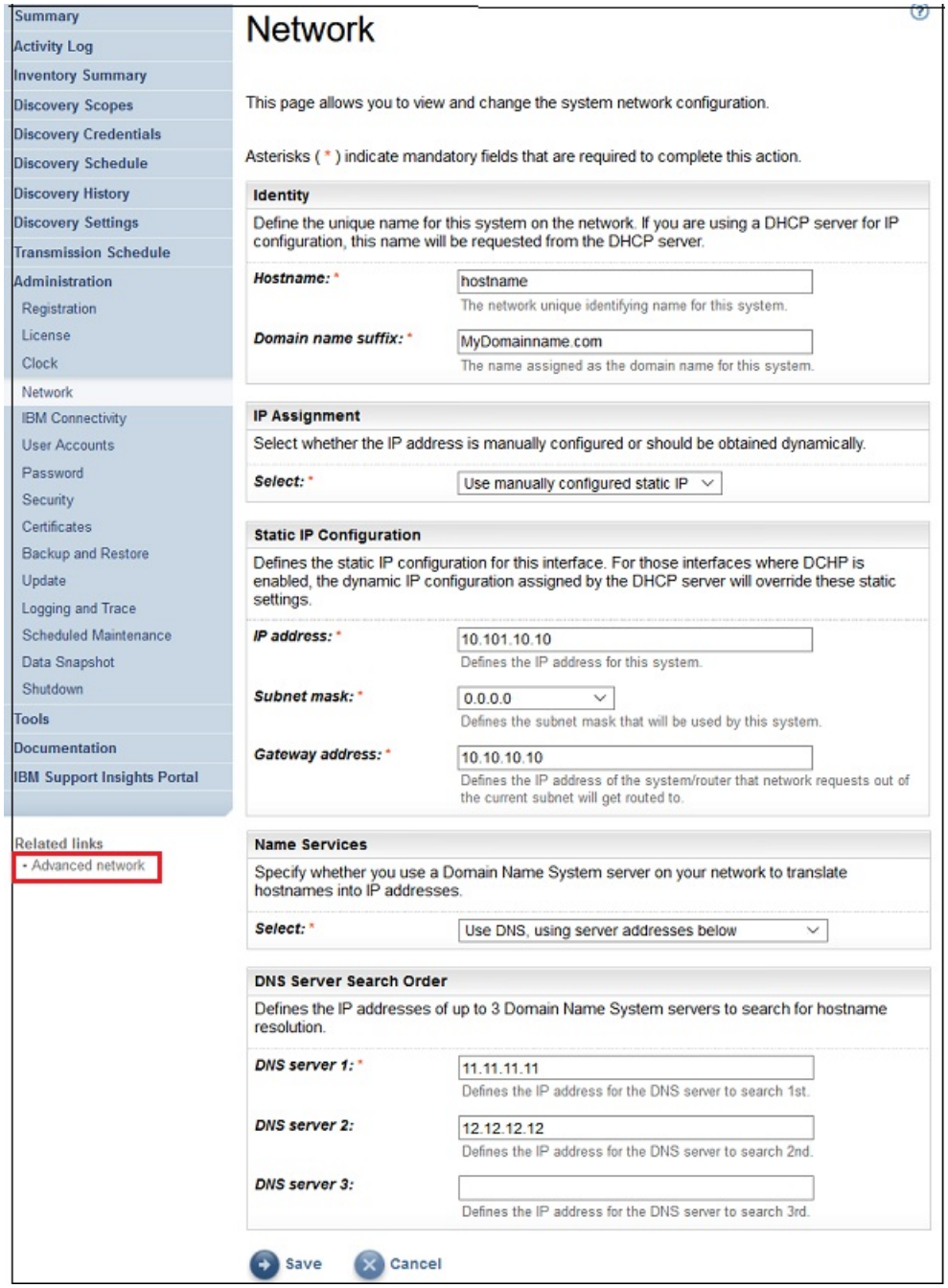

Abbildung 31. Auf die Seite Netz (erweitert) zugreifen

Die Seite **Netz (erweitert)** wird angezeigt.

Die Seite **Netz (erweitert)** besteht aus folgenden Unterseiten:

- Global
- Netzschnittstellen
- DNS-Einstellungen
- Netzrouten

Zum Aufrufen dieser Unterseiten klicken Sie auf die Registerkarte der anzuzeigenden Seite.

Wichtig: Bevor Sie eine Seite verlassen, müssen Sie auf **Speichern** klicken, um eventuelle Änderungen an Feldern auf dieser Seite zu speichern. Sie werden aufgefordert, das System neu zu starten, damit die Änderungen wirksam werden.

Global

Verwenden Sie diese Seite, um globale Netzeinstellungen anzuzeigen und zu ändern:

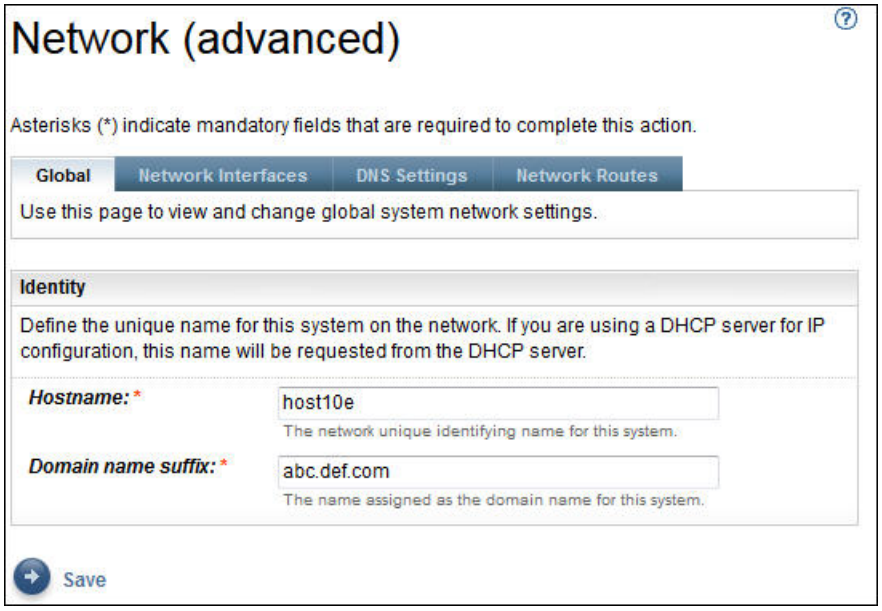

Abbildung 32. Netz (erweitert) – Global

Identität

Definieren Sie die Identität dieses Systems im Netz.

1. Geben Sie im Feld **Hostname** einen eindeutigen Namen für dieses System an.
2. Geben Sie im Feld **Domänennamenssuffix** den Namen an, der als Domänenname für dieses System verwendet wird.

Netzschnittstellen

Die TSA ist für die Verwendung von zwei Netzschnittstellencontrollern (NICs) konfiguriert – eth0 und eth1. Verwenden Sie diese Seite, um die aktuellen Einstellungen für die ausgewählte Netzschnittstelle anzuzeigen und zu ändern.

1. Klicken Sie auf **eth0**, um die eth0-Netzschnittstelle auszuwählen.
2. Klicken Sie auf **eth1**, um die eth1-Netzschnittstelle auszuwählen.

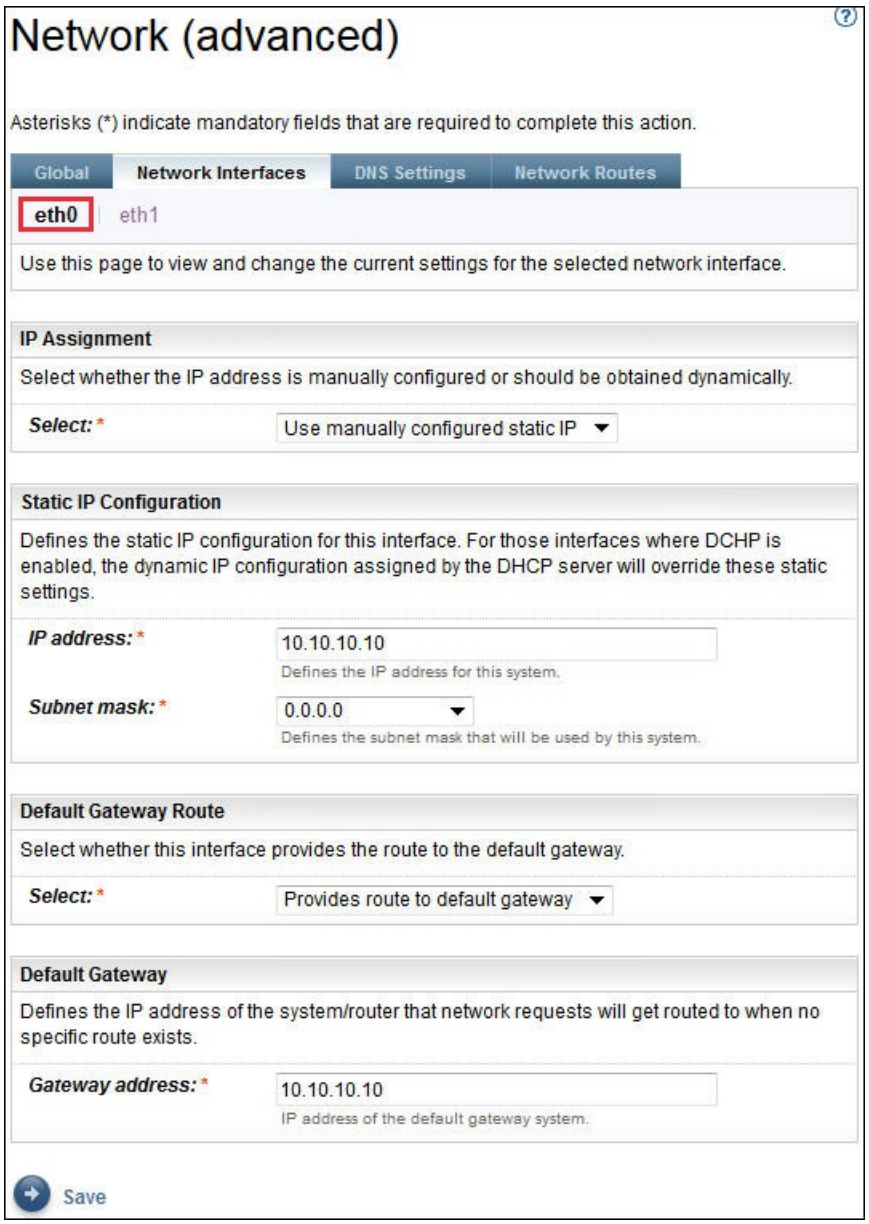

Abbildung 33. Netz (erweitert) – Netzschnittstellen

IP-Adressenzuweisung

Wählen Sie eine Methode für die Zuweisung der IP-Adresse zu diesem System aus. Die möglichen Optionen sind dynamisches Abrufen der IP-Adresse von einem DHCP-Server oder Verwenden einer manuell konfigurierten statischen IP-Adresse. Wenn Sie eine manuell konfigurierte statische IP-Adresse verwenden möchten, müssen Sie auf dieser Seite die IP-Adresse des Systems konfigurieren.

Statische IP-Konfiguration

Wenn Sie ausgewählt haben, eine manuell konfigurierte statische IP-Adresse zu verwenden, geben Sie hier die IP-Informationen für die Netzschnittstelle wie folgt an:

1. Geben Sie im Feld **IP-Adresse** die IP-Adresse für dieses System an.
2. Wählen Sie in der Dropdown-Liste **Teilnetzmaske** die Teilnetzmaske aus, die von diesem System verwendet werden soll.

Standardgateway-Route

Geben Sie an, ob diese Netzschnittstelle eine Route zum Standardgateway bereitstellen soll.

Standardgateway

Geben Sie im Feld **Gateway-Adresse** die IP-Adresse des Standardgateways für dieses System an.

DNS-Einstellungen

Verwenden Sie diese Seite zum Anzeigen und Ändern der DNS-Einstellungen.

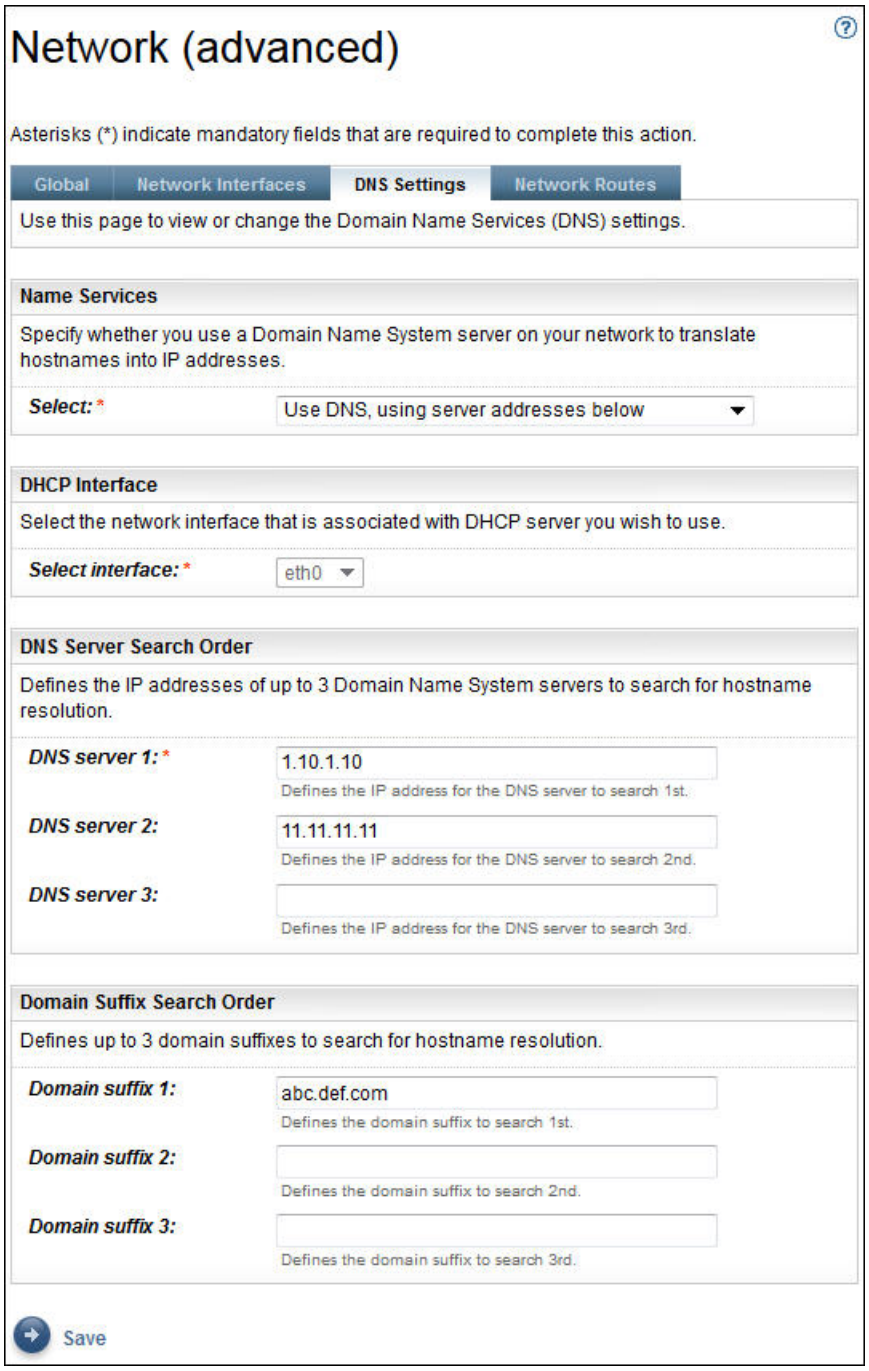

Abbildung 34. Netz (erweitert) – DNS-Einstellungen

Namensservices

Geben Sie ein Domain Name System (DNS) in Ihrem Netz an, um Hostnamen in IP-Adressen umzuwandeln. Sie können zwischen folgenden Optionen wählen:

- DNS verwenden, aber Serveradressen über DHCP abrufen:

Wenn Sie diese Option auswählen, müssen Sie die Netzschnittstelle angeben, die dem zu verwendenden DHCP-Server zugeordnet ist.

- DNS mit den unten angegebenen Serveradressen verwenden:

  Wenn Sie diese Option auswählen, müssen Sie auf dieser Seite mindestens einen DNS-Server angeben.

DHCP-Schnittstelle
Wählen Sie die Netzschnittstelle aus, die dem zu verwendenden DHCP-Server zugeordnet ist.

DNS-Server-Suchreihenfolge
Wenn Sie ausgewählt haben, DNS mit selbst angegebenen Serveradressen zu verwenden, geben Sie bis zu drei IP-Adressen für DNS-Server (Domain Name System) an, die bei der Auflösung von Hostnamen verwendet werden sollen. Die TSA sucht die Server in der Reihenfolge, in der sie aufgeführt sind.

Domänensuffix-Suchreihenfolge
Wenn Sie ausgewählt haben, DNS mit selbst angegebenen Serveradressen zu verwenden, geben Sie bis zu drei Domänennamenssuffixe an, die bei der Auflösung von Hostnamen verwendet werden sollen. Die TSA sucht die Domänennamenssuffixe in der Reihenfolge, in der sie aufgeführt sind.

Netzrouten

Verwenden Sie diese Seite zum Anzeigen, Hinzufügen, Ändern oder Löschen von statischen Routingeinträgen.

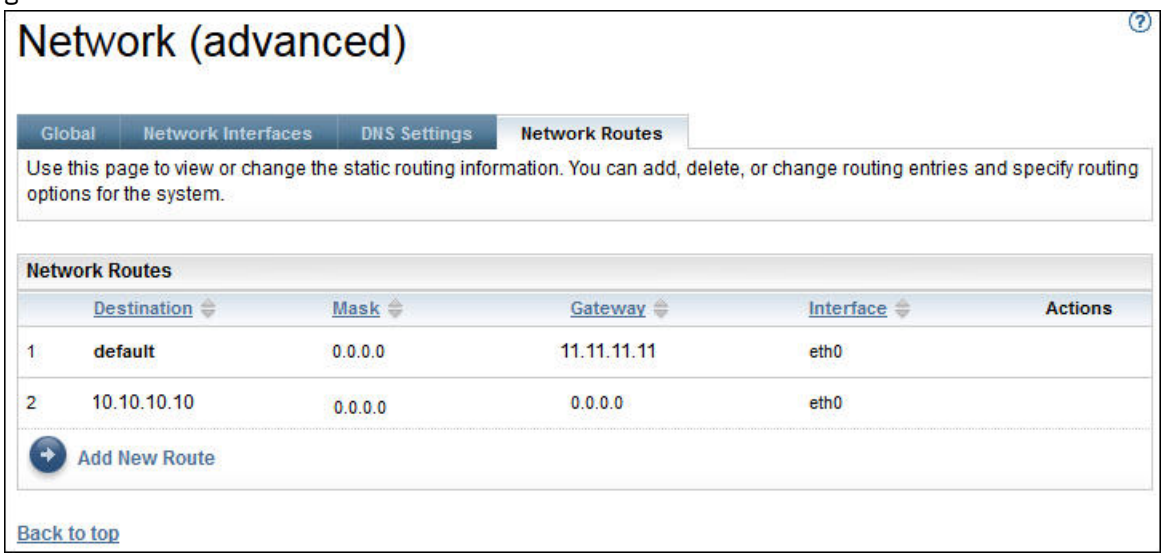

Abbildung 35. Netz (erweitert) – Netzrouten

Zu jeder Netzroute werden folgende Informationen angezeigt:

Ziel

Gibt die TCP/IP-Host- oder Teilnetzadresse des Zielnetzes an.

Maske
Gibt die Teilnetzmaske an die beim Hinzufügen einer Route als Netzmaske verwendet werden soll. Dies ist die Teilnetzadresse für den Hostabschnitt der IP-Adresse. Netzschnittstellen können verschiedene Teilnetzmasken verwenden, was bedeutet, dass Routen durch Auswahl einer Teilnetzmaske hinzugefügt werden können (variable Teilnetzrouten). Die beim Hinzufügen einer Route auszuwählenden Teilnetzmasken müssen in 32-Bit-Schreibweise mit Trennzeichen formatiert sein.

Gateway
Die TCP/IP-Gateway-Adresse für das Routing der IP-Pakete.

Schnittstelle
Wählen Sie im Menü den gewünschten Adapter aus. Dies ist der Name des Netzadapters, der der Netzroute zugeordnet wird.

Aktionen

Klicken Sie auf das Symbol **Löschen** ( ), um die Route zu löschen.

Anmerkung: Die beiden Routen in der Abbildung können weder geändert noch gelöscht werden.

Klicken Sie auf **Neue Route hinzufügen**, um eine neue statische Netzroute zu definieren. Die Seite **Netzroute** wird angezeigt.

Netzrouten hinzufügen

Sie können statische Netzrouten hinzufügen.

Vorgehensweise

Führen Sie zum Hinzufügen einer Netzroute die folgenden Schritte durch:

1. Klicken Sie auf der Seite **Netz (erweitert) – Netzrouten** auf **Neue Route hinzufügen**. Die Seite **Netzroute** wird angezeigt.

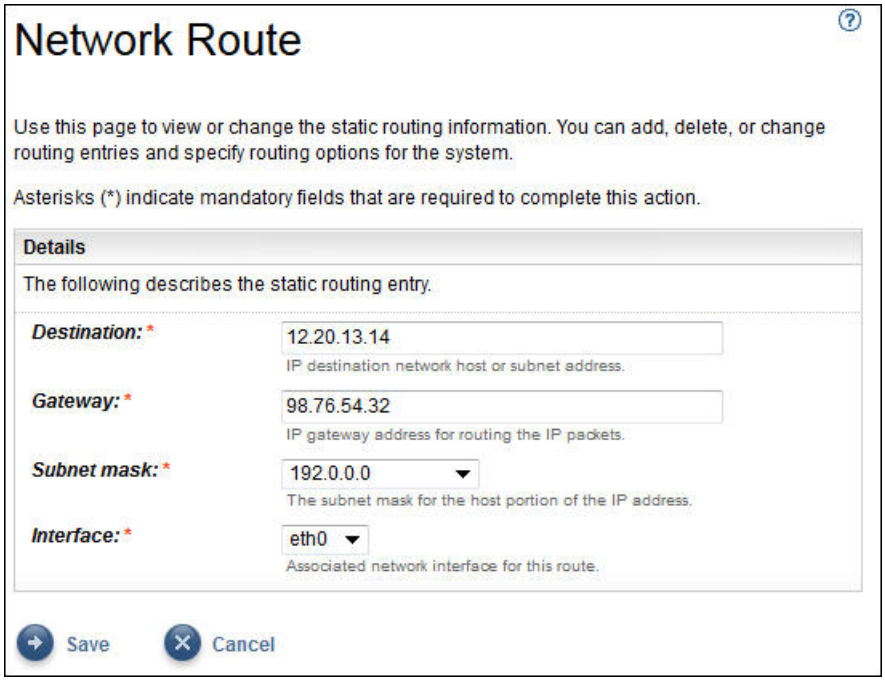

Abbildung 36. Neue Netzroute

2. Geben Sie im Feld **Ziel** die IP-Adresse für den Host oder das Teilnetz des TCP/IP-Zielnetzes ein.
3. Geben Sie im Feld **Gateway** die TCP/IP-Gateway-Adresse für das Routing der Informationen ein. Die Adresse muss in 32-Bit-Schreibweise mit Trennzeichen angegeben werden. Beispiel: `xxx.xxx.xxx.xxx`.
4. Wählen Sie in der Dropdown-Liste **Teilnetzmaske** die Teilnetzmaske aus, die als Netzmaske für diese Route verwendet werden soll.
5. Wählen Sie in der Dropdown-Liste **Schnittstelle** den Netzadapter aus, der dieser Route zugeordnet werden soll.
6. Klicken Sie auf **Speichern**, um diese Netzroute zu speichern.

Zertifikate einrichten

Auf der Seite **Zertifikate** können Sie Zertifikatsignaturdaten anzeigen, Zertifikate generieren und installieren sowie Zertifikate importieren. Diese Serverzertifikate präsentiert die TSA gegenüber dem Webserver, wenn die Benutzerschnittstelle aufgerufen wird.

In der Standardkonfiguration implementiert die TSA ein allgemeines selbst signiertes SSL-Serverzertifikat, um die Einrichtung zu ermöglichen. Zur Erhöhung der Sicherheit empfehlen wir Ihnen, das Standardzerti-

fikat nach Abschluss der erstmaligen Bereitstellungs- und Konfigurationsschritte zu ersetzen. In der TSA können Sie ein selbst signiertes SSL-Serverzertifikat generieren und installieren, das für diese TSA eindeutig ist, ein von einer Zertifizierungsstelle Ihrer Wahl signiertes benutzerdefiniertes Zertifikat generieren und installieren oder eine eigene Java-Keystore-Datei hochladen, die ein benutzerdefiniertes SSL-Serverzertifikat enthält.

Ein benutzerdefiniertes Zertifikat kann auf die folgenden Arten installiert werden:

- „Benutzerdefiniertes Zertifikat installieren (mit Unterzeichnern)” auf Seite 44
- „Benutzerdefiniertes Zertifikat installieren (Alternativmethode) ” auf Seite 45

Status des SSL-Serverzertifikats anzeigen

Beim Konfigurieren der TSA wird das im Lieferumfang der Technical Support Appliance enthaltene TSA-Standardzertifikat installiert.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Zertifikate**.
   Die Seite **Zertifikate** wird angezeigt.

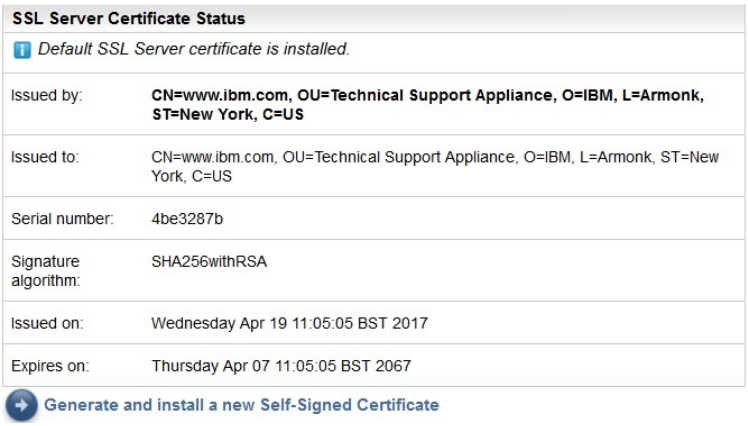

Abbildung 37. Status des SSL-Serverzertifikats

   Im Abschnitt **Status des SSL-Serverzertifikats** finden Sie Informationen zum SSL-Serverzertifikat, das in TSA installiert ist. Folgende Zertifikatsinformationen werden angezeigt: *Ausgestellt durch*, *Ausgestellt für*, *Ausgestellt am*, *Ablauf am*, *Seriennummer* und *Signaturalgorithmus*.
2. Klicken Sie auf **Neues selbst signiertes Zertifikat generieren und installieren**, um ein selbst signiertes Zertifikat zu installieren, das für diese TSA eindeutig ist. Daraufhin wird ein Warnhinweis angezeigt, dass nach dem Erstellen und Installieren eines selbst signierten Zertifikats automatisch ein Neustart der Appliance durchgeführt wird.

   Anmerkung: Die Schaltfläche **Neues selbst signiertes Zertifikat generieren und installieren** ist nur sichtbar, wenn das Standardzertifikat in der TSA installiert ist.

CSR generieren und herunterladen

Zum Anfordern eines von einer Zertifizierungsstelle ausgestellten SSL-Zertifikats müssen Sie die folgenden Informationen angeben, um eine CSR-Datei (Certificate Signing Request) zu generieren und herunterzuladen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Zertifikate**.
   Die Seite **Zertifikate** wird angezeigt.

Abbildung 38. Zertifikatssignieranforderung

2. Geben Sie im Feld **Allgemeiner Name** den vollständig qualifizierten Hostnamen (FQDN) der TSA ein. Die Zeichenzahl muss zwischen 1 und 64 Zeichen liegen.
3. Geben Sie im Feld **Organisationseinheit** den Organisationsnamen an, der zur Bezeichnung verschiedener Abteilungen innerhalb eines Unternehmens verwendet wird.
4. Geben Sie im Feld **Organisation** den Namen des Unternehmens bzw. der Kommanditgesellschaft, Universität oder Regierungsbehörde an.
5. Geben Sie im Feld **Ort** den Namen des Orts an, an dem die TSA ausgeführt wird.
6. Geben Sie im Feld **Bundesland** das Bundesland an, in dem die TSA ausgeführt wird. Falls Ihnen das Bundesland nicht bekannt ist oder Bundesland nicht für Ihr Land zutrifft, geben Sie *Unbekannt* ein.
7. Wählen Sie im Dropdown-Menü **Land** das Land aus, in dem die TSA ausgeführt wird.
8. Geben Sie im Feld **Anzahl der Tage bis Ablauf** die Anzahl von Tagen ein, für die das Zertifikat gültig ist, beginnend ab dem Zeitpunkt der Erstellung des Zertifikats.
9. Klicken Sie auf **CSR-Datei (Certificate Signing Request) generieren und herunterladen**, um die CSR-Datei mit den angegebenen Informationen herunterzuladen.

   Anmerkung: Weitere Informationen zur Wiederherstellung des Standardzertifikats, das in der TSA enthalten ist, finden Sie im Abschnitt „Standardzertifikat wiederherstellen” auf Seite 46.

Benutzerdefiniertes Zertifikat installieren (mit Unterzeichnern)

Verwenden Sie diese Funktion zum Installieren eines benutzerdefinierten Zertifikats. Sie benötigen das von einer Zertifizierungsstelle generierte Serverzertifikat, das Stammzertifikat für die Zertifizierungsstelle sowie Zwischenzertifikate für die Zertifizierungsstelle.

Vorbereitende Schritte

Stellen Sie sicher, dass die Zertifikatsdateien (Stamm-, Zwischen- und Serverzertifikat) eines der folgenden Formate aufweisen:

- *.crt*
- *.der*
- *.pem*

Vorgehensweise

Führen Sie zum Hochladen und Installieren der Zertifikate in der TSA die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Zertifikate**.

   Die Seite **Zertifikate** wird angezeigt.

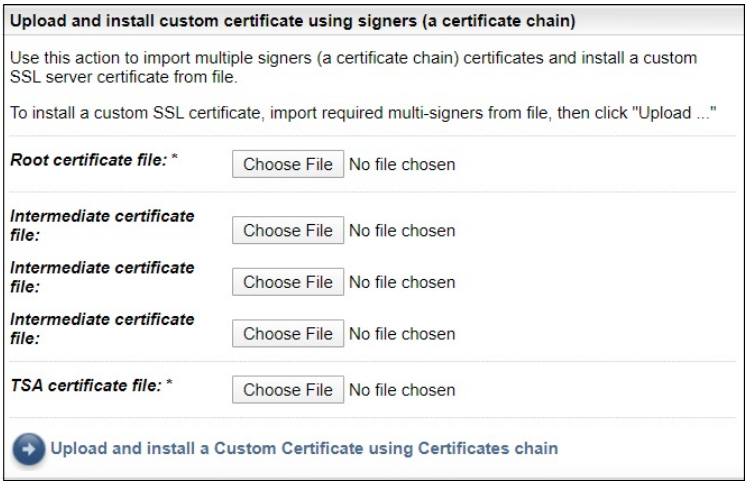

Abbildung 39. Benutzerdefiniertes Zertifikat installieren

2. Geben Sie im Feld **Stammzertifikatsdatei** den Speicherort der Stammzertifikatsdatei an, die Sie in der TSA installieren möchten.
3. Geben Sie im Feld **Zwischenzertifikatsdatei** den Speicherort der Zwischenzertifikatsdatei an, die Sie in der TSA installieren möchten.

   Anmerkung: Entsprechend den verschiedenen Unterzeichnern, die importiert werden, können mehrere Zwischenzertifikatsdateien (maximal 3) vorhanden sein.
4. Geben Sie im Feld **TSA-Zertifikatsdatei** den Speicherort der TSA-Zertifikatsdatei an, die Sie in der TSA installieren möchten.
5. Klicken Sie auf **Angepasstes Zertifikat mithilfe der Zertifikatskette hochladen und installieren**, um alle von Ihnen angegebenen Dateien (*Stammzertifikatsdatei*, *Zwischenzertifikatsdateien* und *TSA-Zertifikatsdatei*) hochzuladen und ein benutzerdefiniertes Zertifikat unter Verwendung der Zertifikatskette zu installieren.

   Anmerkung: Weitere Informationen zur Wiederherstellung des Standardzertifikats, das in der TSA enthalten ist, finden Sie im Abschnitt „Standardzertifikat wiederherstellen” auf Seite 46.

Benutzerdefiniertes Zertifikat installieren (Alternativmethode)

Verwenden Sie diese Funktion zum Installieren eines benutzerdefinierten Zertifikats. Sie können diese Funktion für die Bereitstellung einer bereits erstellten vollständigen Java-Keystore-Datei verwenden.

Vorbereitende Schritte

Es wird empfohlen, zur Bereitstellung eines benutzerdefinierten Zertifikats die Funktionen **Signieranforderung an Zertifizierungsstelle** und **Benutzerdefiniertes Zertifikat mit Unterzeichnern (Zertifikatskette) hochladen und installieren** auf der Seite **Zertifikate** zu verwenden. Falls Sie jedoch bereits unabhängig davon eine vollständige Java-Keystore-Datei mit Schlüsseln, benutzerdefiniertem Zertifikat und relevanten CA-Zertifikaten erstellt haben, können Sie mit dieser Funktion die Keystore-Datei implementieren. Dabei müssen Sie den Speicherort und das Kennwort für die Keystore-Datei angeben.

Anmerkung: Stellen Sie beim Erstellen der Keystore-Datei sicher, dass Schlüsseleintragskennwort und Keystore-Kennwort identisch sind.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Zertifikate**.

   Die Seite **Zertifikate** wird angezeigt.

Abbildung 40. Benutzerdefiniertes Zertifikat installieren

2. Führen Sie zum Installieren eines benutzerdefinierten Serverzertifikats die folgenden Schritte durch:
   a) Geben Sie im Feld **Zertifikatskennwort** das Kennwort für das Zertifikat ein.
   b) Geben Sie im Feld **Kennwortbestätigung** das Kennwort erneut ein.

      Bevor das Kennwort gespeichert wird, werden die beiden von Ihnen eingegebenen Kennwörter verglichen, um zu bestätigen, dass sie übereinstimmen.
   c) Geben Sie im Feld **Datei mit angepasstem Zertifikat** den Speicherort der Java-Keystore-Datei an, die das benutzerdefinierte Zertifikat enthält.
   d) Klicken Sie auf **Vollständige JKS-Datei hochladen und installieren**, um die angegebene Java-Keystore-Datei hochzuladen und ein benutzerdefiniertes Zertifikat zu installieren. Die Java-Keystore-Datei muss das benutzerdefinierte Zertifikat sowie alle relevanten Stamm- und Zwischenzertifikate der Zertifizierungsstelle (CA) enthalten. Die Appliance wird neu gestartet, um die Nutzung des neuen Zertifikats zu aktivieren.

   Anmerkung: Weitere Informationen zur Wiederherstellung des Standardzertifikats, das in der TSA enthalten ist, finden Sie im Abschnitt „Standardzertifikat wiederherstellen” auf Seite 46.

Ergebnisse

Nachdem das neue Zertifikat installiert ist, wird TSA automatisch neu gestartet. Nach dem Neustart wird in Ihrem Browser eventuell ein Sicherheitshinweis mit der Frage angezeigt, ob das neue Zertifikat als vertrauenswürdig anerkannt werden soll.

Standardzertifikat wiederherstellen

Verwenden Sie zur Wiederherstellung des Standardzertifikats, das in der TSA enthalten ist, die TSA-Konsole und wählen Sie die Option **Set Appliance certificate to default** aus.

Vorgehensweise

1. Starten Sie die TSA-Konsole.
2. Wählen Sie im **TSA-Konfigurationsmenü** die Option **3) Set Appliance certificate to default** aus.

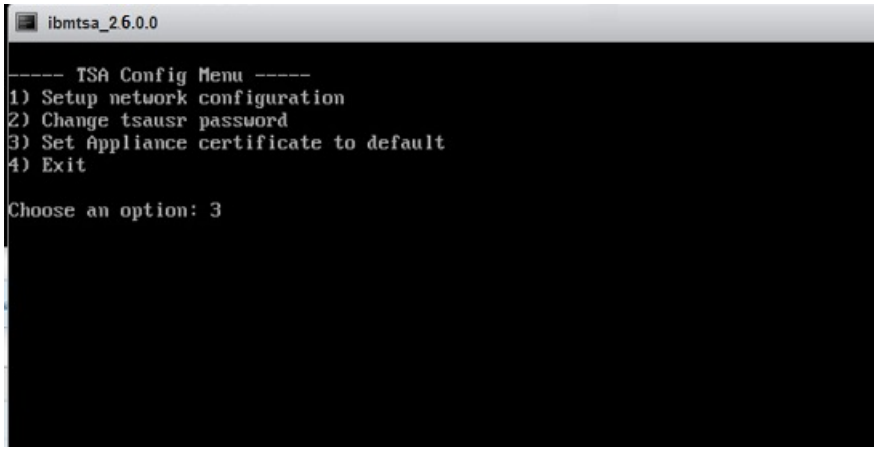

Abbildung 41. Appliance-Zertifikat auf Standardzertifikat festlegen

3. **Confirm setting appliance certificate to default certificate [y|n]:** Geben Sie **y** ein, um das Zurücksetzen des TSA-Zertifikats auf das Standardzertifikat zu bestätigen.

Ergebnisse

Wenn das Standardzertifikat installiert ist, wird die TSA nach 5 Sekunden automatisch neu gestartet. Nach dem Neustart wird in Ihrem Browser eventuell ein Sicherheitshinweis mit der Frage angezeigt, ob das Standardzertifikat als vertrauenswürdig anerkannt werden soll.

Bereinigung von Bestandsdaten planen

Sie können für alle Bestandsdaten, die auf den Ressourcen erfasst werden, ab dem Zeitpunkt der Erkennung eine Bereinigungstask planen oder manuell ausführen.

Informationen zu diesem Vorgang

Achtung: Für die meisten Installation wird empfohlen, die Bereinigungstask einmal wöchentlich auszuführen.

Um den aktuellen Zeitplan für die Bestandsbereinigungstask anzuzeigen, wählen Sie **Bestandszusammenfassung** > **Zeitplan für Bestandsbereinigung** aus.

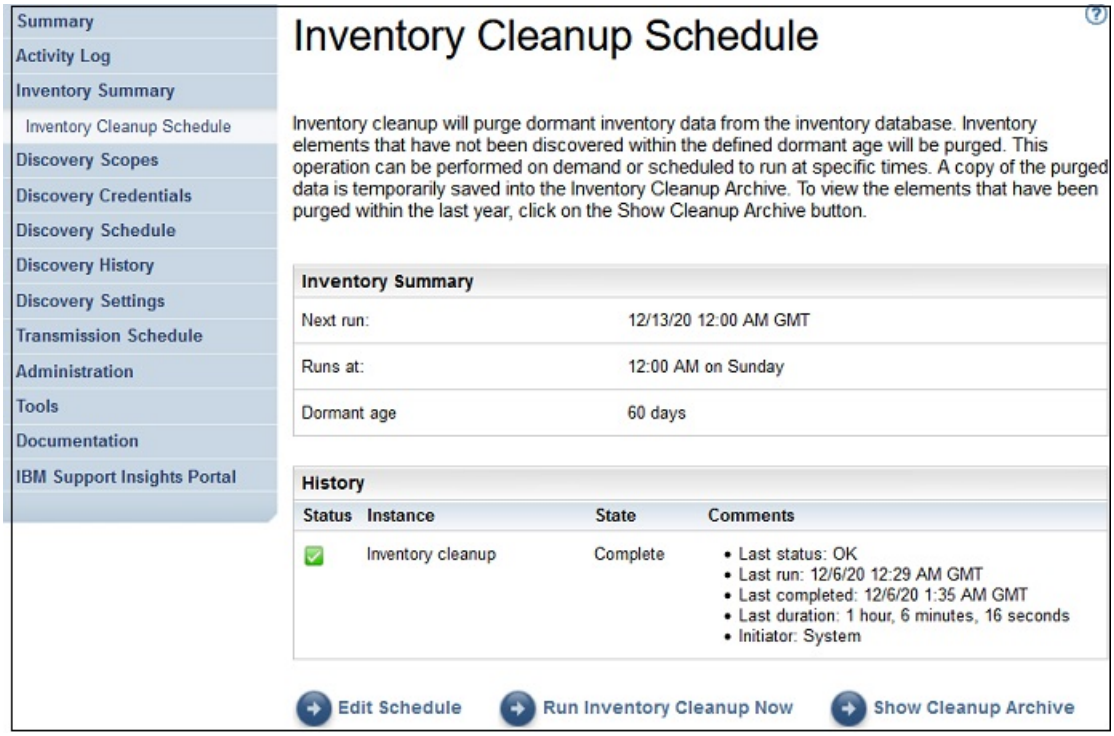

Abbildung 42. Zeitplan für Bestandsbereinigung

Klicken Sie auf **Bestandsbereinigung jetzt ausführen**, um die Bestandsbereinigung manuell zu starten.

Um den aktuellen Bestandsbereinigungszeitplan zu bearbeiten, zu aktivieren oder zu inaktivieren, führen Sie die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie auf der Seite **Zeitplan für Bestandsbereinigung** auf **Zeitplan bearbeiten**.
2. Wählen Sie auf der Seite **Bestandsdateneinstellungen** die Option **Geplante Bestandsbereinigung aktivieren** aus, um die Bestandsbereinigungstask zu aktivieren, oder die Option **Geplante Bestandsbereinigung inaktivieren**, um die Bestandsbereinigungstask zu inaktivieren.
3. Wenn Sie die Bestandsbereinigungstask aktivieren, führen Sie danach die folgenden Schritte durch:
   a) Wählen Sie mithilfe der Dropdown-Listen **Stunde** und **Minute** einen neuen Zeitpunkt aus.
   b) Legen Sie den **Tagauswahlmodus** fest. Um die Bestandsdatenbereinigung für einen bestimmten Tag oder mehrere Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus. Um die Bestandsdatenerfassung für einen bestimmten Tag im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.
   c) Aktivieren Sie die jeweiligen Kontrollkästchen im Feld **Tage**, um andere oder zusätzliche Tage in der Woche oder im Monat auszuwählen.

   Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.
4. Wählen Sie in der Liste **Aufbewahrungsdauer** den Zeitraum aus, für den die Bestandsdaten aufbewahrt werden sollen.
5. Klicken Sie auf **Speichern**.

Kapitel 5. Erkennung und Übertragung an IBM einrichten

Nachdem die Einrichtung der TSA abgeschlossen ist, können Sie verschiedene Verwaltungsfunktionen nutzen, um die Erkennung, Übertragung und Jobausführung zu steuern.

Erkennungsbereiche

Ein Erkennungsbereich bezeichnet die IP-Adresse oder den Hostnamen, den Bereich von IP-Adressen oder das Netz, in denen die Erkennung von IT-Elementen stattfinden soll. Die Erkennungsbereiche sind in Erkennungsbereichsgruppen gegliedert.

TSA bietet mehrere Arten von Erkennungsbereichen:

- Dynamische HMC-Bereiche – können verwendet werden, um HMCs zusammen mit allen von ihr verwalteten Partitionen zu erkennen.
- Dynamische VMware-Bereichsgruppen – können verwendet werden, um VMware vCenter- oder ESXi-Hosts zusammen mit allen virtuellen Maschinen auf den ESXi-Hosts zu erkennen.
- Allgemeine Erkennungsbereiche – werden verwendet, um alle anderen Ressourcen zu erkennen, die nicht mithilfe einer dynamischen Bereichsgruppe erkannt werden. Die IP-Adressen, der Bereich von IP-Adressen oder Netze können manuell eingegeben werden. Es kann auch eine Liste von IP-Adressen und Hostnamen aus einer Datei in die TSA importiert werden.

Dynamische HMC-Bereiche

Sie können dynamische HMC-Bereiche definieren, um detaillierte Bestandsdaten aus HMCs, den von ihnen verwalteten IBM Power Systems und auch den VIOS-, AIX- und Linux-LPARs auf diesen Systemen zu erfassen.

Informationen zu diesem Vorgang

Zusätzlich zum Abrufen von Bestandsdaten von den definierten HMCs fragt die TSA auch von diesen HMCs verwaltete LPARs dynamisch ab, ohne dass mehrere Bereichsdefinitionen erstellt und verwaltet werden müssen. Sie müssen lediglich einen Bereich für die HMCs definieren und auswählen, welche Typen von LPARs (AIX, VIOS und Linux) bei der HMC-Erkennung automatisch durchsucht werden sollen. Dies bietet den Vorteil, das die TSA auch bei Änderungen an den LPARs nicht rekonfiguriert werden muss.

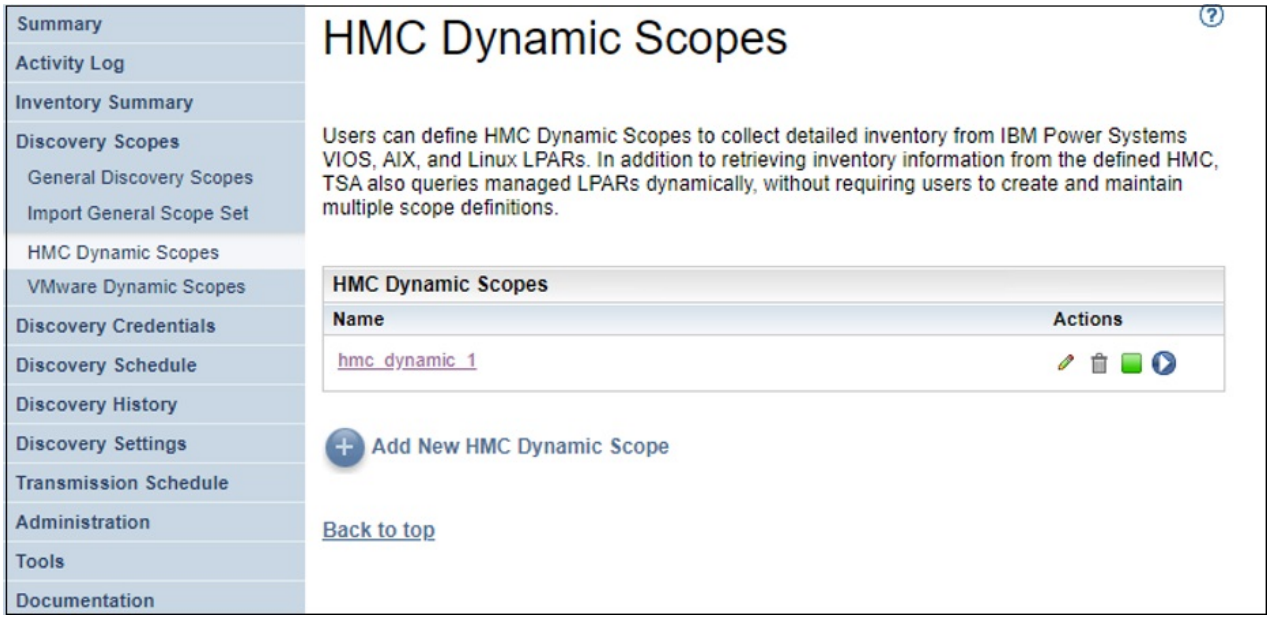

Abbildung 43. Dynamische HMC-Bereiche

Dynamische HMC-Bereiche anzeigen

Sie können die vorhandenen dynamischen HMC-Bereiche anzeigen.

Informationen zu diesem Vorgang

Zum Anzeigen der dynamischen HMC-Bereiche klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**. Die Seite **Dynamische HMC-Bereiche** wird angezeigt. Die dynamischen HMC-Bereiche sind im Fensterbereich **Dynamische HMC-Bereiche** aufgelistet.

Klicken Sie in der Spalte **Name** auf den Namen der Bereichsgruppe, um die Bereiche und Berechtigungsnachweise anzuzeigen, die einer bestimmten dynamischen Bereichsgruppe zugeordnet sind. Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.

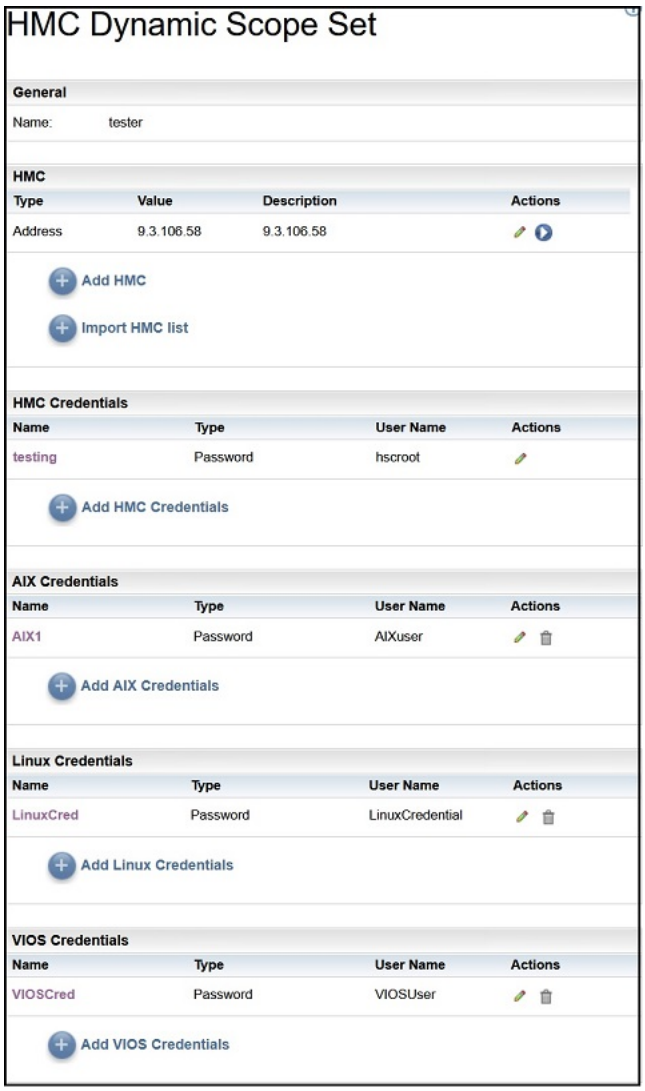

Abbildung 44. Dynamische HMC-Bereichsgruppe anzeigen

Im Fensterbereich **HMC** wird die Liste der IP-Adressen der HMCs angezeigt, die die dynamische Bereichsgruppe erkennt. Wenn die HMC mit einem Hostnamen definiert wurde, wird dieser Wert in der Spalte **Beschreibung** der HMC-Liste angezeigt. In den verschiedenen Fensterbereichen mit Berechtigungsnachweisen, wie z. B. **AIX-Berechtigungsnachweise**, werden die in der Bereichsgruppe konfigurierten Berechtigungsnachweise aufgelistet.

Dynamische HMC-Bereiche hinzufügen

Sie können eine dynamische HMC-Bereichsgruppe hinzufügen, indem Sie die IP-Adresse oder den Hostnamen einer einzigen HMC sowie einen einzigen Berechtigungsnachweis für den Zugriff auf die HMC angeben. Optional können Sie die Berechtigungsnachweise für AIX, Linux und VIOS angeben, um die Erkennung der LPARs der IBM Power Systems, die die HMC verwaltet, zu ermöglichen. Nachdem die dynamische HMC-Bereichsgruppe erstellt wurde, kann sie bearbeitet werden, um zusätzliche HMC-IP-Adressen oder Hostnamen zu definieren. Dynamische HMC-Bereichsgruppen können auch bearbeitet werden, um mehrere Berechtigungsnachweise für den Zugriff auf die HMCs sowie mehrere Berechtigungsnachweise für den Zugriff auf die LPARs zu unterstützen.

Informationen zu diesem Vorgang

Führen Sie zum Hinzufügen einer Bereichsgruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Um eine neue dynamische HMC-Bereichsgruppe zu definieren, klicken Sie auf **Neuen dynamischen HMC-Bereich hinzufügen**.
   Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.

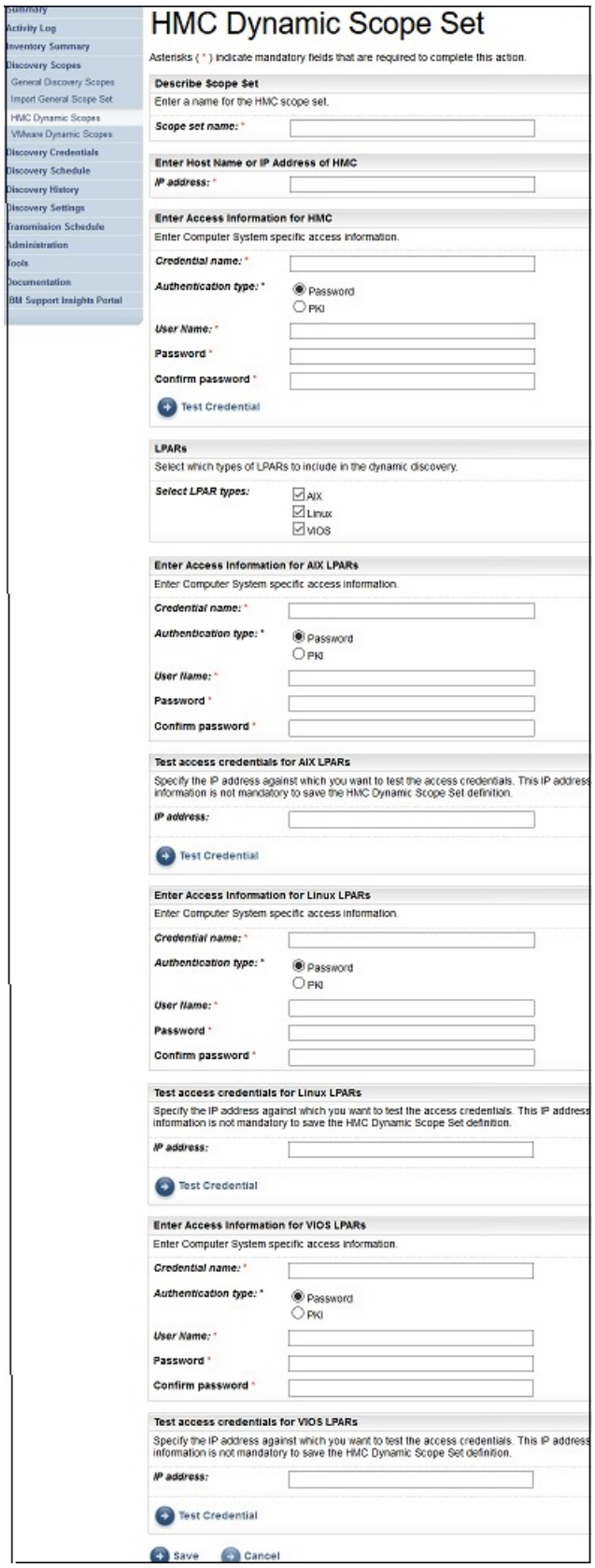

Abbildung 45. Dynamische HMC-Bereichsgruppe hinzufügen

3. Geben Sie im Fensterbereich **Bereichsgruppe beschreiben** im Feld **Bereichsgruppenname** einen eindeutigen Namen für die Bereichsgruppe ein.

4. Geben Sie im Bereich **Hostnamen oder IP-Adresse der HMC eingeben** die IP-Adresse oder den Hostnamen der HMC ein.
5. Geben Sie im Bereich **Zugriffsinformationen für HMC eingeben** die folgenden Details ein:
   a) Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.
   b) Wählen Sie den **Authentifizierungstyp** aus.
      - **Kennwort** – Verwendet das angegebene Kennwort.
      - **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.
   c) Geben Sie unter **Benutzername** den Benutzernamen ein, der an der HMC zur Authentifizierung verwendet wird.
   d) Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.
   e) Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.
   f) Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf der HMC bereitgestellt werden.
   g) Optional: Klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise der Ziel-HMC zu testen.
6. Legen Sie im Fensterbereich **LPARs** fest, welche LPAR-Typen (AIX, Linux, VIOS) in die dynamische Erkennung einbezogen werden sollen.
7. Wenn Sie einen der LPAR-Typen (AIX, Linux, VIOS) ausgewählt haben, geben Sie die entsprechenden Zugriffsinformationen ein.

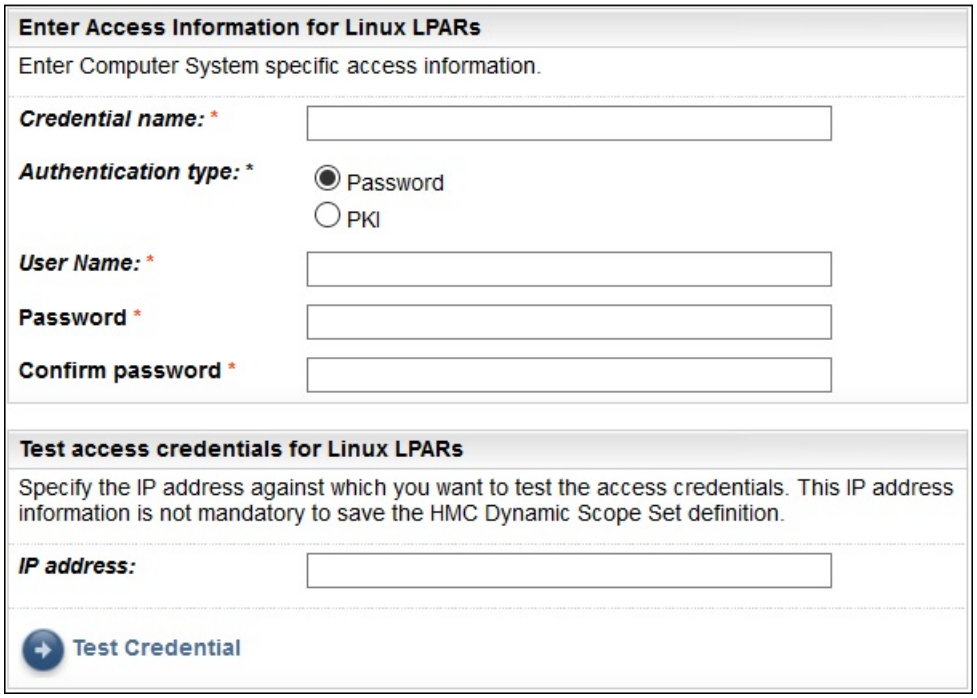

Abbildung 46. Beispiel: Zugriffsinformationen für Linux-LPARs eingeben

   a) Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.
   b) Wählen Sie den **Authentifizierungstyp** aus.
      - **Kennwort** – Verwendet das angegebene Kennwort.
      - **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.

c) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der betreffenden LPAR verwendet wird.

d) Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.

e) Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.

f) Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf jeder LPAR bereitgestellt werden.

g) Optional: Geben Sie die **IP-Adresse** einer LPAR ein, die von dieser HMC verwaltet wird. Klicken Sie dann auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

8. Klicken Sie auf **Speichern**, um die dynamische HMC-Bereichsgruppe zu speichern.

HMC-IP-Adressen für dynamische HMC-Bereiche ändern

Sie können die Liste der HMC-IP-Adressen, die zu einer bestehenden dynamischen HMC-Bereichsgruppe gehören, ändern.

Informationen zu diesem Vorgang

Führen Sie zum Ändern der Liste mit HMC-IP-Adressen die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Zum Bearbeiten der Bereichsgruppe klicken Sie auf das Symbol **Bearbeiten** ( ).
   Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.
   - Führen Sie zum Hinzufügen einer HMC-IP-Adresse oder eines Hostnamens zur Bereichsgruppe die folgenden Schritte durch:
     a. Klicken Sie im Fensterbereich **HMC** auf **HMC hinzufügen**. Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
     b. Geben Sie die IP-Adresse oder den Hostnamen der HMC in das Feld **IP-Adresse** ein.
     c. Klicken Sie auf **Speichern**, um die HMC hinzuzufügen.
   - Führen Sie zum Bearbeiten einer bestehenden HMC-IP-Adresse in der Bereichsgruppe die folgenden Schritte durch:
     a. Klicken Sie im Fensterbereich **HMC** auf das Symbol **Bearbeiten** ( ). Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
     b. Ersetzen Sie im Feld **IP-Adresse** die Adresse durch die IP-Adresse/den Hostnamen der HMC im Fensterbereich **Adresse oder Host beschreiben**.
     c. Klicken Sie auf **Speichern**, um die HMC zu ändern.
   - Führen Sie zum Löschen einer bestehenden HMC-IP-Adresse in der Bereichsgruppe die folgenden Schritte durch:
     a. Klicken Sie im Fensterbereich **HMC** auf das Symbol **Löschen** ( ).
     b. Klicken Sie im Dialogfeld auf **OK**, um das Löschen zu bestätigen.

     Anmerkung: Für eine dynamische HMC-Bereichsgruppe muss immer mindestens eine HMC-IP-Adresse definiert sein. Die TSA lässt nicht zu, dass alle HMC-IP-Adressen gelöscht werden.

Dynamische HMC-Bereichsgruppe importieren

Sie können eine Liste mit IP-Adressen und Hostnamen in eine vorhandene dynamische HMC-Bereichsgruppe importieren.

Informationen zu diesem Vorgang

Eine Liste mit IP-Adressen oder Hostnamen aus einer Eingabedatei kann in eine vorhandene dynamische HMC-Bereichsgruppe importiert werden. Beim Importieren einer Bereichsgruppe führt die TSA folgende Validierungen durch:

- Jede Zeile in der Datei wird validiert, um festzustellen, ob die IP-Adresse oder der Hostname gültig ist.
- Beim Validieren der IP-Adressen oder Hostnamen werden abschließende und führende Leerzeichen ignoriert.
- Doppelte IP-Adressen oder Hostnamen werden ebenfalls ignoriert.
- Alle Einträge werden ignoriert, die dieselbe IP-Adresse oder denselben Hostnamen haben wie eine bestehende HMC-IP-Adresse.

Vorgehensweise

Führen Sie zum Importieren der IP-Adressen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Klicken Sie auf einen vorhandenen Bereich in der Liste. Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.
3. Klicken Sie im HMC-Fensterbereich auf **HMC-Liste importieren**. Die Seite **Dynamische HMC-Bereichsgruppe importieren** wird angezeigt.
4. Klicken Sie auf **Datei auswählen**, um die Textdatei auszuwählen.

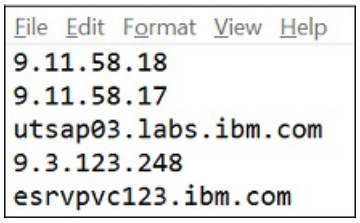

Abbildung 47. Dynamische HMC-Bereichsgruppe importieren

Anmerkung: Die Textdatei muss einspaltig formatiert sein und jede Zeile darf nur eine einzelne IP-Adresse/einen einzelnen Hostnamen und keine sonstigen Daten enthalten.

5. Klicken Sie auf **Datei importieren**, um die IP-Adressen oder Hostnamen zu importieren.
6. Klicken Sie auf **OK**, wenn Sie im Dialogfenster gefragt werden, ob Sie die ausgewählte Liste importieren wollen. Nach erfolgreichem Abschluss des Imports wird die folgende Statusnachricht angezeigt: **`Successfully imported Scope "[n]" IP addresses / hostnames Set`** (Bereich "[n]" IP-Adress-/Hostnamengruppen importiert).

   Anmerkung: Wenn durch die Bereichsgruppendatei die dynamische HMC-Bereichsgruppe mehr als 400 IP-Adressen enthalten würde, wird der folgende Warnhinweis angezeigt: **`Die Auflösung dieser Bereichsgruppe erstreckt sich über 400 IP-Adressen. Zur Vermeidung von Leistungsproblemen sollte die kumulative Anzahl von IP-Adressen in einer Bereichsgruppe diesen Schwellenwert nicht überschreiten.`**
7. Nachdem Sie die IP-Adressen und Hostnamen importiert haben, können Sie die dynamische HMC-Bereichsgruppe auf der Seite **HMC-Erkennungsbereiche** der Benutzerschnittstelle bearbeiten.

Berechtigungsnachweise für dynamische HMC-Bereiche ändern

Sie können die Liste der Berechtigungsnachweise, die zu einer bestehenden dynamischen HMC-Bereichsgruppe gehören, ändern.

Informationen zu diesem Vorgang

Für eine dynamische HMC-Bereichsgruppe muss immer mindestens ein HMC-Berechtigungsnachweis definiert sein. Die TSA lässt nicht zu, dass alle HMC-Berechtigungsnachweise gelöscht werden. Wenn für AIX, Linux oder VIOS keine Berechtigungsnachweise vorliegen, erfasst die TSA keine detaillierten Informationen für diesen LPAR-Typ.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Zum Bearbeiten der Bereichsgruppe klicken Sie auf das Symbol **Bearbeiten** ( ).
   Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.
   - Führen Sie zum Hinzufügen eines Berechtigungsnachweises für HMC, AIX, Linux oder VIOS die folgenden Schritte durch:
     a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf **Berechtigungsnachweise hinzufügen**. Klicken Sie beispielsweise zum Hinzufügen eines HMC-Berechtigungsnachweises im Fensterbereich **HMC-Berechtigungsnachweise** auf **HMC-Berechtigungsnachweise hinzufügen**. Die Seite **Neue HMC-Erkennungsberechtigungsnachweise** wird angezeigt.
     b. Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.
     c. Wählen Sie den **Authentifizierungstyp** aus.
        – **Kennwort** – Verwendet das angegebene Kennwort.
        – **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.
     d. Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der HMC oder der betreffenden LPAR verwendet wird.
     e. Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.
     f. Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.
     g. Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf den HMCs oder LPARs bereitgestellt werden.
     h. **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der HMC oder LPAR im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.
     i. Klicken Sie auf **Speichern**, um den Berechtigungsnachweis der dynamischen HMC-Bereichsgruppe zu speichern.
   - Führen Sie zum Bearbeiten eines Berechtigungsnachweises für HMC, AIX, Linux oder VIOS die folgenden Schritte durch:
     a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf das Symbol **Bearbeiten** ( ) für den Berechtigungsnachweis, den Sie ändern möchten. Klicken Sie beispielsweise zum Bearbeiten eines HMC-Berechtigungsnachweises im Fensterbereich **HMC-Berechtigungsnachweise** auf **Bearbeiten** ( ) für den Berechtigungsnachweis, der geändert werden soll. Die Seite **HMC-Erkennungsberechtigungsnachweise bearbeiten** wird angezeigt.
     b. Im Fensterbereich **Zugriffsinformationen eingeben** können Sie folgende Details ändern:

1) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der HMC oder der betreffenden LPAR verwendet wird.
2) Wählen Sie den **Authentifizierungstyp** aus.
   - **Kennwort** – Verwendet das angegebene Kennwort.
   - **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.
3) Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.
4) Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.
5) Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf jeder HMC oder LPAR bereitgestellt werden.

c. **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der HMC oder LPAR im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.
d. Klicken Sie auf **Speichern**, um den Berechtigungsnachweis zu aktualisieren.

- Führen Sie zum Löschen eines Berechtigungsnachweises für HMC, AIX, Linux oder VIOS die folgenden Schritte durch:
  a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf das Symbol **Löschen** ( ) für den betreffenden Berechtigungsnachweis. Klicken Sie beispielsweise zum Löschen eines HMC-Berechtigungsnachweises im Fensterbereich **HMC-Berechtigungsnachweise** auf das Symbol **Löschen** ( ) für den Berechtigungsnachweis, der gelöscht werden soll. Eine Bestätigungsnachricht wird angezeigt.
  b. Klicken Sie auf **OK**, um den Berechtigungsnachweis zu löschen.
- Führen Sie zum Ändern eines Berechtigungsnachweises für HMC, AIX, Linux oder VIOS die folgenden Schritte durch:
  a. Wenn es mehr als einen Berechtigungsnachweis für HMC, AIX, Linux oder VIOS gibt, kann die Reihenfolge der Berechtigungsnachweise für die HMCs oder LPARs geändert werden. Wenn es nur einen Berechtigungsnachweis gibt, werden in der Spalte **Aktionen** im Fensterbereich mit Berechtigungsnachweisen keine Auf- und Abwärtspfeile angezeigt.
  b. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf die Pfeilsymbole **Aufwärts** ( ) oder **Abwärts** ( ), um die Reihenfolge der betreffenden Berechtigungsnachweise zu ändern.

Dynamische Bereichsgruppen aktivieren oder inaktivieren

Sie können eine dynamische HMC-Bereichsgruppe aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Eine inaktivierte Bereichsgruppe wird bei einer geplanten Erkennung übersprungen.

Anmerkung: Eine manuelle Erkennung kann unabhängig vom Status der Bereichsgruppe jederzeit ausgeführt werden.

Dynamische Bereichsgruppen inaktivieren

Vorgehensweise

Führen Sie zum Inaktivieren einer dynamischen HMC-Bereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.

Die Seite **Dynamische HMC-Bereiche** wird angezeigt.

2. Klicken Sie auf das Symbol **Aktivieren** () neben der Bereichsgruppe, die Sie inaktivieren möchten.

Dynamische Bereichsgruppen aktivieren

Vorgehensweise

Führen Sie zum Aktivieren einer dynamischen HMC-Bereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Inaktivieren** () neben der Bereichsgruppe, die Sie aktivieren möchten.

Eine HMC erkennen

Sie können eine Erkennung einer einzigen HMC in einer dynamischen HMC-Bereichsgruppe manuell initiieren. Die Erkennung erfasst Informationen über die HMC sowie die zugehörigen LPARs.

Vorgehensweise

Führen Sie zum manuellen Initiieren einer Erkennung einer HMC die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Bearbeiten** () für die erforderliche dynamische HMC-Bereichsgruppe.
   Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt.
3. Klicken Sie auf das Symbol **Ausführen** () neben der HMC-spezifischen IP-Adresse, die Sie erkennen möchten.

Dynamische Bereichsgruppen erkennen

Sie können eine Erkennung für eine dynamische HMC-Bereichsgruppe manuell initiieren. Die Erkennung erfasst Informationen über alle in der Bereichsgruppe definierten HMCs sowie die zugehörigen LPARs.

Vorgehensweise

Führen Sie zum manuellen Initiieren einer Erkennung für eine dynamische HMC-Bereichsgruppe die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Ausführen** () neben der Bereichsgruppe, die Sie erkennen möchten.

Dynamische HMC-Bereiche löschen

Sie können einen vorhandenen dynamischen HMC-Bereich löschen.

Vorgehensweise

Führen Sie zum Löschen eines dynamischen HMC-Bereichs die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Löschen** () neben der zu löschenden Bereichsgruppe.
3. Klicken Sie auf **OK**, um zu bestätigen, dass die dynamische HMC-Bereichsgruppe gelöscht werden soll.

   Anmerkung: Wenn Sie das Löschen der dynamischen HMC-Bereichsgruppe bestätigen, werden auch die jeweiligen Zugriffsinformationen für AIX-, Linux- oder VIOS-LPARs gelöscht.

Dynamische VMware-Bereiche

Sie können dynamische VMware-Bereiche definieren, um detaillierte Bestandsdaten aus VMware vCenter Server- und ESXi-Instanzen zu erfassen. Dynamische VMware-Bereiche erfassen auch Informationen über die x86-Server, die von den VMware vCenter Server- oder ESXi-Instanzen verwaltet werden, und die virtuellen Linux- und Windows-Maschinen auf diesen Systemen.

Die TSA ruft Bestandsinformationen aus den definierten VMware vCenter Server- und ESXi-Instanzen ab. Die TSA fragt zudem virtuelle Maschinen ab, die von den VMware-Instanzen dynamisch verwaltet werden, ohne dass mehrere Bereichsdefinitionen erstellt und gepflegt werden müssen. Sie müssen lediglich einen Bereich für die VMware-Instanzen definieren und auswählen, welche virtuellen Maschinentypen (Linux und Windows) bei der VMware-Erkennung automatisch durchsucht werden sollen. Dies bietet den Vorteil, das die TSA auch bei Änderungen an den virtuellen Maschinen nicht rekonfiguriert werden muss.

Die VMware vCenter Server-Erkennung findet alle VMware ESXi-Instanzen, die verwaltet werden, wodurch die Notwendigkeit der direkten Erkennung von VMware ESXi-Instanzen entfällt. Bei VMware ESXi-Instanzen, die nicht von einem VMware vCenter Server verwaltet werden, kann eine Erkennung direkt durch die TSA erfolgen, indem die VMware ESXi im dynamischen VMware-Bereich definiert wird.

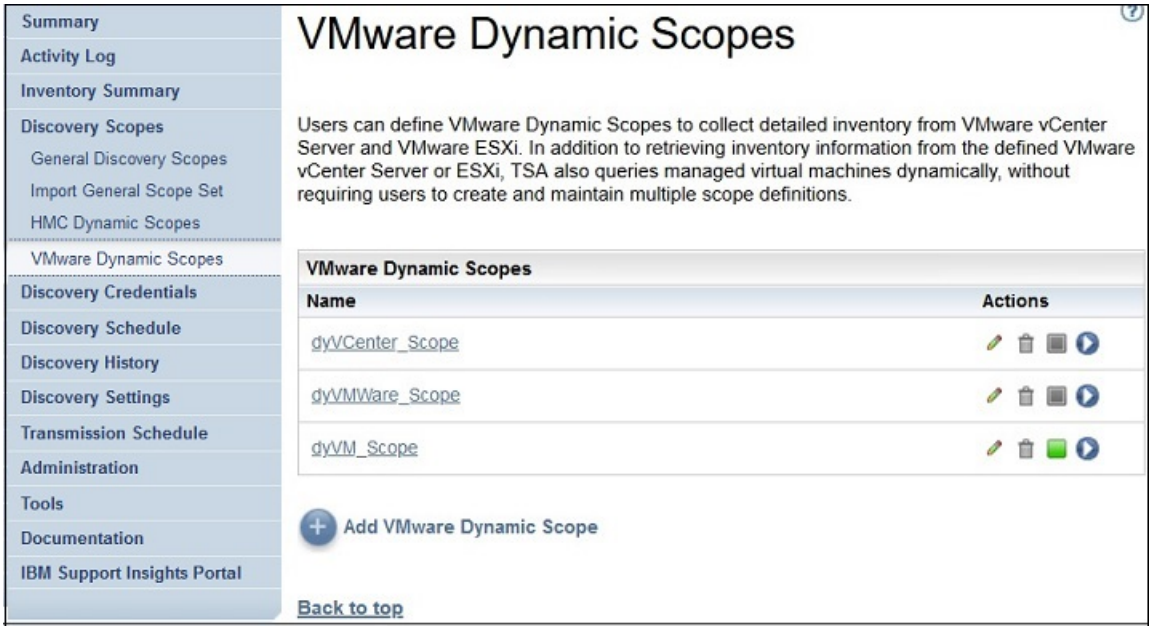

Abbildung 48. Dynamische VMware-Bereiche

Dynamische VMware-Bereiche, Bereichsgruppen und Berechtigungsnachweise anzeigen

Sie können die vorhandenen dynamischen VMware-Bereiche und -Bereichsgruppen anzeigen.

Informationen zu diesem Vorgang

Zum Anzeigen der vorhandenen dynamischen VMware-Bereichsgruppen klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**. Die Seite **Dynamische VMware-Bereiche** wird angezeigt.Die dynamischen VMware-Bereiche sind im Fensterbereich **Dynamische VMware-Bereiche** aufgelistet.

Klicken Sie in der Spalte **Name** auf den Namen der Bereichsgruppe, um die Bereiche und Berechtigungsnachweise anzuzeigen, die einer bestimmten dynamischen Bereichsgruppe zugeordnet sind. Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.

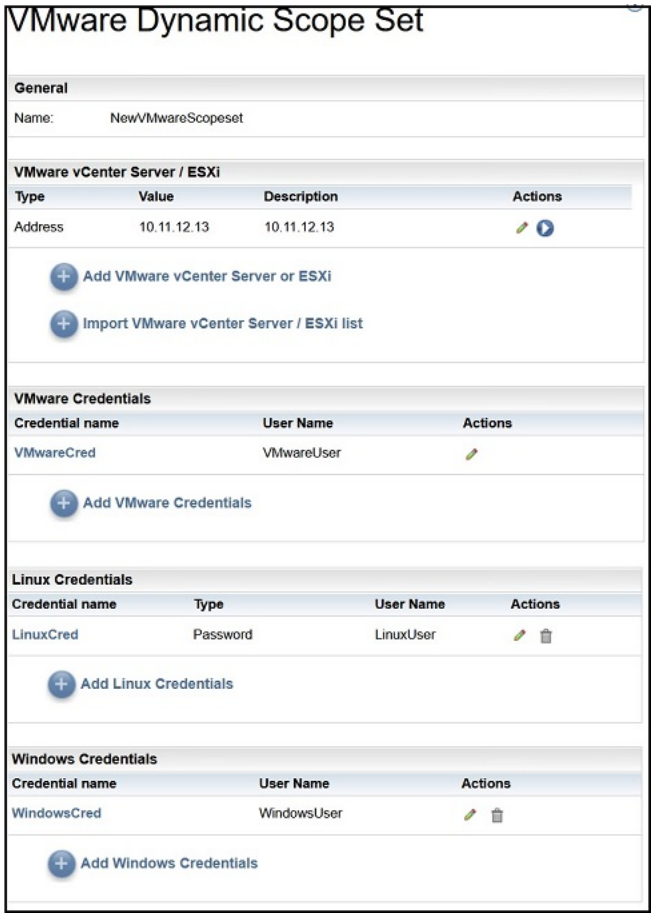

Abbildung 49. Dynamische VMware-Bereichsgruppe anzeigen

Im Fensterbereich **VMware vCenter Server/ESXi** wird die Liste der IP-Adressen der VMware vCenter Server- und ESXi-Instanzen angezeigt, die die dynamische Bereichsgruppe erkennt. Wenn die VMware vCenter-Server- oder ESXi-Instanz mit einem Hostnamen definiert wurde, wird dieser Wert in der Spalte **Beschreibung** in der VMware vCenter Server/ESXi-Liste angezeigt. In den verschiedenen Fensterbereichen mit Berechtigungsnachweisen, wie **Linux-Berechtigungsnachweise**, werden die in der Bereichsgruppe konfigurierten Berechtigungsnachweise aufgelistet.

Dynamische VMware-Bereiche hinzufügen

Sie können eine dynamische VMware-Bereichsgruppe hinzufügen, indem Sie die IP-Adresse oder den Hostnamen einer einzigen VMware vCenter Server- oder ESXi-Instanz sowie einen einzigen Berechtigungsnachweis für den Zugriff auf die VMware-Instanz angeben. Optional können Sie die Berechtigungsnachweise für Linux und Windows angeben, um die Erkennung der virtuellen Maschinen der x86-Server, die die VMware-Instanz verwaltet, zu ermöglichen. Nachdem die dynamische VMware-Bereichsgruppe erstellt wurde, kann sie bearbeitet werden, um zusätzliche VMware vCenter Server- oder ESXi-IP-Adressen oder -Hostnamen zu definieren. Dynamische VMware-Bereichsgruppen können auch bearbeitet werden, um mehrere Berechtigungsnachweise für den Zugriff auf die VMware-Instanz sowie mehrere Berechtigungsnachweise für den Zugriff auf die virtuellen Maschinen zu unterstützen.

Informationen zu diesem Vorgang

Führen Sie zum Hinzufügen einer dynamischen VMware-Bereichsgruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.

Die Seite **Dynamische VMware-Bereiche** wird angezeigt.

2. Um eine neue dynamische VMware-Bereichsgruppe zu definieren, klicken Sie auf **Dynamischen VMware-Bereich hinzufügen**.

   Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.

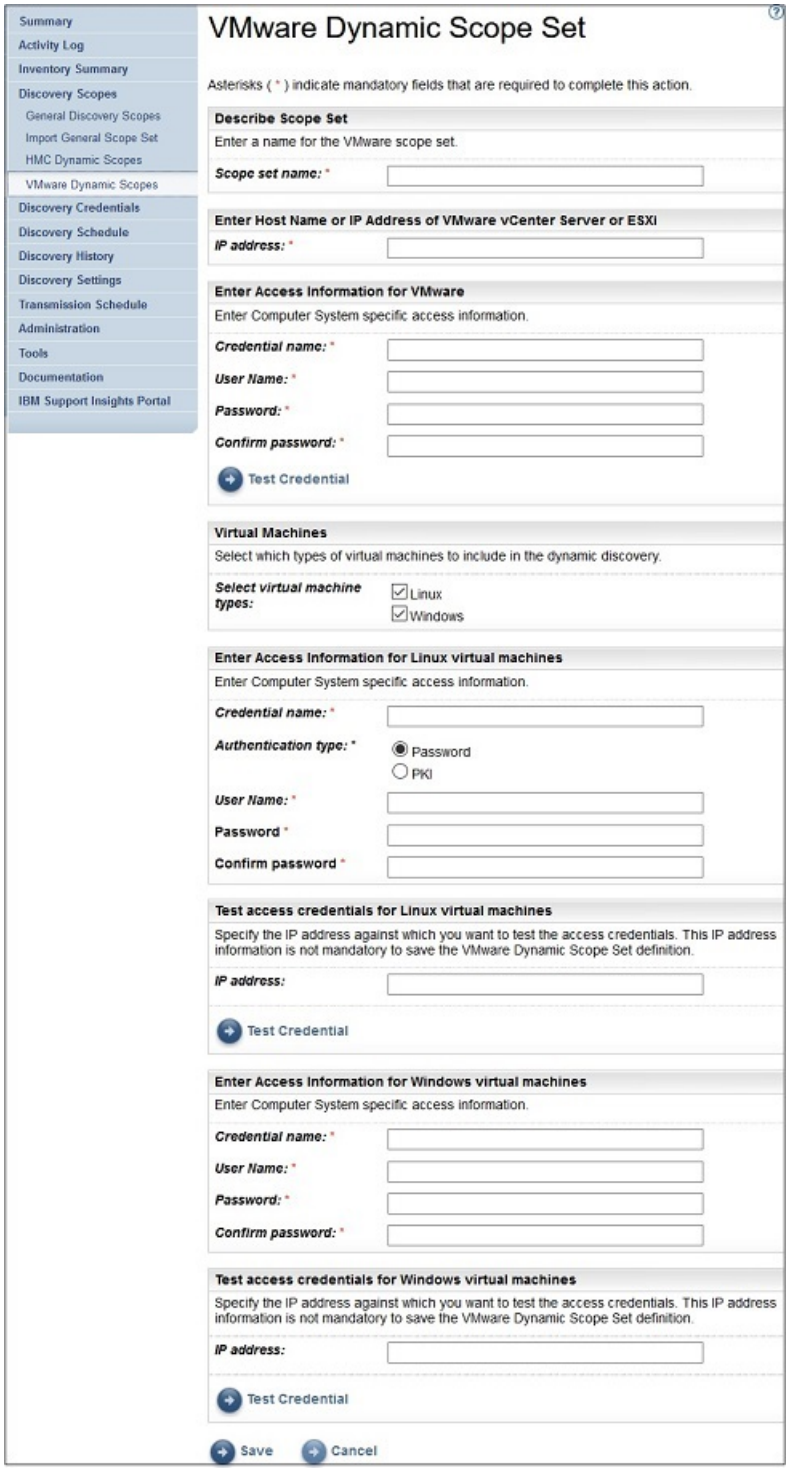

Abbildung 50. Dynamische VMware-Bereichsgruppe hinzufügen

3. Geben Sie im Fensterbereich **Bereichsgruppe beschreiben** im Feld **Bereichsgruppenname** einen eindeutigen Namen für die Bereichsgruppe ein.
4. Geben Sie im Bereich **Hostnamen oder IP-Adresse von VMware vCenter Server oder ESXi eingeben** die IP-Adresse oder den Hostnamen der VMware vCenter Server- oder ESXi-Instanz ein.
5. Geben Sie im Bereich **Zugriffsinformationen für VMware eingeben** die folgenden Details ein:

a) Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.

b) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der VMware vCenter Server- oder ESXi-Instanz verwendet wird.

c) Geben Sie unter **Kennwort** und **Kennwort bestätigen** das Kennwort ein.

d) Optional: Klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise für die Ziel-VMware vCenter Server- oder ESXi-Instanz zu testen.

6. Legen Sie im Bereich **Virtuelle Maschinen** fest, welche virtuellen Maschinen (Linux, Windows) in die dynamische Erkennung einbezogen werden sollen.
7. Wenn Sie die virtuelle Linux-Maschine auswählen, geben Sie bitte die entsprechenden Zugriffsinformationen ein.

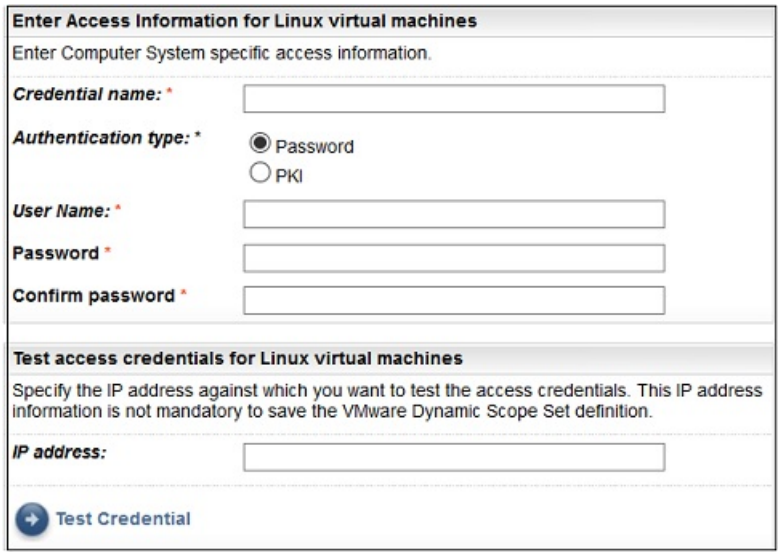

Abbildung 51. Zugriffsinformationen für die virtuelle Linux-Maschine eingeben

a) Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.

b) Wählen Sie den **Authentifizierungstyp** aus.

- **Kennwort** – Verwendet das angegebene Kennwort.
- **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.

c) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der betreffenden virtuellen Maschine verwendet wird.

d) Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.

e) Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.

f) Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Sie müssen den öffentlichen Schlüssel extern auf jeder virtuellen Maschine bereitstellen.

g) Optional: Geben Sie die IP-Adresse oder den Hostnamen der virtuellen Linux-Maschine im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

8. Wenn Sie die virtuelle Windows-Maschine auswählen, geben Sie bitte die entsprechenden Zugriffsinformationen ein.

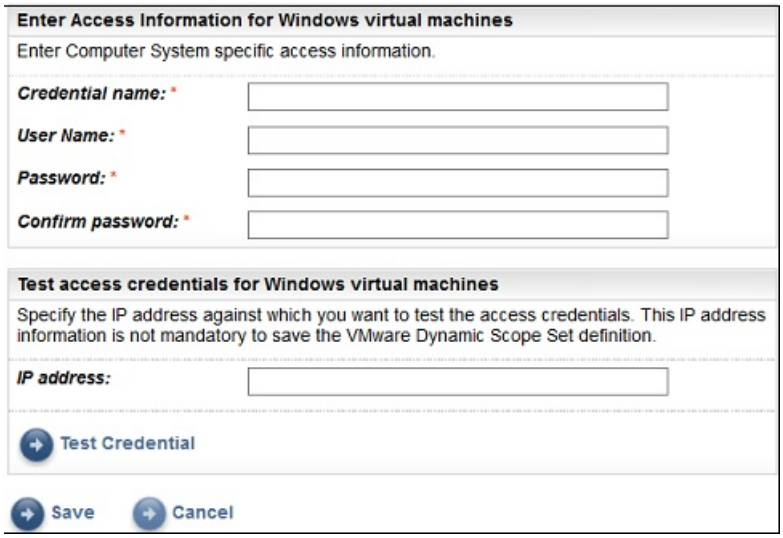

Abbildung 52. Zugriffsinformationen für die virtuelle Windows-Maschine eingeben

a) Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.

b) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung gegenüber der betreffenden virtuellen Maschine verwendet wird.

c) Geben Sie unter **Kennwort** und **Kennwort bestätigen** das Kennwort ein.

d) Optional: Geben Sie die IP-Adresse oder den Hostnamen der virtuellen Windows-Maschine im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

9. Klicken Sie auf **Speichern**, um die dynamische VMware-Bereichsgruppe zu speichern.

VMware vCenter Server- oder ESXi-IP-Adressen für dynamische VMware-Bereiche ändern

Sie können die Liste der VMware vCenter Server- oder ESXi-IP-Adressen oder -Hostnamen, die zu einer bestehenden dynamischen VMware-Bereichsgruppe gehören, ändern.

Informationen zu diesem Vorgang

Führen Sie zum Ändern der Liste mit VMware vCenter Server- oder ESXi-IP-Adressen oder -Hostnamen die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Zum Bearbeiten der Bereichsgruppe klicken Sie auf das Symbol **Bearbeiten** ( ).
   Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.
   - Führen Sie zum Hinzufügen einer VMware vCenter Server- oder ESXi-IP-Adresse oder eines Hostnamens zur Bereichsgruppe die folgenden Schritte durch:
     a. Klicken Sie im Fensterbereich **VMware vCenter Server/ESXi** auf **VMware vCenter Server oder ESXi hinzufügen**. Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
     b. Geben Sie im Fensterbereich **Adresse oder Host beschreiben** die IP-Adresse oder den Hostnamen der VMware vCenter Server- oder ESXi-Instanz in das Feld **IP-Adresse** ein.
     c. Klicken Sie auf **Speichern**, um die VMware vCenter Server- oder ESXi-Instanz hinzuzufügen.

- Führen Sie zum Bearbeiten einer bestehenden VMware vCenter Server- oder ESXi-IP-Adresse in der Bereichsgruppe die folgenden Schritte durch:
  a. Klicken Sie im Fensterbereich **VMware vCenter Server/ESXi** auf das Symbol **Bearbeiten** ( ). Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
  b. Ändern Sie im Fensterbereich **Adresse oder Host beschreiben** die IP-Adresse oder den Hostnamen der VMware vCenter Server- oder ESXi-Instanz im Feld **IP-Adresse**.
  c. Klicken Sie auf **Speichern**.
- Führen Sie zum Löschen einer bestehenden VMware vCenter Server- oder ESXi-IP-Adresse in der Bereichsgruppe die folgenden Schritte durch:
  a. Klicken Sie im Fensterbereich **VMware vCenter Server/ESXi** auf das Symbol **Löschen** ( ).
  b. Klicken Sie im Dialogfeld auf **OK**, um das Löschen zu bestätigen.

  Anmerkung: Für eine dynamische VMware-Bereichsgruppe muss immer mindestens eine VMware vCenter Server- oder ESXi-IP-Adresse definiert sein. Die TSA lässt nicht zu, dass alle VMware-IP-Adressen gelöscht werden.

Dynamische VMware-Bereichsgruppe importieren

Sie können eine Liste mit IP-Adressen und Hostnamen in eine vorhandene dynamische VMware-Bereichsgruppe importieren.

Informationen zu diesem Vorgang

Eine Liste mit IP-Adressen oder Hostnamen aus einer Eingabedatei kann in eine vorhandene dynamische VMware-Bereichsgruppe importiert werden. Beim Importieren einer Bereichsgruppe führt die TSA folgende Validierungen durch:

- Jede Zeile in der Datei wird validiert, um festzustellen, ob die IP-Adresse oder der Hostname gültig ist.
- Beim Validieren der IP-Adressen oder Hostnamen werden abschließende und führende Leerzeichen ignoriert.
- Doppelte IP-Adressen oder Hostnamen werden ebenfalls ignoriert.
- Alle Einträge werden ignoriert, die dieselbe IP-Adresse oder denselben Hostnamen haben wie eine bestehende VMware vCenter Server- oder ESXi-Adresse.

Vorgehensweise

Führen Sie zum Importieren der IP-Adressen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf einen vorhandenen Bereich in der Liste. Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.
3. Klicken Sie im Fensterbereich **VMware vCenter Server/ESXi** auf **VMware vCenter Server-/ESXi-Liste importieren**. Die Seite **Dynamische VMware-Bereichsgruppe importieren** wird angezeigt.
4. Klicken Sie auf **Datei auswählen**, um die Textdatei auszuwählen.

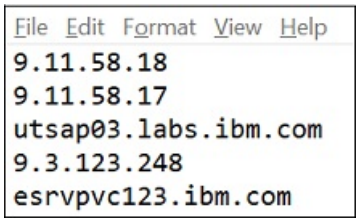

Abbildung 53. Dynamische VMware-Bereichsgruppe importieren

Anmerkung: Die Textdatei muss einspaltig formatiert sein und jede Zeile darf nur eine einzelne IP-Adresse/einen einzelnen Hostnamen und keine sonstigen Daten enthalten.

5. Klicken Sie auf **Datei importieren**, um die IP-Adressen oder Hostnamen zu importieren.
6. Klicken Sie auf **OK**, wenn Sie im Dialogfenster gefragt werden, ob Sie die ausgewählte Liste importieren wollen. Nach erfolgreichem Abschluss des Imports wird die folgende Statusnachricht angezeigt: **`Successfully imported Scope "[n]" IP addresses / hostnames Set`** (Bereich "[n]" IP-Adress-/Hostnamengruppen importiert).

   Anmerkung: Wenn durch die Bereichsgruppendatei die dynamische VMware-Bereichsgruppe mehr als 400 IP-Adressen enthalten würde, wird der folgende Warnhinweis angezeigt: **`Die Auflösung dieser Bereichsgruppe erstreckt sich über 400 IP-Adressen. Zur Vermeidung von Leistungsproblemen sollte die kumulative Anzahl von IP-Adressen in einer Bereichsgruppe diesen Schwellenwert nicht überschreiten.`**
7. Nachdem Sie die IP-Adressen und Hostnamen importiert haben, können Sie die dynamische VMware-Bereichsgruppe auf der Seite **VMware-Erkennungsbereiche** der Benutzerschnittstelle bearbeiten.

Berechtigungsnachweise für dynamische VMware-Bereiche ändern

Sie können die Liste der Berechtigungsnachweise, die zu einer bestehenden dynamischen VMware-Bereichsgruppe gehören, ändern.

Informationen zu diesem Vorgang

Für eine dynamische VMware-Bereichsgruppe muss immer mindestens ein VMware-Berechtigungsnachweis definiert sein. Die TSA lässt nicht zu, dass alle VMware-Berechtigungsnachweise gelöscht werden. Wenn für Linux oder Windows keine Berechtigungsnachweise vorliegen, erfasst die TSA keine detaillierten Informationen für diesen virtuellen Maschinentyp.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Zum Bearbeiten der Bereichsgruppe klicken Sie auf das Symbol **Bearbeiten** ( ).
   Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.
   - Führen Sie zum Hinzufügen von Berechtigungsnachweisen für VMware oder Windows die folgenden Schritte durch:
     a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf **Berechtigungsnachweise hinzufügen**. Klicken Sie beispielsweise, um einen VMware-Berechtigungsnachweis hinzuzufügen, im Fensterbereich **VMware-Berechtigungsnachweise** auf **VMware-Berechtigungsnachweise hinzufügen**. Die Seite **Neue VMware-Erkennungsberechtigungsnachweise** wird angezeigt.
     b. Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.
     c. Geben Sie unter **Benutzername** den Namen ein, der bei der Authentifizierung mit dem VMware vCenter Server, ESXi oder virtuellen Windows-Maschinen verwendet wird.
     d. Geben Sie unter **Kennwort** und **Kennwort bestätigen** das Kennwort ein.
     e. **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der VMware vCenter Server- oder ESXi-Instanz, oder der virtuellen Windows-Maschine, im Feld **IP-Adresse** an und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.
     f. Klicken Sie auf **Speichern**, um den Berechtigungsnachweis zu speichern.
   - Zum Hinzufügen eines Berechtigungsnachweises für Linux führen Sie die folgenden Schritte durch:
     a. Klicken Sie im Fensterbereich **Linux-Berechtigungsnachweise** auf **Linux-Berechtigungsnachweise hinzufügen**. Die Seite **Neue VMware-Erkennungsberechtigungsnachweise** wird angezeigt.

b. Geben Sie unter **Berechtigungsnachweisname** den Berechtigungsnachweisnamen ein.

c. Wählen Sie den **Authentifizierungstyp** aus.

   – **Kennwort** – Verwendet das angegebene Kennwort.

   – **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.

d. Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung mit der virtuellen Linux-Maschine verwendet wird.

e. Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.

f. Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.

g. Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf der virtuellen Linux-Maschine bereitgestellt werden.

h. **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der virtuellen Linux-Maschine im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

i. Klicken Sie auf **Speichern**, um den Linux-Berechtigungsnachweis zu speichern.

- Führen Sie zum Bearbeiten eines Berechtigungsnachweises für VMware oder Windows die folgenden Schritte durch:

  a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf das Symbol **Bearbeiten** ( ) für den Berechtigungsnachweis, den Sie ändern möchten. Klicken Sie beispielsweise zum Bearbeiten eines VMware-Berechtigungsnachweises im Fensterbereich **VMware-Berechtigungsnachweise** auf **Bearbeiten** ( ) für den Berechtigungsnachweis, der geändert werden soll. Die Seite **VMware-Erkennungsberechtigungsnachweise bearbeiten** wird angezeigt.

  b. Im Fensterbereich **Zugriffsinformationen eingeben** können Sie folgende Details ändern:

     1) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung mit den VMware vCenter Server- oder ESXi-Instanzen bzw. mit der virtuellen Windows-Maschine verwendet wird.

     2) Geben Sie unter **Kennwort** und **Kennwort bestätigen** das Kennwort ein.

  c. **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der VMware vCenter Server- oder ESXi-Instanz, oder der virtuellen Windows-Maschine, im Feld **IP-Adresse** an und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

  d. Klicken Sie auf **Speichern**, um den Berechtigungsnachweis zu aktualisieren.

- Führen Sie zum Bearbeiten eines Berechtigungsnachweises für Linux die folgenden Schritte durch:

  a. Klicken Sie im Fensterbereich **Berechtigungsnachweise** auf das Symbol **Bearbeiten** ( ) für den Berechtigungsnachweis, den Sie ändern möchten. Die Seite **VMware-Erkennungsberechtigungsnachweise bearbeiten** wird angezeigt.

  b. Im Fensterbereich **Zugriffsinformationen eingeben** können Sie folgende Details ändern:

     1) Wählen Sie den **Authentifizierungstyp** aus.

        – **Kennwort** – Verwendet das angegebene Kennwort.

        – **PKI** – Verwendet den SSH-Schlüssel, der der betreffenden Bereichsgruppe zugeordnet ist.

     2) Geben Sie unter **Benutzername** den Benutzernamen ein, der zur Authentifizierung mit der virtuellen Linux-Maschine verwendet wird.

     3) Wenn **Authentifizierungstyp** den Wert **Kennwort** hat, geben Sie das **Kennwort** und das **Bestätigungskennwort** ein.

4) Wenn **Authentifizierungstyp** den Wert **PKI** hat, geben Sie die **Kennphrase** ein und bestätigen die Kennphrase durch **Kennphrase bestätigen**, wenn der SSH-Schlüssel verschlüsselt ist. Wenn der SSH-Schlüssel nicht verschlüsselt ist, lassen Sie die beiden Felder leer.
5) Wenn **Authentifizierungstyp** den Wert **PKI** hat, klicken Sie auf **Datei auswählen** und laden den privaten Schlüssel zur TSA hoch. Der öffentliche Schlüssel muss extern auf der virtuellen Linux-Maschine bereitgestellt werden.
6) **Optional:** Geben Sie die IP-Adresse oder den Hostnamen der virtuellen Linux-Maschine im Feld **IP-Adresse** ein und klicken Sie auf **Berechtigungsnachweis testen**, um die Berechtigungsnachweise zu testen.

c. Klicken Sie auf **Speichern**, um den Berechtigungsnachweis zu aktualisieren.

- Führen Sie zum Löschen eines Berechtigungsnachweises für VMware, Linux oder Windows die folgenden Schritte durch:
  a. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf das Symbol **Löschen** ( ) für den betreffenden Berechtigungsnachweis. Klicken Sie beispielsweise zum Bearbeiten eines VMware-Berechtigungsnachweises im Fensterbereich **VMware-Berechtigungsnachweise** auf das Symbol **Bearbeiten** ( ) für den Berechtigungsnachweis, der gelöscht werden soll. Eine Bestätigungsnachricht wird angezeigt.
  b. Klicken Sie auf **OK**, um den Berechtigungsnachweis zu löschen.
- Führen Sie zum Ändern der Reihenfolge eines Berechtigungsnachweises für VMware, Linux oder Windows die folgenden Schritte durch:
  a. Wenn es mehr als einen Berechtigungsnachweis für VMware, Linux oder Windows gibt, kann die Reihenfolge der Berechtigungsnachweise für die VMwares oder virtuellen Maschinen geändert werden. Wenn es nur einen Berechtigungsnachweis gibt, werden in der Spalte **Aktionen** im Fensterbereich mit Berechtigungsnachweisen keine Auf- und Abwärtspfeile angezeigt.
  b. Klicken Sie im betreffenden Fensterbereich **Berechtigungsnachweise** auf die Pfeilsymbole **Aufwärts** ( ) oder **Abwärts** ( ), um die Reihenfolge der betreffenden Berechtigungsnachweise zu ändern.

Dynamische Bereichsgruppen aktivieren oder inaktivieren

Sie können eine dynamische VMware-Bereichsgruppe aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Eine inaktivierte Bereichsgruppe wird bei einer geplanten Erkennung übersprungen.

Anmerkung: Eine manuelle Erkennung kann unabhängig vom Status der Bereichsgruppe jederzeit ausgeführt werden.

Dynamische Bereichsgruppen inaktivieren

Vorgehensweise

Führen Sie zum Inaktivieren einer dynamischen VMware-Bereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Aktivieren** ( ) neben der Bereichsgruppe, die Sie inaktivieren möchten.

Dynamische Bereichsgruppen aktivieren

Vorgehensweise

Führen Sie zum Aktivieren einer dynamischen VMware-Bereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Inaktivieren** ( ) neben der Bereichsgruppe, die Sie aktivieren möchten.

VMware vCenter oder ESXi erkennen

Sie können eine Erkennung einer einzigen VMware vCenter Server- oder ESXi-Instanz in einer dynamischen VMware-Bereichsgruppe manuell initiieren. Die Erkennung erfasst Informationen über die VMware-Instanz sowie die zugehörigen virtuellen Maschinen.

Vorgehensweise

Führen Sie zum manuellen Initiieren einer Erkennung einer VMware vCenter Server- oder ESXi-Instanz die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Bearbeiten** ( ) für die erforderliche dynamische VMware-Bereichsgruppe. Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt.
3. Klicken Sie auf das Symbol **Ausführen** ( ) neben der VMware vCenter Server- oder ESXi-IP-Adresse, für die die Erkennung ausgeführt werden soll.

Dynamische Bereichsgruppen erkennen

Sie können eine Erkennung für eine dynamische VMware-Bereichsgruppe manuell initiieren. Die Erkennung erfasst Informationen über alle in der Bereichsgruppe definierten VMware vCenter Server- oder ESXi-Instanzen sowie die zugehörigen virtuellen Maschinen.

Vorgehensweise

Führen Sie zum manuellen Initiieren einer Erkennung für eine dynamische VMware-Bereichsgruppe die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Ausführen** ( ) neben der Bereichsgruppe, die Sie erkennen möchten.

Dynamische VMware-Bereiche löschen

Sie können einen vorhandenen dynamischen VMware-Bereich löschen.

Vorgehensweise

Führen Sie zum Löschen eines dynamischen VMware-Bereichs die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Dynamische VMware-Bereiche**.
   Die Seite **Dynamische VMware-Bereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Löschen** ( ) neben der zu löschenden Bereichsgruppe.
3. Klicken Sie auf **OK**, um zu bestätigen, dass die dynamische VMware-Bereichsgruppe gelöscht werden soll.

   Anmerkung: Wenn Sie das Löschen der dynamischen VMware-Bereichsgruppe bestätigen, werden auch die jeweiligen Zugriffsinformationen für virtuelle Linux- oder Windows-Maschinen gelöscht.

Allgemeine Erkennungsbereiche

Der Erkennungsprozess sucht nach IT-Elementen in Ihrer Infrastruktur. Ein Erkennungsbereich definiert eine einzige IP-Adresse, einen IP-Adressbereich oder ein Teilnetz, die während des Erkennungsprozesses erkannt werden. Die Erkennungsbereiche sind in vom Benutzer benannte Bereichsgruppen gegliedert.

Erkennungsbereiche und -bereichsgruppen anzeigen

Sie können die vorhandenen Erkennungsbereiche und -bereichsgruppen anzeigen.

Informationen zu diesem Vorgang

Zum Anzeigen der vorhandenen Erkennungsbereichsgruppen klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**. Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt. Bereichsgruppen sind im Fensterbereich **Allgemeine Erkennungsbereiche** aufgelistet.

Um die Bereiche anzuzeigen, die in einer Bereichsgruppe enthalten sind, klicken Sie auf die Bereichsgruppe. Die Seite **Erkennungsbereichsgruppe** wird angezeigt.

- Im Fensterbereich **Allgemein** wird der Name der Bereichsgruppe angezeigt.
- Im Fensterbereich **Anzahl IP-Adressen** wird die Gesamtzahl der IP-Adressen in der Bereichsgruppe angezeigt.
- Im Fensterbereich **Bereiche** werden Details zu den einzelnen Bereichen in der Bereichsgruppe angezeigt.

Erkennungsbereiche hinzufügen

Sie können eine Bereichsgruppe erstellen und einen neuen Bereich zu dieser Gruppe hinzufügen, einen Bereich zu einer vorhandenen Bereichsgruppe hinzufügen oder Bereiche in andere Bereichsgruppen verschieben. Zum Definieren eines Bereichs geben Sie eine gültige IP-Adresse/einen gültigen Hostnamen, einen Bereich von IP-Adressen, ein Netz oder ein Teilnetz an.

Informationen zu diesem Vorgang

Tipps: Bei der Einrichtung von Erkennungsbereichen und -bereichsgruppen sind einige praktische Erwägungen zu berücksichtigen.

- Je mehr IP-Adressen ein Erkennungsbereich umfasst, desto länger dauert der Erkennungsprozess. Sie können den Erkennungsumfang ändern, indem Sie Bereichsgruppen inaktivieren/aktivieren oder indem Sie IP-Adressen, IP-Adressbereiche oder Netze/Teilnetze aus einem Bereich innerhalb einer Bereichsgruppe ausschließen.

  Um die Erkennungszeit zu minimieren, richten Sie Erkennungsbereiche ein, sodass nur die gewünschten Elemente erfasst werden, und inaktivieren Sie Bereichsgruppen oder schließen Sie IP-Adressen, IP-Adressbereiche oder Netze/Teilnetze aus, die nicht erkannt werden sollen ober müssen.

  Anmerkung: Zur Optimierung des Leistungsverhaltens empfiehlt es sich, die Gesamtzahl von IP-Adressen in einer Bereichsgruppe auf maximal 400 zu begrenzen. Informationen zum Importieren einer Bereichsgruppe finden Sie im Abschnitt „Bereichsgruppe importieren” auf Seite 75
- Nicht alle Elemente sind gleich. Beispielsweise dauert eine vollständige Erkennung bei einem Router mit Dutzenden Schnittstellen länger als bei einem einzelnen Host.
- Wenn bei der Geräteerkennung PKI-Authentifizierung verwendet wird, kann jeder Bereichsgruppe nur ein SSH-Schlüssel zugeordnet werden.

Weitere Informationen und Best Practices zum Einrichten von Erkennungsbereichen finden Sie im Leitfaden zum TSA-Konfigurationsassistenten.

Führen Sie zum Hinzufügen einer Bereichsgruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.
   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
2. Um eine neue Erkennungsbereichsgruppe zu definieren, klicken Sie auf **Neue Bereichsgruppe hinzufügen**.
   Die Seite **Erkennungsbereichsgruppe** wird angezeigt.

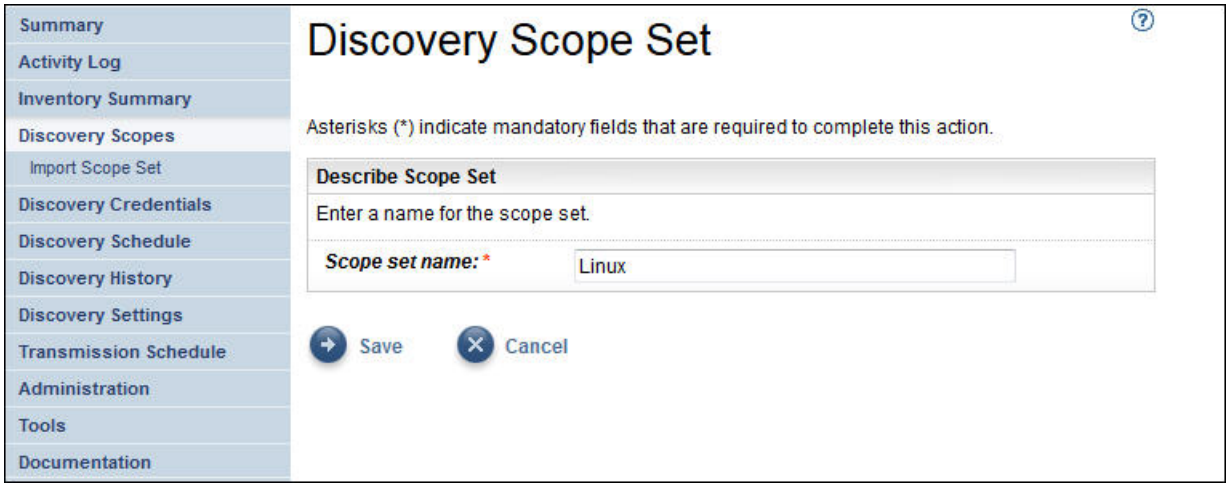

Abbildung 54. Erkennungsbereichsgruppe

a) Geben Sie im Namensfeld **Bereichsgruppe** einen eindeutigen Namen für die Bereichsgruppe ein.

b) Klicken Sie auf **Speichern**.
   Die neue Bereichsgruppe wird erzeugt und die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.

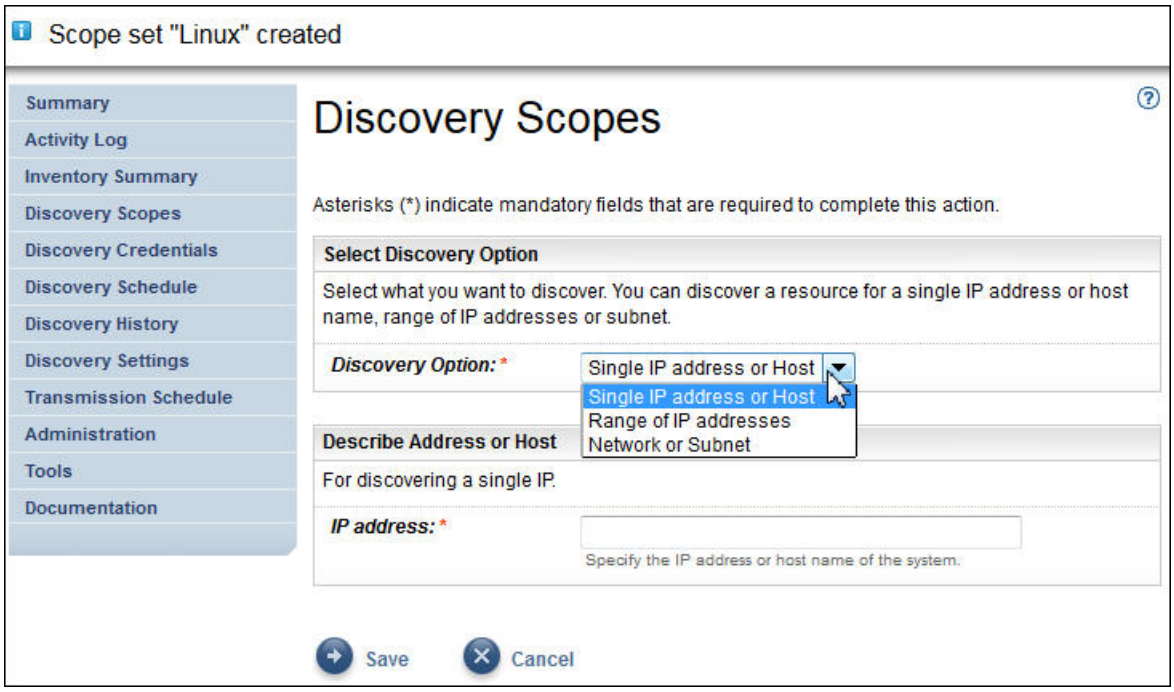

Abbildung 55. Allgemeine Erkennungsbereiche

3. Geben Sie im Fenster **Erkennungsoption auswählen** eine der folgenden Optionen an.

   - `Einzelne IP-Adresse oder einzelner Host`

     Geben Sie in **Adresse oder Host beschreiben** die IP-Adresse bzw. den Hostnamen ein.

- `Bereich von IP-Adressen`

  Geben Sie unter **Adressbereich beschreiben** in den jeweiligen Feldern die erste und letzte IP-Adresse sowie optional eine Beschreibung ein.
- `Netz oder Teilnetz`

  Geben Sie unter **Netz oder Teilnetz beschreiben** in den jeweiligen Feldern die IP-Adresse, die Netzmaske sowie optional eine Beschreibung ein.

4. Wenn Sie bestimmte IP-Adressen, den Bereich von IP-Adressen oder Teilnetze von der Erkennung ausschließen möchten, klicken Sie auf **Ausschluss hinzufügen** und führen Sie die folgenden Schritte durch:
   a) Wählen Sie **Host**, **Bereich** oder **Teilnetz** aus.
   b) Geben Sie die IP-Adresse, den Bereich von IP-Adressen oder das Teilnetz an, die Sie von der Erkennung ausschließen möchten.
   c) Optional: Geben Sie eine Beschreibung für die IP-Adresse, den Bereich von IP-Adressen oder das Teilnetz ein, die von der Erkennung ausgeschlossen werden.

      Anmerkung: Ausschlüsse gelten nur für einen Bereich, der mit einem Bereich von IP-Adressen oder einem Teilnetz definiert ist.

      Anmerkung: IP-Adressen, IP-Adressbereiche, Teilnetze oder Beschreibungen können nicht in anderen Bereichen oder Ausschlüssen einer Bereichsgruppe wiederverwendet werden.
   d) Zum Hinzufügen weiterer Ausschlüsse klicken Sie auf **Ausschluss hinzufügen** und führen die oben beschriebenen Schritte erneut aus, um weitere Ausschlüsse zu definieren.
5. Klicken Sie auf **Speichern**, um den Bereich und die Ausschlüsse zu speichern. Die Seite **Erkennungsbereichsgruppe** wird mit dem neuen Bereich in der Liste angezeigt.
6. Wenn Sie weitere Bereiche zu dieser Bereichsgruppe hinzufügen möchten, klicken Sie auf **Neuen Bereich hinzufügen** und führen Sie die oben beschriebenen Schritte durch, um weitere Bereiche zu definieren.

   Anmerkung: Zur Optimierung des Leistungsverhaltens empfiehlt es sich, die Gesamtzahl von IP-Adressen in einer Bereichsgruppe auf maximal 400 zu begrenzen.

Erkennungsbereich zu einer vorhandenen Bereichsgruppe hinzufügen

Sie können einen Bereich zu einer vorhandenen Bereichsgruppe hinzufügen.

Vorgehensweise

Führen Sie zum Hinzufügen eines Bereichs zu einer vorhandenen Bereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.

   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
2. Klicken Sie unter **Allgemeine Erkennungsbereiche** auf die Bereichsgruppe, zu der Sie einen Bereich hinzufügen möchten.

   Die Seite **Erkennungsbereichsgruppe** wird angezeigt.
3. Klicken Sie auf **Neuen Bereich hinzufügen**.

   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
4. Wählen Sie im Bereich **Erkennungsoption auswählen** eine der folgenden Optionen aus.
   - `Einzelne IP-Adresse oder einzelner Host`

     Geben Sie in **Adresse oder Host beschreiben** die IP-Adresse bzw. den Hostnamen ein.
   - `Bereich von IP-Adressen`

     Geben Sie unter **Adressbereich beschreiben** in den jeweiligen Feldern die erste und letzte IP-Adresse sowie optional eine Beschreibung ein.
   - `Netz oder Teilnetz`

Geben Sie unter **Netz oder Teilnetz beschreiben** in den jeweiligen Feldern die IP-Adresse, die Netzmaske sowie optional eine Beschreibung ein.

5. Wenn Sie bestimmte IP-Adressen, den Bereich von IP-Adressen oder Teilnetze von der Erkennung ausschließen möchten, klicken Sie auf **Ausschluss hinzufügen** und führen Sie die folgenden Schritte durch:
   a) Wählen Sie **Host**, **Bereich** oder **Teilnetz** aus.
   b) Geben Sie die IP-Adresse, den Bereich von IP-Adressen oder das Teilnetz an, die Sie von der Erkennung ausschließen möchten.
   c) Optional: Geben Sie eine Beschreibung für die IP-Adresse, den Bereich von IP-Adressen oder das Teilnetz ein, die von der Erkennung ausgeschlossen werden.

      Anmerkung: Ausschlüsse gelten nur für einen Bereich, der mit einem Bereich von IP-Adressen oder einem Teilnetz definiert ist.

      Anmerkung: IP-Adressen, IP-Adressbereiche, Teilnetze oder Beschreibungen können nicht in anderen Bereichen oder Ausschlüssen einer Bereichsgruppe wiederverwendet werden.
   d) Zum Hinzufügen weiterer Ausschlüsse klicken Sie auf **Ausschluss hinzufügen** und führen die oben beschriebenen Schritte erneut aus, um weitere Ausschlüsse zu definieren.
6. Klicken Sie auf **Speichern**, um den Bereich und die Ausschlüsse zu speichern.
   Die Seite **Erkennungsbereichsgruppe** wird mit dem neuen Bereich in der Liste angezeigt.

Erkennungsbereichsgruppe ändern

Sie können eine vorhandene Erkennungsbereichsgruppe ändern, indem Sie die Einstellungen für die Bereichsgruppe bearbeiten.

Informationen zu diesem Vorgang

Führen Sie zum Ändern einer vorhandenen Erkennungsbereichsgruppe die folgenden Schritte durch.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.
   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
2. Zum Bearbeiten der Bereichsgruppe klicken Sie auf das Symbol **Bearbeiten** ( ) neben der Bereichsgruppe.
   Die Seite **Erkennungsbereichsgruppe** wird angezeigt.Sie können die Bereichsgruppe bearbeiten, indem Sie Bereiche ändern, hinzufügen, in eine andere Bereichsgruppe verschieben oder löschen.
   - Führen Sie zum Hinzufügen eines Bereichs die folgenden Schritte durch:
     a. Klicken Sie auf **Neuen Bereich hinzufügen**.
     b. Wählen Sie im Bereich **Erkennungsoption auswählen** eine der folgenden Optionen aus:
        – `Einzelne IP-Adresse oder einzelner Host`

          Geben Sie in **Adresse oder Host beschreiben** die IP-Adresse bzw. den Hostnamen ein.
        – `Bereich von IP-Adressen`

          Geben Sie unter **Adressbereich beschreiben** in den jeweiligen Feldern die erste und letzte IP-Adresse sowie optional eine Beschreibung ein.
        – `Netz oder Teilnetz`

          Geben Sie unter **Netz oder Teilnetz beschreiben** in den jeweiligen Feldern die IP-Adresse, die Netzmaske sowie optional eine Beschreibung ein.

     Anmerkung: Geben Sie unter **Beschreibung** eine eindeutige Bezeichnung ein. Wenn Sie eine Beschreibung eingeben, die bereits für einen anderen Bereich in dieser Bereichsgruppe existiert, lässt die TSA die Erstellung des neuen Bereichs nicht zu. Wird das Feld **Beschreibung** leer

gelassen, erstellt die TSA automatisch eine Beschreibung anhand des IP-Adressbereichs bzw. der Teilnetzmaske.

c. Wenn Sie IP-Adressen oder Teilnetze von der Erkennung ausschließen möchten, klicken Sie auf **Ausschluss hinzufügen** und führen Sie die folgenden Schritte durch:

1) Wählen Sie **Host**, **Bereich** oder **Teilnetz** aus.

2) Geben Sie die IP-Adresse, den Bereich von IP-Adressen oder das Teilnetz an, die Sie von der Erkennung ausschließen möchten.

3) Zum Hinzufügen weiterer Ausschlüsse klicken Sie auf **Ausschluss hinzufügen** und führen die oben beschriebenen Schritte erneut aus, um weitere Ausschlüsse zu definieren.

d. Klicken Sie auf **Speichern**, um den Bereich und die Ausschlüsse zu speichern. Die Seite **Erkennungsbereichsgruppe** wird mit dem neuen Bereich in der Liste angezeigt.

- Führen Sie zum Verschieben eines Bereichs in eine andere Bereichsgruppe die folgenden Schritte durch:

a. Klicken Sie auf **Bereiche verschieben**.

b. Wählen Sie auf der Seite **Bereiche aus einer Gruppe in eine andere verschieben** in der Liste **Bereiche** die Bereiche aus, die Sie verschieben möchten.

c. Wählen Sie in der Liste **Zielbereichsgruppe** die Bereichsgruppe aus, in die die Bereiche verschoben werden sollen.

d. Klicken Sie auf **Verschieben**.

- Führen Sie zum Bearbeiten eines Bereichs die folgenden Schritte durch:

a. Klicken Sie auf das Symbol **Bearbeiten** ( ) eines bestimmten Bereichs.

b. Sie können die **Erkennungsoption**, die **IP-Adressen**, **Ausschlüsse** und andere Einstellungen ändern.

c. Klicken Sie auf **Speichern**, um den Bereich und die Ausschlüsse zu speichern. Die Seite **Erkennungsbereichsgruppe** wird mit dem neuen Bereich in der Liste angezeigt.

- Führen Sie zum Löschen eines Bereichs die folgenden Schritte durch:

a. Klicken Sie auf das Symbol **Löschen** ( ) neben dem zu löschenden Bereich.

b. Klicken Sie auf **OK**, um zu bestätigen, dass der Erkennungsbereich gelöscht werden soll.

Erkennungsbereiche löschen

Sie können vorhandene Erkennungsbereiche innerhalb einer Bereichsgruppe löschen oder ganze Bereichsgruppen löschen.

Informationen zu diesem Vorgang

Vorgehensweise

Führen Sie zum Löschen eines Erkennungsbereichs die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.
   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
2. Öffnen Sie die Bereichsgruppe, die den zu löschenden Erkennungsbereich enthält, indem Sie auf das Symbol **Bearbeiten** ( ) neben der Bereichsgruppe klicken.
   Die Seite **Erkennungsbereichsgruppe** wird angezeigt.
3. Klicken Sie auf das Symbol **Löschen** ( ) neben dem zu löschenden Bereich.
4. Klicken Sie auf **OK**, um zu bestätigen, dass der Erkennungsbereich gelöscht werden soll.

Erkennungsbereichsgruppen löschen

Sie können vorhandene Erkennungsbereichsgruppen löschen.

Vorgehensweise

Anmerkung: Damit Sie eine Bereichsgruppe löschen können, müssen Sie zunächst alle dieser Bereichsgruppe zugeordneten Berechtigungsnachweise löschen.

Führen Sie zum Löschen einer Erkennungsbereichsgruppe die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.
   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.
2. Klicken Sie auf das Symbol **Löschen** ( ) neben der zu löschenden Bereichsgruppe.
3. Klicken Sie auf **OK**, um zu bestätigen, dass die Erkennungsbereichsgruppe gelöscht werden soll.

Bereichsgruppe importieren

Sie können eine Liste mit IP-Adressen oder Hostnamen importieren, um eine neue Bereichsgruppe zu definieren.

Informationen zu diesem Vorgang

Eine neue Bereichsgruppe wird mithilfe des angegebenen Namens und der Liste von IP-Adressen oder Hostnamen aus der Eingabedatei erstellt. Beim Importieren einer Bereichsgruppe führt die TSA folgende Validierungen durch:

- Sie überprüft, ob der Name der Bereichsgruppe bereits vorhanden ist.
- Sie validiert jede Zeile der Datei, um festzustellen, ob die IP-Adresse/der Hostname gültig ist.
- Beim Validieren der IP-Adressen oder Hostnamen werden abschließende und führende Leerzeichen ignoriert.
- Doppelte IP-Adressen oder Hostnamen werden ebenfalls ignoriert.

Vorgehensweise

Führen Sie zum Importieren der IP-Adressen oder Hostnamen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeinen Erkennungsbereich importieren**.
   Die Seite **Allgemeinen Erkennungsbereich importieren** wird angezeigt.
2. Geben Sie unter **Neuer Bereichsgruppenname** einen Namen ein.

   Anmerkung: Es muss ein eindeutiger Name sein, der nicht bereits für andere Bereichsgruppen verwendet wird. Wird ein bereits vorhandener Bereichsgruppenname eingegeben, wird die Fehlernachricht `Bereichsgruppenname existiert bereits` angezeigt.
3. Klicken Sie auf **Datei auswählen**, um die Textdatei auszuwählen.

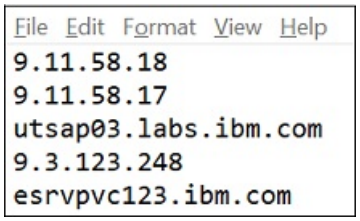

Abbildung 56. Bereichsgruppe importieren

Anmerkung: Die Textdatei muss einspaltig formatiert sein und jede Zeile darf nur eine einzelne IP-Adresse/einen einzelnen Hostnamen und keine sonstigen Daten enthalten.

4. Klicken Sie auf **Bereichsgruppendatei importieren**, um die Bereichsgruppe zu importieren. Nach Abschluss des Imports wird die folgende Statusnachricht angezeigt: **`Bereichsgruppe erfolgreich importiert`**.

   Anmerkung: Wenn die Bereichsgruppendatei mehr als 400 IP-Adressen enthält, wird der folgende Warnhinweis angezeigt: **`Bereichsgruppe erfolgreich importiert. Die Anzahl der Elemente liegt jedoch oberhalb der empfohlenen Richtlinie und sollte für ein besseres Leistungsverhalten auf 400 beschränkt werden.`**
5. Nachdem die Bereichsgruppe importiert wurde, können Sie sie im Abschnitt **Allgemeine Erkennungsbereiche** der Benutzerschnittstelle bearbeiten und ihr im Abschnitt **Erkennungsberechtigungsnachweise** entsprechende Berechtigungsnachweise zuordnen.

Erkennungseinstellungen

Verwenden Sie die Seite **Erkennungseinstellungen** zum Anpassen der Erkennungseinstellungen.

Verbindungseinstellungen konfigurieren

Die Seite **Verbindungseinstellungen** dient zum Konfigurieren der SLP-Erkennung und zum Erkennen von EMC-Speichereinheiten anhand von EMC SMI-S-Providern.

Informationen zu diesem Vorgang

Standardmäßig versucht ein Erkennungsjob, EMC SMI-S Provider zu finden, indem er eine SLP-Abfrage zur Ermittlung der IP-Adresse und des Ports ausführt. Falls SLP in Ihrem Netz nicht verfügbar ist (z. B. wenn SLP-Nachrichten aufgrund von Sicherheitsrichtlinien blockiert werden), kann die Erkennung von EMC-Speichergeräten trotzdem durchgeführt werden, indem die SLP-Erkennung inaktiviert wird und stattdessen die Ports konfiguriert werden, die der EMC SMI-S Provider auf Abfrageanforderungen überwacht.

Vorgehensweise

1. Wählen Sie die Optionen **Aktivieren** oder **Inaktivieren** aus, um die SLP-Erkennung zu aktivieren oder inaktivieren.

   Anmerkung: Standardmäßig ist die SLP-Erkennung aktiviert.
2. Wenn Sie die SLP-Erkennung inaktivieren, müssen Sie einen oder mehrere Ports für EMC SMI-S-Provider-Verbindungen einrichten.
   a) **HTTPS-Port(s) für EMC SMI-S:** 5989 ist der HTTPS-Standardport, den der EMC SMI-S Provider auf Abfrageanforderungen überwacht. Falls Sie mehrere Ports angeben, trennen Sie diese durch Kommas. Diese Ports werden von EMC SMI-S auf Verbindungsanforderungen überwacht (z.B. von der TSA). Die TSA muss den Port kennen, um die Verbindung aufbauen zu können.
   b) **HTTP-Port(s) für EMC SMI-S:** 5988 ist der HTTP-Standardport, den der EMC SMI-S Provider auf Abfrageanforderungen überwacht. Die TSA versucht zunächst, die HTTPS-Verbindung zu verwenden (sofern konfiguriert). Wenn diese fehlschlägt, versucht sie die Verbindung über die definierten HTTP-Ports herzustellen. Falls Sie HTTP-Verbindungen vermeiden möchten, definieren Sie keine HTTP-Ports. Sollten Sie mehrere HTTP-Ports angeben, trennen Sie diese durch Kommas. Diese Ports werden von EMC SMI-S auf Verbindungsanforderungen überwacht (z.B. von der TSA). Die TSA muss den Port kennen, um die Verbindung aufbauen zu können.
3. Klicken Sie auf **Speichern**, um die Verbindungseinstellungen zu speichern. Daraufhin erhalten Sie die Nachricht *Die Verbindungseinstellungen wurden erfolgreich gespeichert.*

Erkennungsberechtigungsnachweise

Erkennungsberechtigungsnachweise sind die Benutzernamen, Kennwörter oder SSH-Schlüssel sowie SNMP-Community-Zeichenfolgen (Simple Network Management Protocol), die die TSA für den Zugriff auf Ressourcen nutzt, die während der Erkennung in **Allgemeine Erkennungsbereiche** konfiguriert werden.

Berechtigungsnachweise anzeigen

Für den Erkennungsprozess werden Berechtigungsnachweise benötigt, z. B. Benutzer-IDs und Kennwörter für den Zugriff auf Ressourcen.

Informationen zu diesem Vorgang

Wichtig: Die Zugriffsinformationen müssen mit den Zugriffsinformationen für die Zielressource der Erkennung übereinstimmen. Wenn Sie Zugriffsinformationen wie ein Kennwort auf einer Zielressource ändern, achten Sie darauf, die entsprechenden Zugriffsinformationen auf der Technical Support Appliance ebenfalls zu ändern.

Sie können die vorhandenen Berechtigungsnachweise anzeigen, indem Sie im Navigationsbereich auf **Erkennungsberechtigungsnachweise** klicken. Die Seite **Erkennungsberechtigungsnachweise** wird angezeigt.

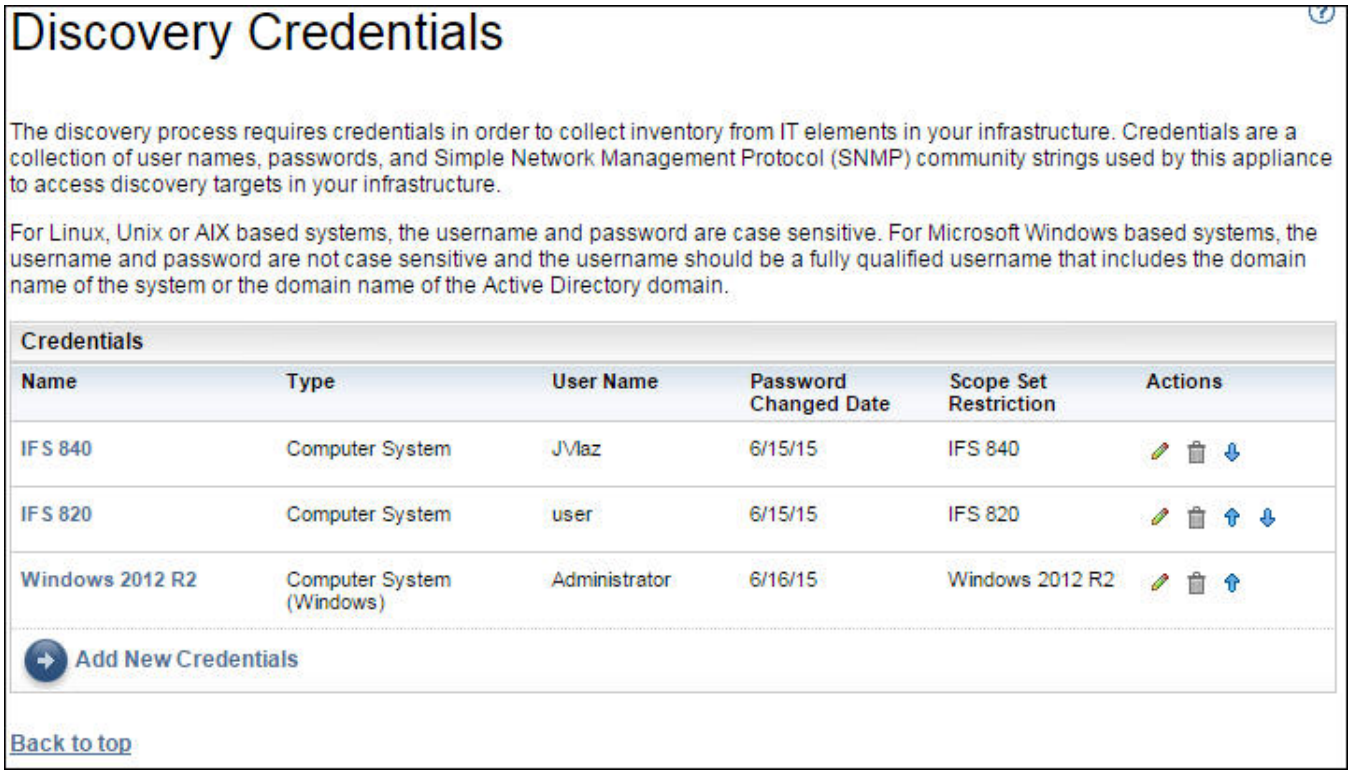

Abbildung 57. Neue Erkennungsberechtigungsnachweise

Berechtigungsnachweisdetails anzeigen

Sie können Detailinformationen zu einem bestimmten Erkennungsberechtigungsnachweis anzeigen.

Informationen zu diesem Vorgang

Führen Sie zum Anzeigen der Berechtigungsnachweisdetails die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsberechtigungsnachweise**.
   Die Seite **Erkennungsberechtigungsnachweise** wird mit einer Liste aller vorhandenen Berechtigungsnachweisliste angezeigt.
2. Um Details zu einem bestimmten Berechtigungsnachweis anzuzeigen, klicken Sie auf den Namen des Berechtigungsnachweises.
   Die Seite **Erkennungsberechtigungsnachweise** wird mit näheren Informationen zum ausgewählten Berechtigungsnachweis angezeigt.

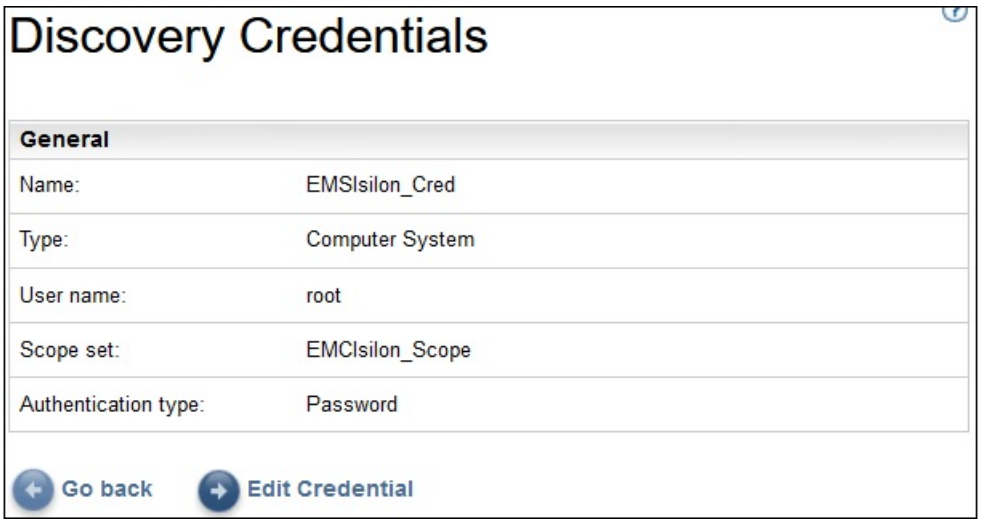

Abbildung 58. Erkennungsberechtigungsnachweise – Details

Zugehörige Tasks

Berechtigungsnachweise ändern

Sie können Berechtigungsnachweise ändern, um die Zugriffssteuerung für den Erkennungsprozess neu festzulegen.

Berechtigungsnachweise hinzufügen

Fügen Sie Berechtigungsnachweise hinzu, um die Zugriffssteuerung für den Erkennungsprozess festzulegen.

Informationen zu diesem Vorgang

Führen Sie zum Hinzufügen von Berechtigungsnachweisen die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Erkennungsberechtigungsnachweise**.
   Die Seite **Erkennungsberechtigungsnachweise** wird angezeigt.
2. Klicken Sie zum Erstellen eines Berechtigungsnachweises auf **Neue Berechtigungsnachweise hinzufügen**.
   Die Seite **Neue Erkennungsberechtigungsnachweise** wird angezeigt.

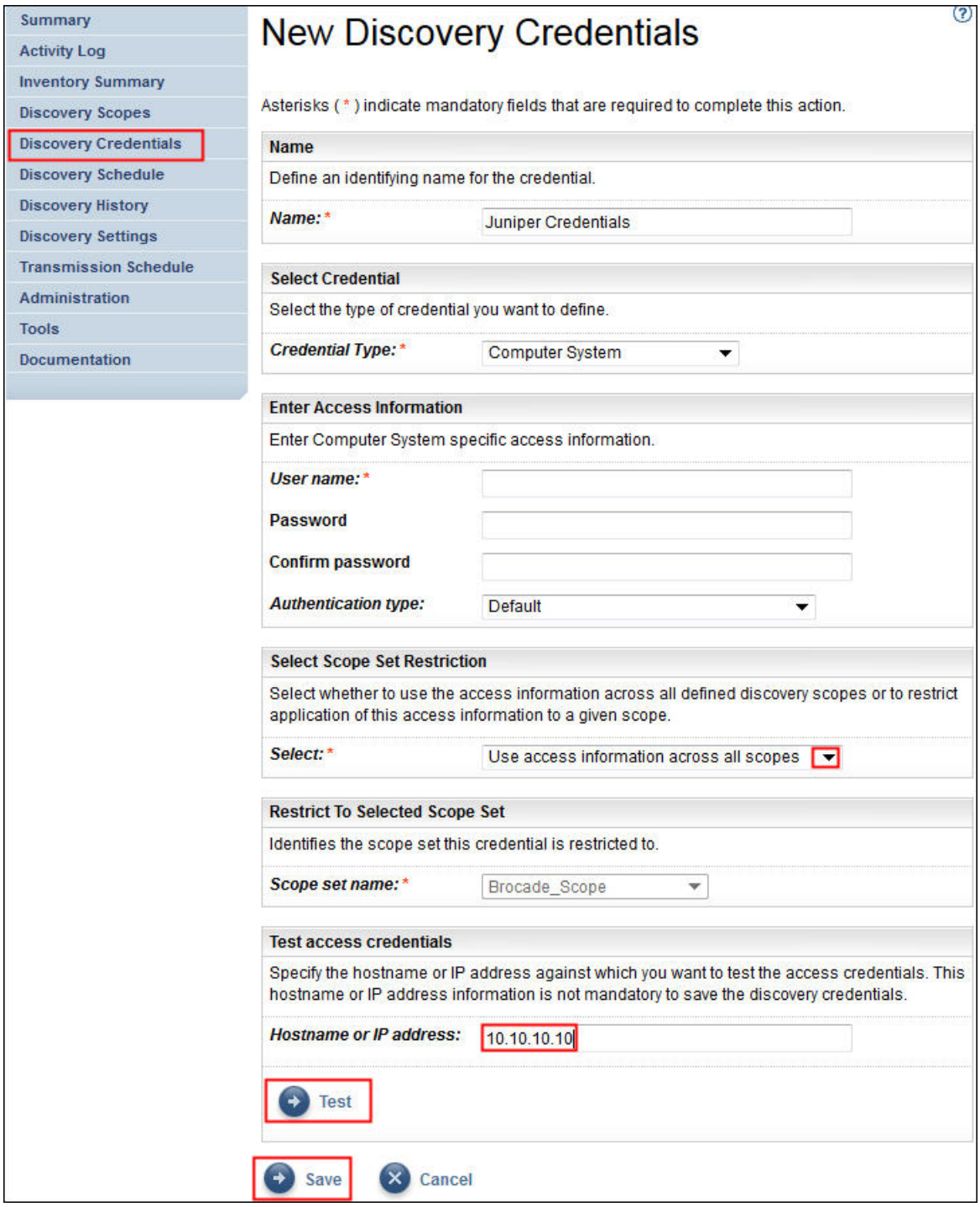

Abbildung 59. Neue Erkennungsberechtigungsnachweise

a) Geben Sie im Feld **Name** einen beschreibenden Namen für den Berechtigungsnachweis ein.

b) Wählen Sie in der Dropdown-Liste **Berechtigungsnachweistyp** den Typ des Berechtigungsnachweises aus, den Sie erstellen möchten.

c) Geben Sie im Fensterbereich **Zugriffsinformationen eingeben** die erforderlichen Informationen zum ausgewählten Berechtigungsnachweistyp ein.

   Welche Informationen erforderlich sind hängt vom jeweiligen Berechtigungsnachweistyp ab. Nähere Einzelheiten zu den erforderlichen Zugriffsinformationen für jeden Berechtigungsnachweistyp finden Sie unter „Berechtigungsnachweise und Softwareanforderungen für die Erkennungsumgebung ” auf Seite 6.

Wichtig: Die Zugriffsinformationen müssen mit den Zugriffsinformationen für die Zielressource der Erkennung übereinstimmen. Wenn Sie Zugriffsinformationen für eine Zielressource ändern, achten Sie darauf, die entsprechenden Zugriffsinformationen auf der TSA ebenfalls zu ändern. Weitere Informationen erhalten Sie im Leitfaden zum Konfigurationsassistenten der IBM Technical Support Appliance.

Tipp: Auf der Seite **Erkennungsberechtigungsnachweise** wird der Zeitpunkt angezeigt, an dem das Kennwort zuletzt geändert wurde. Wenn Sie das Kennwort auf der Zielressource regelmäßig ändern, können Sie sich anhand dieses Datums vergewissern, dass Sie das Kennwort auf der TSA ebenfalls entsprechend dem Kennwort für die Zielressource geändert haben. Informationen zum Anzeigen der Erkennungsberechtigungsnachweise finden Sie unter „Berechtigungsnachweise anzeigen" auf Seite 77.

d) Im Fensterbereich **Bereichsgruppenbeschränkung auswählen** wird angegeben, ob ein Berechtigungsnachweis auf eine einzige Bereichsgruppe beschränkt ist oder für alle Bereichsgruppen gilt. Wenn **Berechtigungsnachweistyp** den Wert **Computersystem** und **Authentifizierungstyp** den Wert **PKI** hat, wird dieser Fensterbereich nicht angezeigt. PKI-Berechtigungsnachweise müssen immer auf eine einzige Bereichsgruppe beschränkt sein.

Tipp: Durch Beschränkung der Erkennungsberechtigungsnachweise auf eine bestimmte Bereichsgruppe kann sich das Leistungsverhalten verbessern, da die Anzahl von Berechtigungsnachweisen, die an den zu erkennenden Ressourcen angewendet werden, verringert wird.

e) Der Fensterbereich **Auf ausgewählte Bereichsgruppe beschränken** wird verwendet, um einen Berechtigungsnachweis auf eine einzige Bereichsgruppe zu beschränken. Dieser Fensterbereich ist unter einer dieser beiden Bedingungen sichtbar.

- Für den Fensterbereich **Bereichsgruppenbeschränkung auswählen** wurde **Zugriffsinformationen auf angegebenen Bereich beschränken** ausgewählt oder
- Der **Berechtigungsnachweistyp** lautet **Computersystem** und der **Authentifizierungstyp** lautet **PKI**.

Der Berechtigungsnachweis wird nun nur für Erkennungen an der ausgewählten Bereichsgruppe verwendet. Bei Erkennungsoperationen an einer anderen Bereichsgruppe wird der Berechtigungsnachweis nicht verwendet. Durch diese Methode lassen sich ungültige Anmeldeversuche verhindern, die dazu führen können, dass Sie aus dem Konto ausgesperrt werden.

f) Bei Berechtigungsnachweisen des Typs **Computersystem**, **Computersystem (Windows)**, **SNMP** oder **SNMPv3** können Sie die Gültigkeit des Nachweises überprüfen. Die Funktion **Testen** für den Berechtigungsnachweistyp **Computersystem** unterstützt die folgenden Geräte:

- Geräte, die SSH- oder Telnet-basierte Authentifizierung verwenden
- XIV
- DS6000 & DS8000
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON/VNX/VMAX via EMC SMI-S
- IBM TS3100/TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4300
- IBM TS4500
- IBM TS7700
- IBM DS3000, DS4000 und DS5000, sofern kennwortgeschützt
- Windows
- Palo Alto Networks (PAN-OS)

Zum Testen von Berechtigungsnachweisen geben Sie die IP-Adresse oder den Hostnamen des Ziels ein, an dem Sie die Berechtigungsnachweise testen möchten, und klicken Sie auf **Testen**.

Anmerkung:

- Der eingegebene Hostname darf keinen Unterstrich ("_") enthalten.
- Zum Ausführen von Erkennungsoperationen oder zum Testen von Berechtigungsnachweisen auf Systemen mit den Betriebssystemen Linux, AIX, IBM i oder HP-UX muss SSH aktiviert sein.

g) Klicken Sie auf **Speichern**.

Der neue Berechtigungsnachweis wird auf der Seite **Erkennungsberechtigungsnachweise** angezeigt.

Anmerkung: Als Best Practice wird empfohlen, vor dem Erstellen oder Ändern von Erkennungsberechtigungsnachweisen eine Sicherung der TSA-Konfiguration zu erstellen.

3. Zum Ändern der Reihenfolge, in der ein Berechtigungsnachweis von der TSA beim Zugriff auf eine Ressource verwendet wird, können Sie den betreffenden Berechtigungsnachweis mithilfe der Symbole **Aufwärtspfeil** und **Abwärtspfeil** in der Liste verschieben.

Informationen zur Anwendung der Reihenfolge finden Sie unter „Erkennungsberechtigungsnachweise" auf Seite 2.

Die Seite **Erkennungsberechtigungsnachweise** wird mit der neuen Reihenfolge angezeigt.

Berechtigungsnachweise ändern

Sie können Berechtigungsnachweise ändern, um die Zugriffssteuerung für den Erkennungsprozess neu festzulegen.

Informationen zu diesem Vorgang

Führen Sie zum Ändern von Berechtigungsnachweisen die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsberechtigungsnachweise**.

   Die Seite **Erkennungsberechtigungsnachweise** wird mit einer Liste aller vorhandenen Berechtigungsnachweisliste angezeigt.

2. Zum Bearbeiten des Berechtigungsnachweises klicken Sie auf das Symbol **Bearbeiten** ( ) neben dem Berechtigungsnachweis.

   Die Seite **Erkennungsberechtigungsnachweise bearbeiten** wird angezeigt.

   a) Im Fensterbereich **Zugriffsinformationen ändern** können Sie die Zugriffsinformationen für diesen Berechtigungsnachweisändern.

   Wichtig: Die Zugriffsinformationen müssen mit den Zugriffsinformationen für die Zielressource der Erkennung übereinstimmen. Wenn Sie Zugriffsinformationen für eine Zielressource ändern, achten Sie darauf, die entsprechenden Zugriffsinformationen auf der TSA ebenfalls zu ändern. Weitere Informationen erhalten Sie im Leitfaden zum Konfigurationsassistenten der IBM Technical Support Appliance.

   Tipp: Auf der Seite **Erkennungsberechtigungsnachweise** wird der Zeitpunkt angezeigt, an dem das Kennwort zuletzt geändert wurde. Wenn Sie das Kennwort auf der Zielressource regelmäßig ändern, können Sie sich anhand dieses Datums vergewissern, dass Sie das Kennwort auf der TSA ebenfalls entsprechend dem Kennwort für die Zielressource geändert haben. Informationen zum Anzeigen der Erkennungsberechtigungsnachweise finden Sie unter „Berechtigungsnachweise anzeigen" auf Seite 77.

   b) Im Fensterbereich **Bereichsgruppenbeschränkung auswählen** wird angegeben, ob ein Berechtigungsnachweis auf eine einzige Bereichsgruppe beschränkt ist oder für alle Bereichsgruppen gilt. Wenn **Berechtigungsnachweistyp** den Wert **Computersystem** und **Authentifizierungstyp** den

Wert **PKI** hat, wird dieser Fensterbereich nicht angezeigt. PKI-Berechtigungsnachweise müssen immer auf eine einzige Bereichsgruppe beschränkt sein.

Tipp: Durch Beschränkung der Erkennungsberechtigungsnachweise auf eine bestimmte Bereichsgruppe kann sich das Leistungsverhalten verbessern, da die Anzahl von Berechtigungsnachweisen, die an den zu erkennenden Ressourcen angewendet werden, verringert wird.

c) Der Fensterbereich **Auf ausgewählte Bereichsgruppe beschränken** wird verwendet, um einen Berechtigungsnachweis auf eine einzige Bereichsgruppe zu beschränken. Dieser Fensterbereich ist unter einer dieser beiden Bedingungen sichtbar:

- Für den Fensterbereich **Bereichsgruppenbeschränkung auswählen** wurde **Zugriffsinformationen auf angegebenen Bereich beschränken** ausgewählt oder
- Der **Berechtigungsnachweistyp** lautet **Computersystem** und der **Authentifizierungstyp** lautet **PKI**.

Der Berechtigungsnachweis wird nur bei Erkennungsoperationen in der ausgewählten Bereichsgruppe verwendet. In anderen Bereichsgruppen wird der Berechtigungsnachweis nicht verwendet. Durch diese Methode lassen sich ungültige Anmeldeversuche verhindern, die dazu führen können, dass der Benutzer aus dem Konto ausgesperrt wird.

d) Bei Berechtigungsnachweisen des Typs **Computersystem**, **Computersystem (Windows)**, **SNMP** oder **SNMPv3** können Sie die Gültigkeit des Nachweises überprüfen. Um den Berechtigungsnachweis zu testen, geben Sie die IP-Adresse oder den Hostnamen des Ziels ein, an dem Sie den Berechtigungsnachweis testen möchten, und klicken Sie auf **Testen**.

Anmerkung: Der eingegebene Hostname darf keinen Unterstrich ("_") enthalten.

e) Klicken Sie auf **Speichern**.

Der geänderte Berechtigungsnachweis wird auf der Seite **Erkennungsberechtigungsnachweise** angezeigt.

3. Zum Ändern der Prioritätsreihenfolge, in der ein Berechtigungsnachweis von der TSA beim Zugriff auf eine Ressource verwendet wird, können Sie den betreffenden Berechtigungsnachweis mithilfe der Symbole **Aufwärtspfeil** ( ) und **Abwärtspfeil** ( ) in der Liste verschieben.

Informationen zur Anwendung der Reihenfolge finden Sie unter „Erkennungsberechtigungsnachweise" auf Seite 2.

Die Seite **Erkennungsberechtigungsnachweise** wird mit der neuen Reihenfolge angezeigt.

Zugehörige Konzepte

Erkennungsberechtigungsnachweise
Erkennungsberechtigungsnachweise sind eine Sammlung von Benutzernamen, Kennwörtern oder SSH-Schlüsseln sowie SNMP-Community-Zeichenfolgen (Simple Network Management Protocol), die die TSA für den Zugriff auf Ressourcen während der Erkennung verwendet.

Berechtigungsnachweise und Softwareanforderungen für die Erkennungsumgebung
Für die Erkennung von Endpunkten oder Ressourcen in Ihrer Umgebung muss die TSA Zugriff auf diese Ressourcen haben. Es empfiehlt sich, auf jeder Ressource ein spezielles Servicekonto einzurichten, das die TSA beim Zugriff auf die Ressource nutzen kann.

Berechtigungsnachweise löschen

Sie können Berechtigungsnachweise löschen, die die TSA für den Zugriff auf Ressourcen verwendet.

Informationen zu diesem Vorgang

Führen Sie zum Löschen eines Berechtigungsnachweises die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsberechtigungsnachweise**.
   Die Seite **Erkennungsberechtigungsnachweise** wird angezeigt.

2. Klicken Sie auf das Symbol **Löschen** neben dem zu löschenden Berechtigungsnachweis.
3. Klicken Sie auf **OK**, um zu bestätigen, dass der Berechtigungsnachweis gelöscht werden soll.

Erkennungszeitplan

Erkennungsoperationen werden nach einem Zeitplan ausgeführt, um sicherzustellen, dass die erkannten Daten stets aktuell und korrekt sind. Sie können den Erkennungszeitplan und die Details der letzten Erkennungsoperationen anzeigen, den Erkennungszeitplan ändern und geplante Erkennungsoperationen inaktivieren. Alternativ können Sie eine Erkennung auch jederzeit manuell ausführen.

Vorbereitende Schritte

Standardmäßig verwendet die TSA den Zeitplan "Vollständige Erkennung", um alle IT-Elemente zu erkennen, die in dynamischen HMC- und VMware-Bereichen sowie in den allgemeinen Erkennungsbereichen definiert sind. TSA breitet automatisch die Erkennung von IT-Elementen während des Erkennungsprozesses aus, um die Auswirkungen zu minimieren.

Eine Alternative besteht darin, mehrere benutzerdefinierte Zeitpläne zu erstellen. Dies ermöglicht die Erkennung von spezifischen Erkennungsbereichen, die auf verschiedene Datums- und Zeiträume verteilt werden, wenn die Auswirkungen auf Ihr Netz und Ihre IT-Elemente minimal (oder ideal) sind. In diesem Fall sollte der Zeitplan für die vollständige Erkennung zugunsten der benutzerdefinierten Zeitpläne inaktiviert werden.

Vor Beginn einer geplanten Erkennung führt die Appliance den vorgelagerten Wartungsjob aus. Während dieses Vorgangs sind einige Funktionen wie Bestandszusammenfassung, Erkennungsbereiche, Erkennungszeitpläne und Berechtigungsnachweise nicht verfügbar. Im Verlauf des vorgelagerten Wartungsjobs zeigt der **Discovery Manager**-Status in der Anzeige **Zusammenfassung** das Warnsymbol () an. Darüber hinaus wird in den TSA-Anzeigen ein Warnhinweis mit der Nachricht angezeigt, dass einige Funktionen vorübergehend nicht verfügbar sind: `As part of Pre-Discovery Maintenance, the Discovery Manager is temporarily offline. Some UI functions related to discovery or inventory could display partial or no information during this time (typically up to 10 minutes).`

Nachdem die vorgelagerte Wartung erfolgreich abgeschlossen wurde, ändert sich der **Discovery Manager**-Status auf der Seite **Zusammenfassung** in *OK* () und die vollständige Erkennungsaktivität wird fortgesetzt (innerhalb von 10 Minuten).

Erkennungszeitplan anzeigen

Sie können eine Zusammenfassung der Informationen zu einem Erkennungszeitplan anzeigen.

Informationen zu diesem Vorgang

Führen Sie zum Anzeigen des Erkennungszeitplans die folgenden Schritte durch:

Vorgehensweise

Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.

Die Seite **Erkennungszeitplan** wird angezeigt.

Im Fensterbereich **Zeitplan** werden der Name des Zeitplans, die nächste geplante Ausführung, der Ausführungszeitplan und die Aktionen (Bearbeiten ( ), Löschen ( ), Aktivieren/Inaktivieren (/), Ausführen ( )) für jeden Zeitplan angezeigt.

Klicken Sie auf das Symbol **Einblenden** ( ), um alle Bereichsgruppen anzuzeigen, die diesem Zeitplan zugeordnet sind. Beim Zeitplan für die vollständige Erkennung werden durch Klicken auf das Symbol alle Bereichsgruppen aufgelistet, die in der TSA definiert sind und standardmäßig zum Zeitplan gehören.

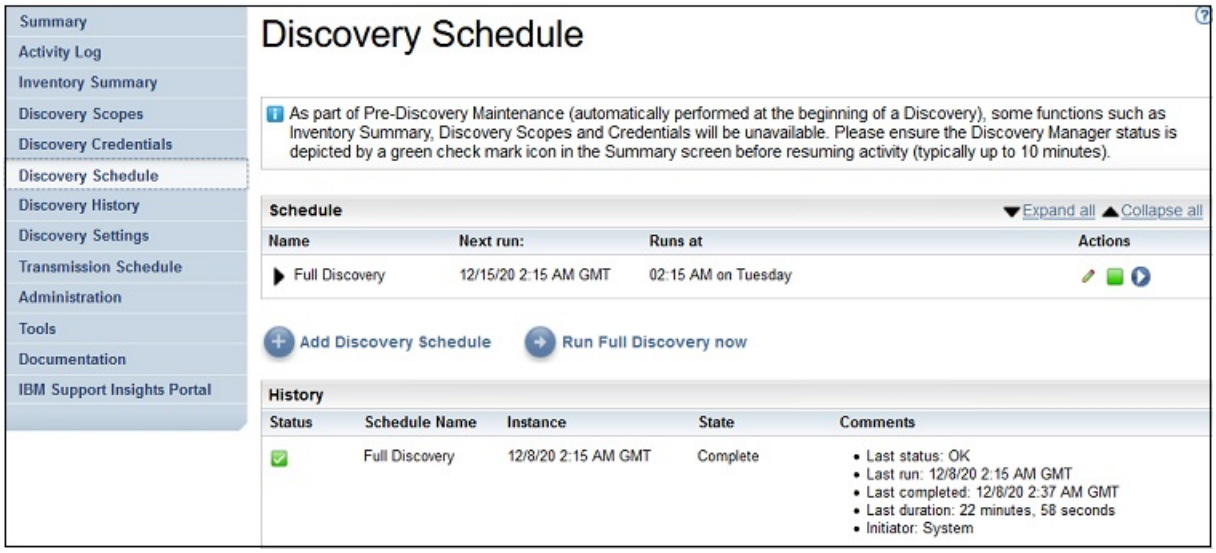

Abbildung 60. Erkennungszeitplan

Anmerkung: Wenn Sie eine TSA haben, die gerade installiert, migriert oder auf die neueste Version aktualisiert wurde, weist die neue TSA einen Erkennungszeitplan namens **Vollständige Erkennung** auf, der mit dem Standarddatum angelegt wird (2:15 Uhr am Dienstag). Der Zeitplan "Vollständige Erkennung" kann bearbeitet oder inaktiviert, aber nicht gelöscht werden. Falls vordefinierte Erkennungszeitpläne (aktiviert oder inaktiviert) vorhanden sind, werden deren Werte nach der Migration wiederhergestellt.

Im Bereich **Verlauf** sind der Status, der Zeitplanname und weitere Details des aktuell ausgeführten und der vorherigen Erkennungsjobs aufgeführt.

Erkennungszeitplan hinzufügen

Sie können neue Zeitpläne hinzufügen, um den Zeitpunkt für die Ausführung des Erkennungsprozesses festzulegen. Die neuen Zeitpläne ermöglichen es der TSA, eine Teilmenge Ihrer IT-Elemente zum geplanten Datum und Zeitpunkt zu erkennen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.
   Die Seite **Erkennungszeitplan** wird angezeigt.
2. Klicken Sie auf **Erkennungszeitplan hinzufügen**. Die Seite **Erkennungszeitplan hinzufügen** wird angezeigt.

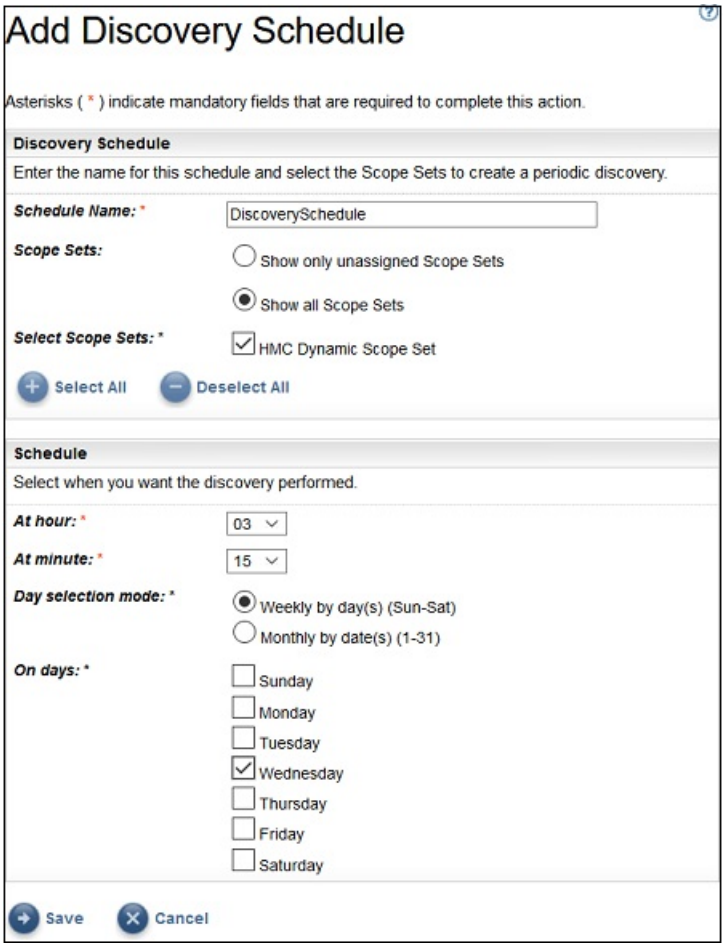

Abbildung 61. Erkennungszeitplan hinzufügen

3. Geben Sie im Feld **Zeitplanname** einen beschreibenden Namen für den Zeitplan ein.
4. **Bereichsgruppen**
   a) Wählen Sie die Option **Nur nicht zugeordnete Bereichsgruppen anzeigen** aus, um nur Bereichsgruppen anzuzeigen, die keinem anderen benutzerdefinierten Erkennungszeitplan zugeordnet sind.
   b) Wählen Sie die Option **Alle Bereichsgruppen anzeigen** aus, um alle Bereichsgruppen anzuzeigen.
5. Wählen Sie in der Liste **Bereichsgruppen auswählen** die gewünschten Bereichsgruppen aus.

   Sie können **Alles auswählen**/**Alles abwählen** verwenden, um alle oder keine Bereichsgruppen auszuwählen.
6. Wählen Sie unter **Stunde** und **Minute** einen neuen Zeitpunkt aus.
7. Legen Sie den **Tagauswahlmodus** fest.

   Wöchentlich nach Tag(en) (So-Sa)
   Um die Erkennung für einen bestimmten Tag oder mehrere Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus.

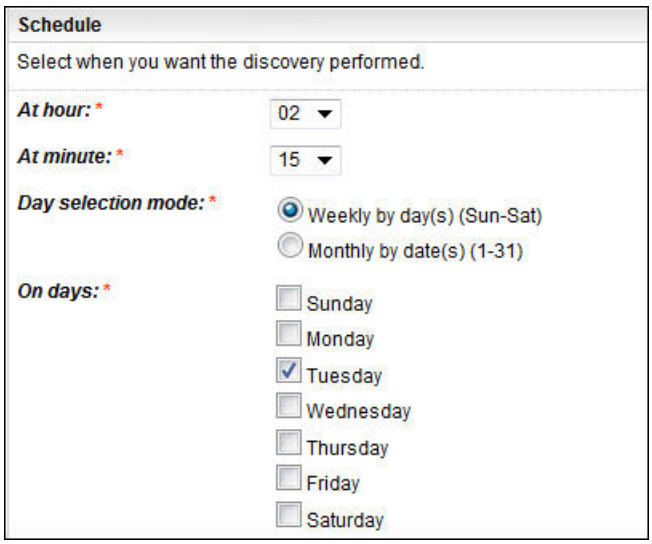

Abbildung 62. Wöchentlich nach Tag(en) (So-Sa)

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Wochentage aus.

Monatlich nach Datum (1-31)
Um die Erkennung für bestimmte Tage im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Tage im Monat aus.

Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.

8. Klicken Sie auf **Speichern**.
   Die Seite **Erkennungszeitplan** wird mit dem neuen Zeitplan angezeigt.

Erkennungszeitplan ändern

In der TSA ist ein Standardzeitplan definiert, nach dem der Erkennungsprozess zu bestimmten Zeiten ausgeführt wird. Sie können je nach Ihren Anforderungen den Standardzeitplan ändern oder die benutzerdefinierten Zeitpläne verwenden.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.
   Die Seite **Erkennungszeitplan** wird angezeigt.
2. Klicken Sie auf das Symbol **Zeitplan bearbeiten** ( ).
   Die Seite **Erkennungszeitplan bearbeiten** wird angezeigt.
   a) Bearbeiten Sie im Fensterbereich **Erkennungszeitplan** nach Bedarf die Angaben unter **Zeitplanname**, **Bereichsgruppen** und **Bereichsgruppen auswählen**.

   Anmerkung: Bei der standardmäßigen vollständigen Erkennung können diese Felder nicht bearbeitet werden.

   b) Bearbeiten Sie im Fensterbereich **Zeitplan** nach Bedarf die Angaben unter **Stunde**, **Minute**, **Tagauswahlmodus** und **Tage**.
3. Klicken Sie auf **Speichern**.
   Die Seite **Erkennungszeitplan** wird mit dem geänderten Zeitplan angezeigt.

Erkennungszeitplan inaktivieren

Sie können geplante Erkennungsoperationen inaktivieren.

Vorbereitende Schritte

Anmerkung: Wenn benutzerdefinierte Erkennungszeitpläne konfiguriert wurden, wird empfohlen, den Zeitplan **Vollständige Erkennung** zu inaktivieren, damit es nicht zu doppelten Erkennungen derselben IT-Elemente kommt.

Vorgehensweise

Führen Sie zum Inaktivieren von geplanten Erkennungen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.
   Die Seite **Erkennungszeitplan** wird angezeigt.
2. Klicken Sie auf das Symbol **Aktivieren/Inaktivieren** (/) neben dem entsprechenden Erkennungszeitplan, um diesen zu aktivieren oder zu inaktivieren.

Erkennungszeitplan löschen

Sie können vorhandene Erkennungszeitpläne löschen.

Vorgehensweise

Führen Sie zum Löschen von Erkennungszeitplänen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.
   Die Seite **Erkennungszeitplan** wird angezeigt.
2. Klicken Sie auf das Symbol () neben dem zu löschenden Zeitplan.

   Anmerkung: Der Zeitplan **Vollständige Erkennung** kann nicht gelöscht, aber auf Wunsch inaktiviert werden.

   Eine Bestätigungsnachricht in Bezug auf das Löschen des ausgewählten Erkennungszeitplans wird angezeigt.
3. Klicken Sie auf **OK**, um den Zeitplan zu löschen.

Erkennung ausführen

Sie können eine Erkennung auch auf Anforderung ausführen statt auf die nächste geplante Erkennung zu warten. Die Erkennung kann an allen definierten Erkennungsbereichen, nach einem bestimmten Erkennungszeitplan oder an bestimmten Erkennungsbereichsgruppen oder -bereichen ausgeführt werden.

Vorgehensweise

Führen Sie zum Ausführen einer Erkennung an allen definierten Bereichen die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungszeitplan**.Die Seite **Erkennungszeitplan** wird angezeigt.
2. Klicken Sie auf **Vollständige Erkennung jetzt ausführen**.Der Fensterbereich "Verlauf" wird aktualisiert und zeigt, dass die Übertragung ausgeführt wird.

   Anmerkung: Die TSA versucht, die Auswirkungen auf die Netzumgebung zu minimieren. Daher wird der Erkennungsprozess nach einer iterativen, messwertbasierten Methode durchgeführt, was dazu führen kann, dass eine vollständige Erkennung bis zu 72 Stunden dauert. Sie können den Erkennungsprozess im Abschnitt **Jobzusammenfassung** auf der Seite **Zusammenfassung** überwachen.
3. Zum Ausführen einer Erkennung an einem bestimmten Bereich klicken Sie auf das Symbol **Ausführen** () für diesen Bereich.
4. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (kli-

cken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an allgemeinen Bereichsgruppen ausführen

Vorgehensweise

Führen Sie zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**.
   Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt. Auf der Seite befindet sich eine Liste aller Bereichsgruppen, die für diese TSA definiert sind.

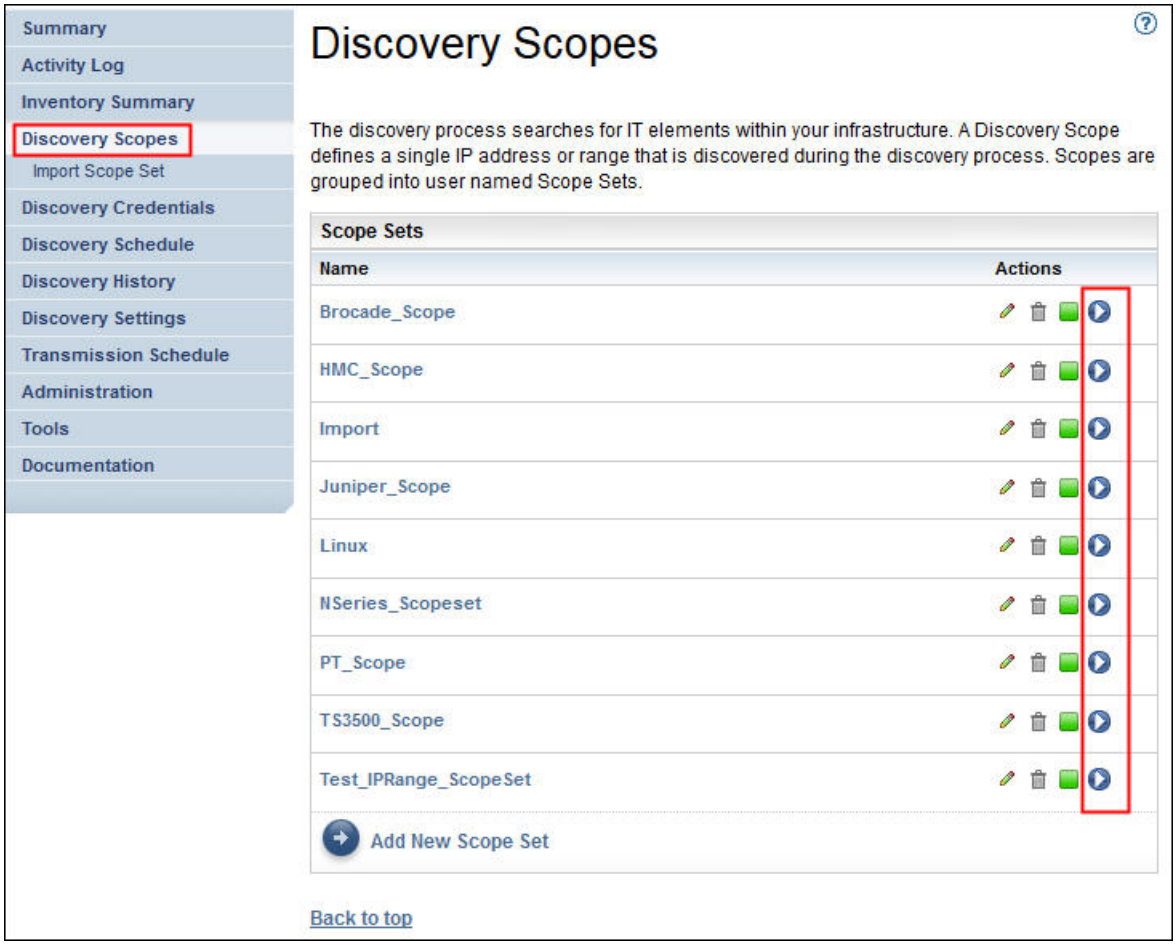

Abbildung 63. Erkennung an bestimmten Bereichen ausführen

2. Zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe klicken Sie auf das Symbol **Ausführen** ( ) für diese Bereichsgruppe.
3. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (klicken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an dynamischen HMC-Bereichsgruppen ausführen

Vorgehensweise

Führen Sie zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**.
   Die Seite **Dynamische HMC-Bereiche** wird angezeigt. Auf der Seite befindet sich eine Liste aller Bereichsgruppen, die für diese TSA definiert sind.

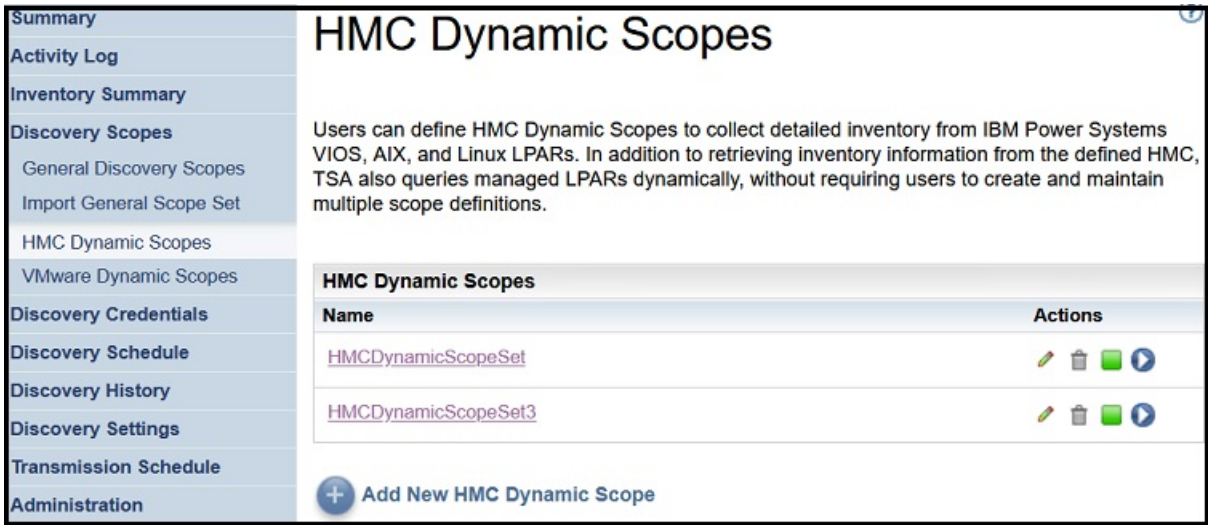

Abbildung 64. Dynamische HMC-Bereiche

2. Zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe klicken Sie auf das Symbol **Ausführen** ( ) für diese Bereichsgruppe.
3. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (klicken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an VMware-Bereichsgruppen ausführen

Vorgehensweise

Führen Sie zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe die folgenden Schritte aus:

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereichsgruppe**.
   Die Seite **Dynamische VMware-Bereichsgruppen** wird angezeigt. Auf der Seite befindet sich eine Liste aller Bereichsgruppen, die für diese TSA definiert sind.

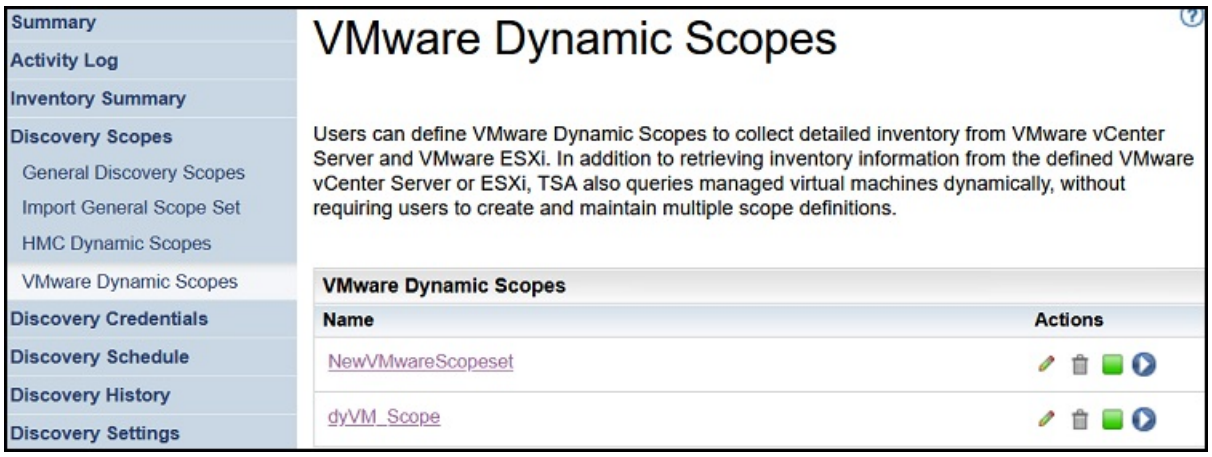

Abbildung 65. Erkennung an dynamischen VMware-Bereichsgruppen ausführen

2. Zum Ausführen einer Erkennung an einer bestimmten Bereichsgruppe klicken Sie auf das Symbol **Ausführen** ( ) für diese Bereichsgruppe.
3. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (klicken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an Bereichen ausführen

Sie können eine Erkennung auch auf Anforderung ausführen statt auf die nächste geplante Erkennung zu warten. Die Erkennung kann an allen definierten Erkennungsbereichen, nach einem bestimmten Erkennungszeitplan oder an bestimmten Erkennungsbereichsgruppen oder -bereichen ausgeführt werden.

Erkennung an allgemeinen Erkennungsbereichen ausführen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Allgemeine Erkennungsbereiche**. Die Seite **Allgemeine Erkennungsbereiche** wird angezeigt.

Abbildung 66. Erkennungsbereiche

2. Klicken Sie auf die Bereichsgruppe, die den zu erkennenden Bereich enthält.

   Die Seite **Erkennungsbereichsgruppe** wird angezeigt.Auf dieser Seite sind alle Bereiche aufgeführt, die für diese Bereichsgruppe definiert sind.

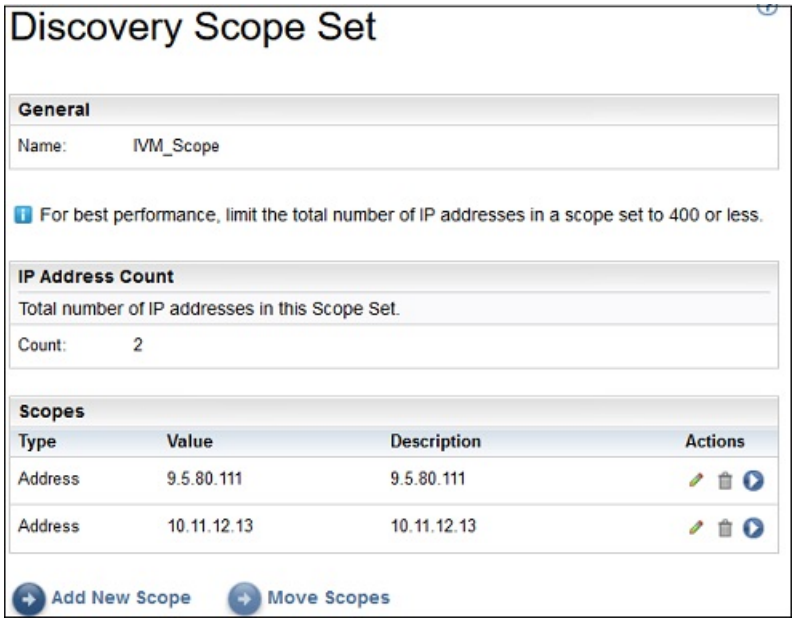

Abbildung 67. Erkennung an bestimmten Bereichen ausführen

3. Zum Ausführen einer Erkennung an einem bestimmten Bereich klicken Sie auf das Symbol **Ausführen** ( ) für diesen Bereich.
4. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (kli-

cken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an dynamischen HMC-Bereichen ausführen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische HMC-Bereiche**. Die Seite **Dynamische HMC-Bereiche** wird angezeigt.

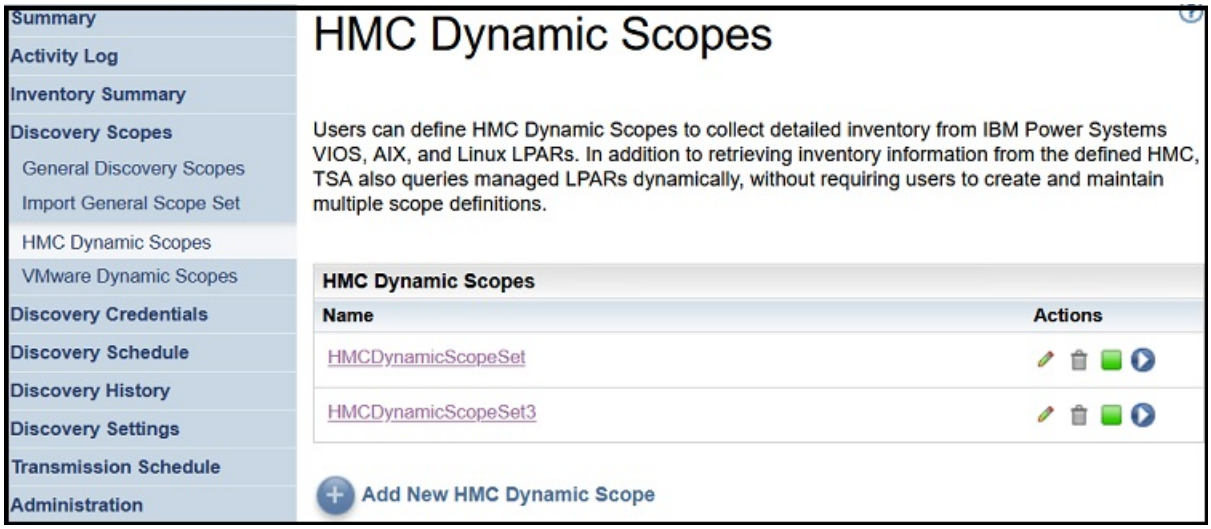

Abbildung 68. Dynamische HMC-Bereiche

2. Klicken Sie auf die Bereichsgruppe, die den zu erkennenden Bereich enthält.

   Die Seite **Dynamische HMC-Bereichsgruppe** wird angezeigt. Auf dieser Seite sind alle Bereiche aufgeführt, die für diese Bereichsgruppe definiert sind.

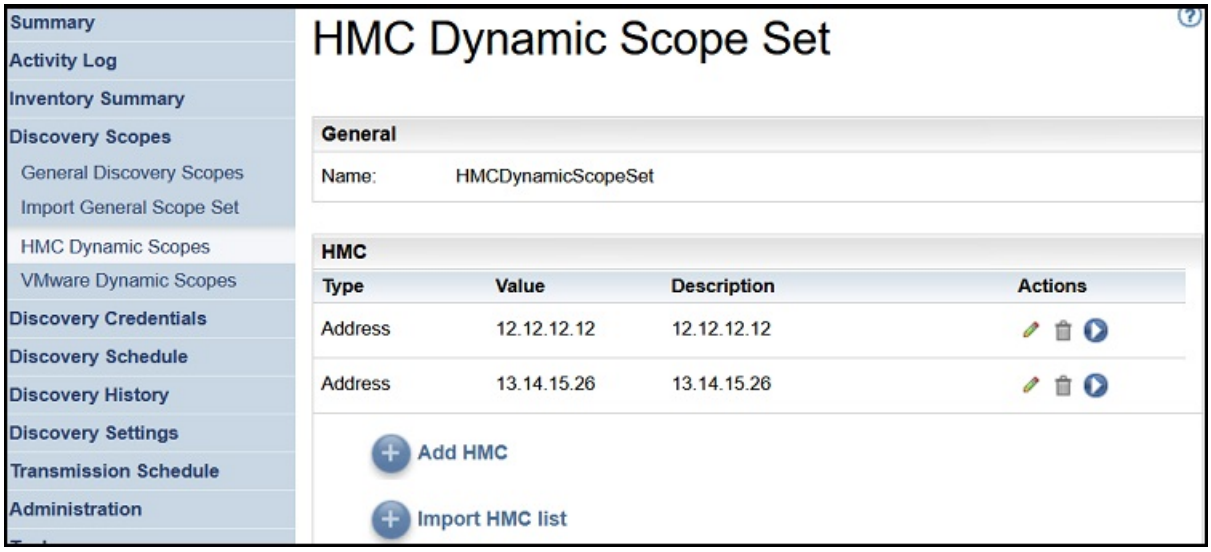

Abbildung 69. Erkennung an bestimmten Bereichen ausführen

3. Zum Ausführen einer Erkennung an einem bestimmten Bereich klicken Sie auf das Symbol **Ausführen** ( ) für diesen Bereich.
4. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (kli-

cken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennung an dynamischen VMware-Bereichen ausführen

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Erkennungsbereiche** > **Dynamische VMware-Bereiche**. Die Seite **Dynamische VMware-Bereiche** wird angezeigt.

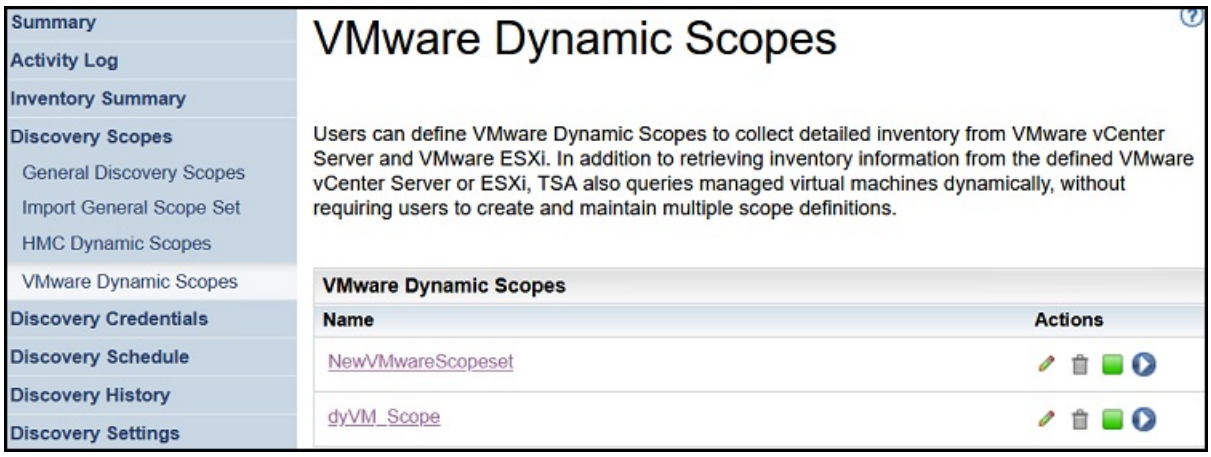

Abbildung 70. Dynamische VMware-Bereiche

2. Klicken Sie auf die Bereichsgruppe, die den zu erkennenden Bereich enthält.

   Die Seite **Dynamische VMware-Bereichsgruppe** wird angezeigt. Auf dieser Seite sind alle Bereiche aufgeführt, die für diese Bereichsgruppe definiert sind.

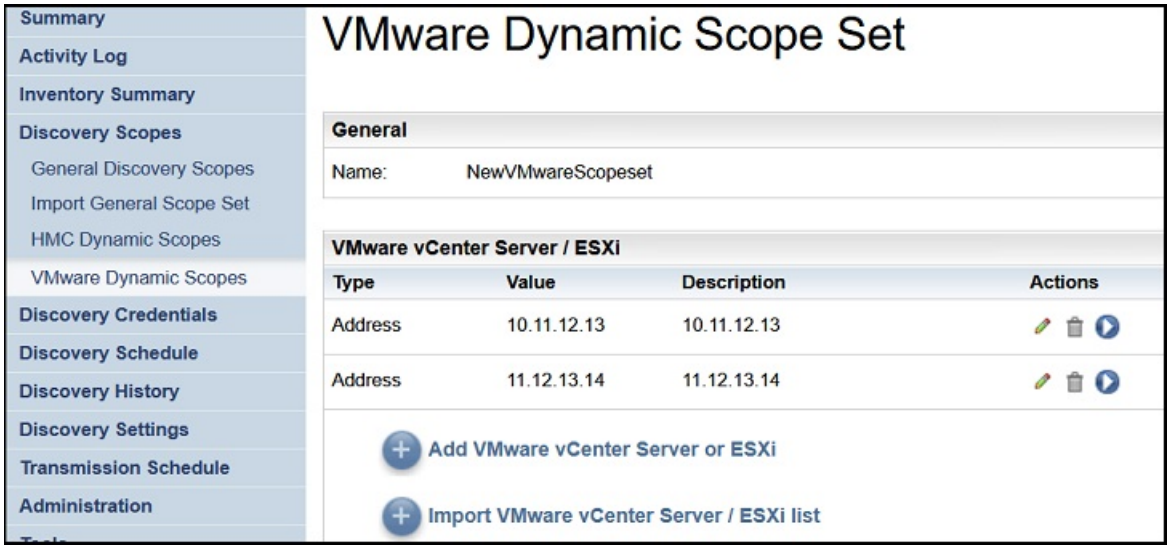

Abbildung 71. Erkennung an dynamischen VMware-Bereichen ausführen

3. Zum Ausführen einer Erkennung an einem bestimmten Bereich klicken Sie auf das Symbol **Ausführen** (▶) für diesen Bereich.
4. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Erkennung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (klicken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Erkennung sollte ohne Fehler abgeschlossen sein.

Erkennungsverlauf

Sie können Details zu einer ausgeführten Erkennung anzeigen und die Diagnoseprotokolldatei zu der Erkennung herunterladen.

Vorgehensweise

Führen Sie die folgenden Schritte durch, um den Erkennungsverlauf anzuzeigen oder eine Diagnoseprotokolldatei herunterzuladen:

1. Klicken Sie im Navigationsbereich auf **Erkennungsverlauf**.

   Die Seite **Erkennungsverlauf** wird angezeigt. Eine Liste mit Erkennungseinträgen wird angezeigt. Jeder Eintrag enthält den Status, den Namen sowie die Start- und Endzeitpunkte einer Erkennung.

   

   Abbildung 72. Erkennungsverlauf
2. Um weitere Informationen zu einem Eintrag in der Liste **Verlaufseinträge** anzuzeigen, klicken Sie auf den Namen des Eintrags.

   Im Fensterbereich **Eintragsinformationen** werden nähere Einzelheiten zur ausgewählten Erkennung angezeigt.
3. Zum Herunterladen einer Diagnoseprotokolldatei für eine Erkennung klicken Sie auf das Symbol **Download** (⭳) für die Erkennung.
4. Zum Löschen einer Diagnoseprotokolldatei für eine Erkennung klicken Sie auf das Symbol **Löschen** (🗑).

Übertragungszeitplan

Die Übertragung von Daten erfolgt nach einem Zeitplan, um sicherzustellen, dass die erkannten Daten regelmäßig an den IBM Support gesendet werden. Sie können den Übertragungszeitplan und die Details der letzten Übertragungen anzeigen, den Übertragungszeitplan ändern und geplante Übertragungen inaktivieren. Alternativ können Sie Ihre Daten auch jederzeit manuell an IBM senden.

Übertragungszeitplan anzeigen

Sie können eine Zusammenfassung der Informationen zu einem Übertragungszeitplan anzeigen.

Informationen zu diesem Vorgang

Führen Sie zum Anzeigen des Übertragungszeitplans die folgenden Schritte durch:

Vorgehensweise

Klicken Sie im Navigationsbereich auf **Übertragungszeitplan**.

Die Seite **Übertragungszeitplan** wird angezeigt.

Im Fensterbereich **Zeitplan** werden die nächste geplante Ausführung und die definierten Ausführungszeitpunkte angezeigt. Im Bereich **Verlauf** sind der Status und weitere Details des aktuell ausgeführten und der vorherigen Übertragungsjobs aufgeführt.

Übertragungszeitplan ändern

In der TSA ist ein Standardzeitplan definiert, nach dem der Übertragungsprozess zu bestimmten Zeiten ausgeführt wird. Sie können diesen Zeitplan gemäß Ihren Anforderungen ändern.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Übertragungszeitplan**.

Die Seite **Übertragungszeitplan** wird angezeigt.

Im Fensterbereich **Zeitplan** werden die nächste geplante Ausführung und die definierten Ausführungszeitpunkte angezeigt. Im Bereich **Verlauf** sind der Status und weitere Details des aktuell ausgeführten und der vorherigen Übertragungsjobs aufgeführt.

2. Klicken Sie auf **Zeitplan bearbeiten**.
   Die Seite **Übertragungszeitplan** wird angezeigt.

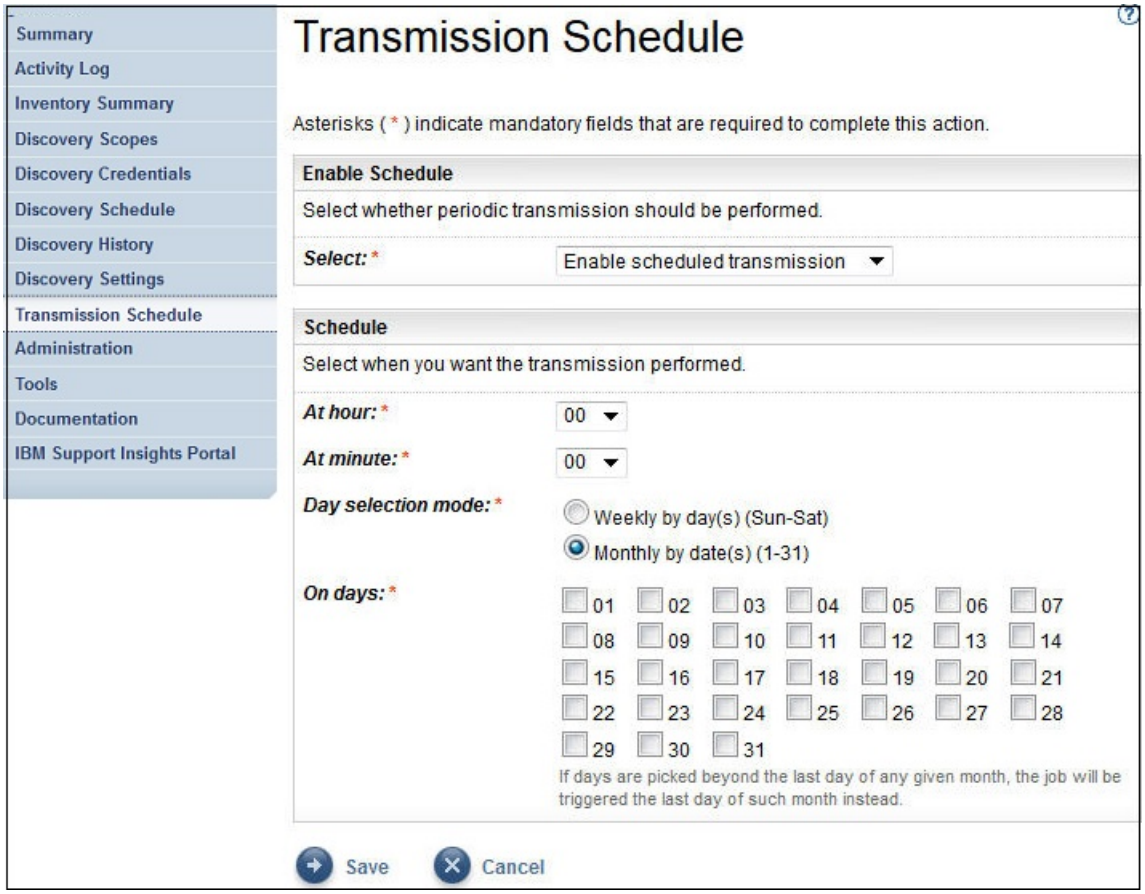

Abbildung 73. Übertragungszeitplan bearbeiten

a) Wählen Sie mithilfe der Dropdown-Listen **Stunde** und **Minute** einen neuen Zeitpunkt aus.

b) Legen Sie den **Tagauswahlmodus** fest.

Wöchentlich nach Tag(en) (So-Sa)
Um die Übertragung für einen bestimmten Tag oder mehrere Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus.

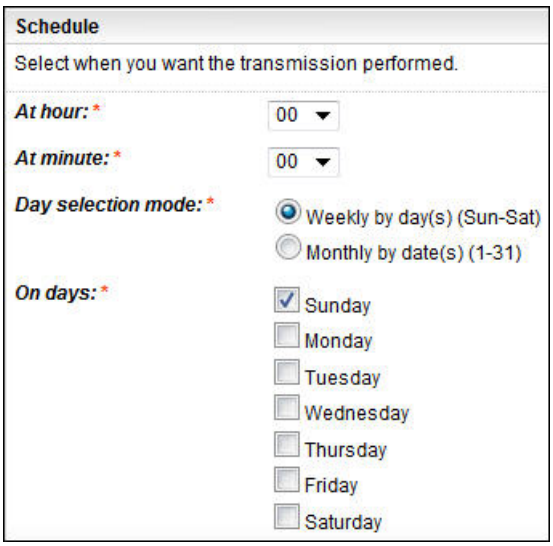

Abbildung 74. Wöchentlich nach Tag(en) (So-Sa)

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Wochentage aus.

Monatlich nach Datum (1-31)
Um die Übertragung für bestimmte Tage im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Tage im Monat aus.

Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.

3. Klicken Sie auf **Speichern**.
   Die Seite **Übertragungszeitplan** wird mit dem neuen Zeitplan angezeigt.

Übertragungszeitplan inaktivieren

Sie können geplante Datenübertragungen inaktivieren.

Vorgehensweise

Führen Sie zum Inaktivieren von geplanten Übertragungen die folgenden Schritte durch:

1. Klicken Sie im Navigationsfenster auf **Übertragungszeitplan**.
   Die Seite **Übertragungszeitplan** wird angezeigt.
2. Klicken Sie auf **Zeitplan bearbeiten**.
   Die Seite **Übertragungszeitplan** wird angezeigt.
3. Wählen Sie im Fensterbereich **Zeitplan aktivieren** die Option **Geplante Übertragung inaktivieren** aus.
4. Klicken Sie auf **Speichern**.
   Die Seite **Erkennungszeitplan** wird angezeigt und im Bereich **Zeitplan** ist zu sehen, dass die geplante Erkennung inaktiviert ist. Durch Klicken auf **Geplante Übertragung aktivieren** können Sie geplante Übertragungen aktivieren.

Übertragung ausführen

Sie können eine Übertragung auch auf Anforderung ausführen statt auf die nächste geplante Übertragung zu warten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Übertragungszeitplan**.

Die Seite **Übertragungszeitplan** wird angezeigt.

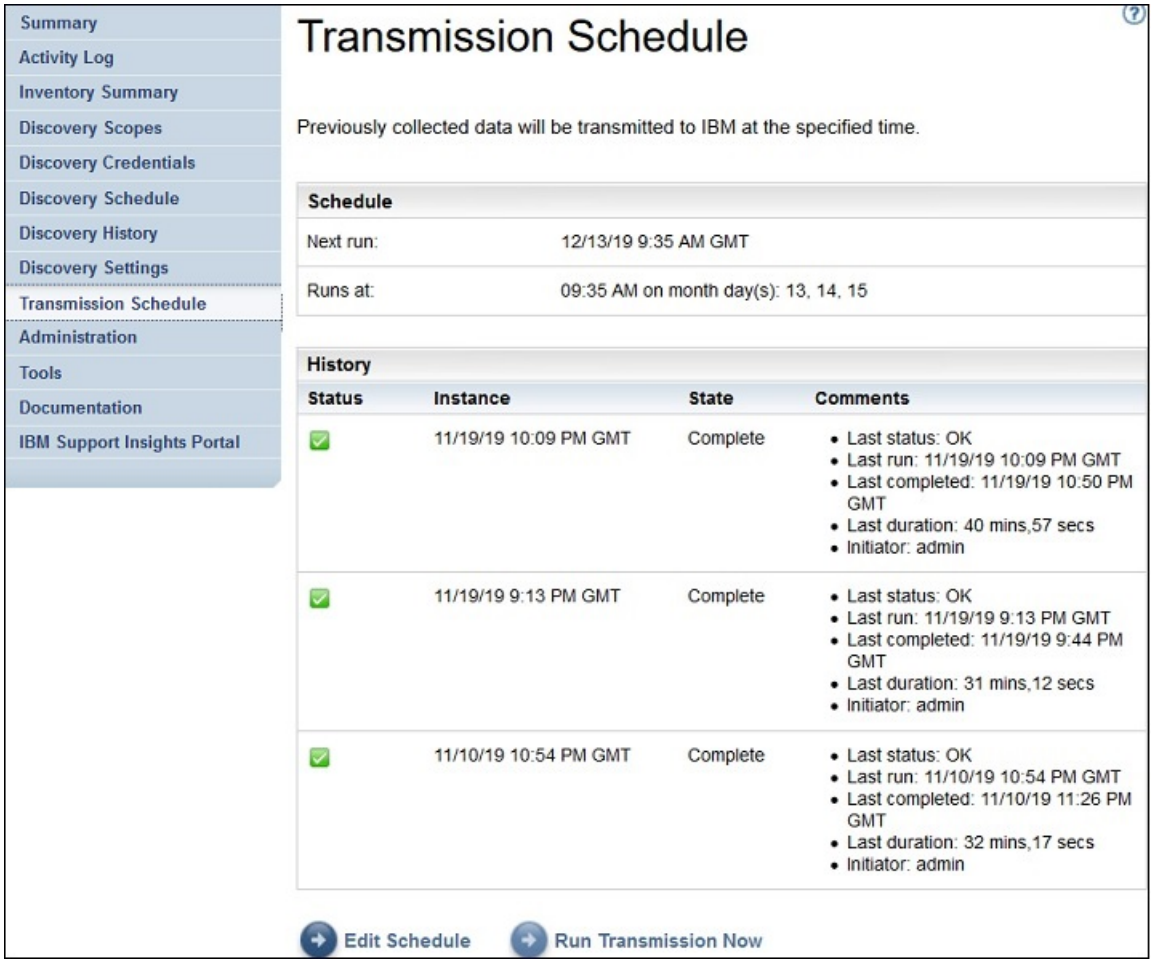

Abbildung 75. Übertragung jetzt ausführen

2. Klicken Sie auf **Übertragung jetzt ausführen**.

   Der Fensterbereich **Verlauf** wird aktualisiert und zeigt, dass die Übertragung ausgeführt wird.

3. Rufen Sie die Seite **Zusammenfassung** auf (klicken Sie im Navigationsbereich auf **Zusammenfassung**). Die Übertragung wird im Fensterbereich **Jobzusammenfassung** angezeigt. Die Seite **Zusammenfassung** wird laufend aktualisiert, um den aktuellen Status der TSA zu zeigen. Wenn der Job nicht mehr im Bereich **Jobzusammenfassung** angezeigt wird, überprüfen Sie das **Aktivitätenprotokoll** (klicken Sie im Navigationsbereich auf **Aktivitätenprotokoll**). Die Übertragung sollte ohne Fehler abgeschlossen sein.

Datenmomentaufnahme

Sie können eine lokale Kopie der von der TSA gesammelten unformatierten Rohdaten erstellen und speichern, ohne die Daten an IBM zu übertragen. Sie können auch die letzten Daten anzeigen, die an IBM übertragen wurden.

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Datenmomentaufnahme**. Die Seite **Datenmomentaufnahme** wird angezeigt.

Abbildung 76. Datenmomentaufnahme

Anmerkung: Die Schaltfläche **Letzte Datenmomentaufnahme herunterladen** ist nur aktiviert, wenn eine abgeschlossene Übertragung oder Datenmomentaufnahme vorhanden ist.

2. Klicken Sie auf **Datenmomentaufnahme jetzt erstellen**, um die zuletzt von der TSA erkannten Daten zu erfassen und eine neue Datenmomentaufnahme zu erstellen. Die folgende Nachricht wird angezeigt: `Datenmomentaufnahme in Bearbeitung. Dies kann bis zu 2 Stunden dauern. Den Status sehen Sie auf den Seiten 'Aktivitätenprotokoll' oder 'Zusammenfassung'.` Klicken Sie im Navigationsmenü auf **Zusammenfassung**, um die Seite **Zusammenfassung** zu öffnen. Im Fensterbereich **Jobzusammenfassung** wird der Status für die Erfassung der Datenmomentaufnahme angezeigt, bis diese abgeschlossen ist. Klicken Sie im Navigationsmenü auf **Aktivitätenprotokoll**, um den Fertigstellungsstatus für die angeforderte Datenmomentaufnahme anzuzeigen.
3. Nachdem die Übertragung oder Datenmomentaufnahme abgeschlossen ist, wird das **Datum der Datenmomentaufnahme** angezeigt.

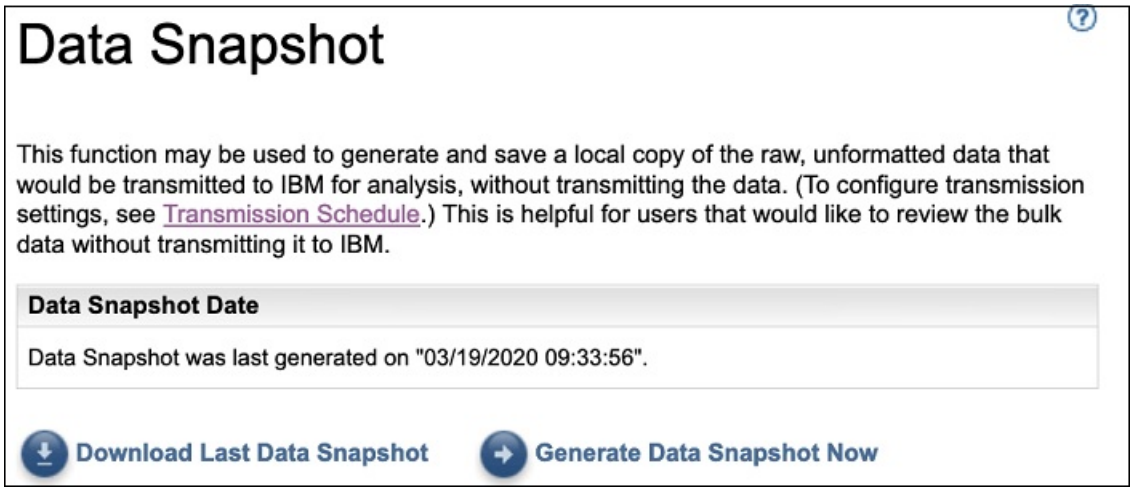

Abbildung 77. Datum der Datenmomentaufnahme

4. Klicken Sie auf **Letzte Datenmomentaufnahme herunterladen**, um die letzte Datenmomentaufnahme herunterzuladen. Geben Sie einen Speicherort für die zugehörige Datei (*collection.tar.xz*) an. Je nach Datenvolumen kann die Downloadoperation einige Zeit dauern. Zum Extrahieren der Inhalte des *.tar.xz*-Archivs können Sie die Dienstprogramme *tar* (für Linux) oder *7-Zip* (für Linux und Windows verfügbar) verwenden.

   Anmerkung:

   - Falls gerade ein Übertragungs- oder Erfassungsjob läuft, wird die folgende Nachricht angezeigt: `Aktuell wird ein Erfassungsjob ausgeführt. Die aktuellste Datenmomentaufnahme wurde erstellt am <<Zeitmarke>>. Wollen Sie diese Datensammlung wirklich herunterladen?`
     - Klicken Sie auf **OK**, um mit dem Herunterladen zu beginnen.
     - Klicken Sie auf **Abbrechen**, um das Herunterladen abzubrechen und auf die Fertigstellung des aktuellen Erfassungsjobs zu warten.

- Falls kein Übertragungs- oder Erfassungsjob läuft, wird die folgende Nachricht angezeigt: `Die aktuellste Datenmomentaufnahme wurde erstellt am <<Zeitmarke>>. Wollen Sie diese Datensammlung wirklich herunterladen?` Klicken Sie auf **OK**, um mit dem Herunterladen zu beginnen.

Bestandszusammenfassung anzeigen

Auf der Seite **Bestandszusammenfassung** wird eine Übersicht über die in die Erkennung einbezogenen IT-Elemente wie Computersysteme, Betriebssysteme und Speichersubsysteme angezeigt.

Klicken Sie im Navigationsbereich auf **Bestandszusammenfassung**, um die Seite **Bestandszusammenfassung** anzuzeigen.

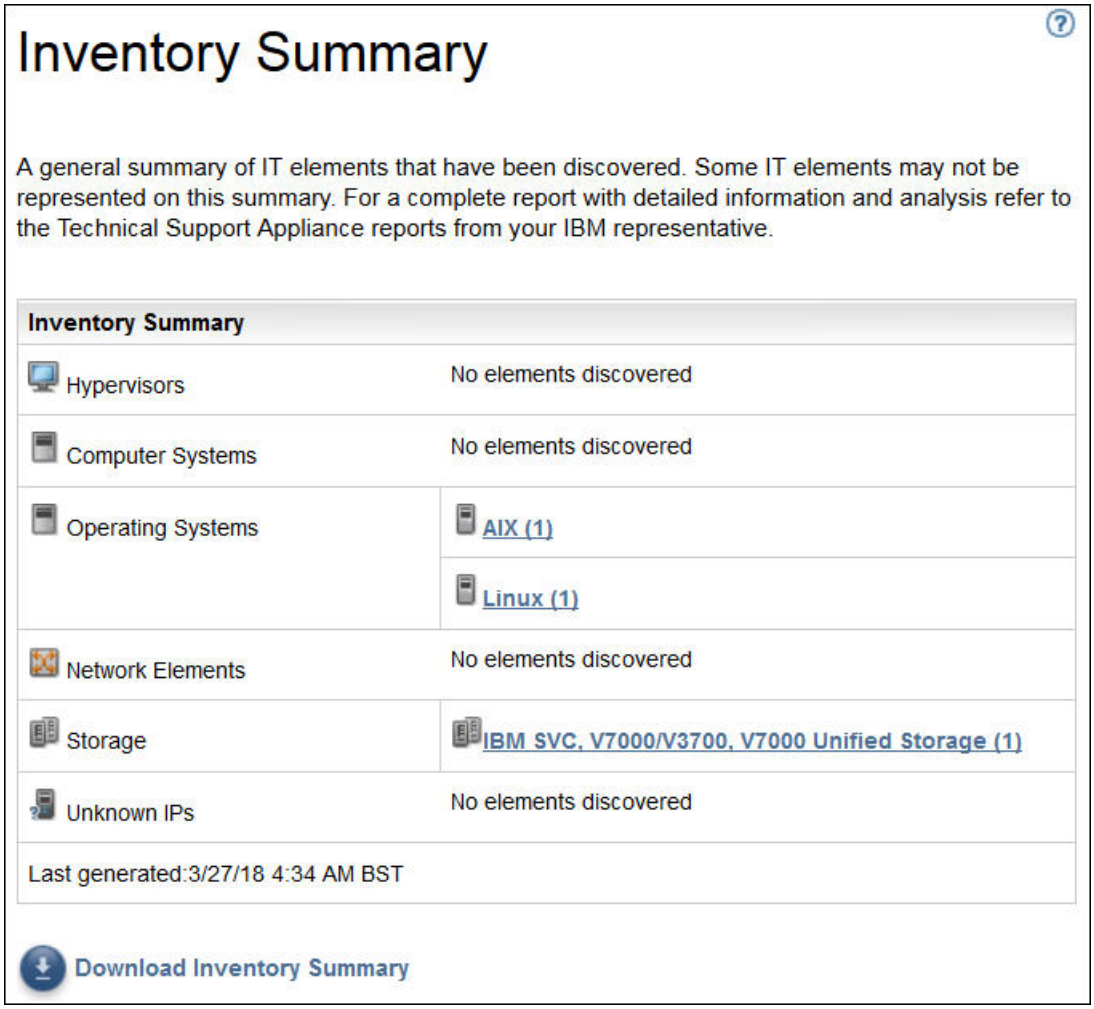

Abbildung 78. Bestandszusammenfassung

Die Seite "Bestandszusammenfassung" zeigt sechs verschiedene Gruppen von IT-Elementen:

- **Hypervisoren**: Umfasst Hypervisoren wie HMC, IBM Flex System Manager, VMware, VIOS usw.
- **Computersysteme**: Umfasst physische Computersysteme.
- **Betriebssysteme**: Umfasst Betriebssysteme wie AIX, Linux usw., die auf Bare-Metal-Systemen oder in einer virtualisierten Umgebung ausgeführt werden.
- **Netzelemente**: Umfasst Switches und Router.
- **Speicher**: Umfasst Speichersubsysteme wie IBM XIV, IBM FlashSystem, EMC und HP Speichereinheiten. Beinhaltet auch Bandeinheiten.
- **Unbekannte IPs**: Geräte, die unter anderem aus folgenden Gründen nicht klassifiziert werden konnten:

- Gerätezugriff wird durch eine Firewall blockiert.
- Für das Gerät sind keine Berechtigungsnachweise definiert. Auf der Seite **Authentifizierungsstatus** (**Tools** → **Authentifizierungsstatus**) finden Sie Informationen zu IP-Adressen und zugehörigen Berechtigungsnachweisen.
- Für den Gerätetyp ist kein Sensor vorhanden.

- In der Zeile **Zuletzt generiert** ist der Zeitpunkt angegeben, an dem die letzte Bestandszusammenfassung erstellt wurde.

Anmerkung: Die Daten in diesem Fensterbereich werden kurz nach dem Start der TSA eingefügt. Wenn Sie die Seite innerhalb dieser Zeitspanne öffnen, wird eine Informationsnachricht angezeigt: **`Bestandszusammenfassung wird generiert`**. Nach dem Einfügen der Zusammenfassungsdaten werden diese etwa alle 30 Minuten aktualisiert. Klicken Sie auf das Symbol **Aktualisieren** des Browsers, um eine manuelle Aktualisierung durchzuführen.

Jede Gruppe enthält eine Liste von Gerätetypen und die Anzahl der Geräte des jeweiligen Typs.

1. Klicken Sie auf einen der Gerätetypen-Hyperlinks, um die Seite **Bestandszusammenfassung – Details** anzuzeigen.

Abbildung 79. Bestandszusammenfassung – Details

2. Wählen Sie ein Gerät aus der Liste aus, um die zugehörigen **Elementinformationen** wie *Kontext-IP*, *Hersteller*, *Modell* und *Seriennummer* anzuzeigen.

   Anmerkung: Für Geräte, die von der TSA erkannt werden, für die jedoch keine gültigen Berechtigungsnachweise definiert wurden, sind keine **Elementinformationen** angegeben. TSA erfordert eine erfolgreiche Anmeldung am Gerät, um diese Einzelheiten bereitstellen zu können.

Klicken Sie auf **Bestandszusammenfassung herunterladen**, um eine Datei mit einer Zusammenfassung der erkannten Geräte herunterzuladen.

Erkennungsprobleme debuggen

Authentifizierungsstatus

Auf der Seite **Authentifizierungsstatus** wird eine Zusammenfassung der IT-Elemente angezeigt, die in Bereichsgruppen definiert sind und bei denen Probleme mit Berechtigungsnachweisen bestehen.

Zum Anzeigen des Authentifizierungsstatus klicken Sie im Navigationsbereich auf **Tools** > **Authentifizierungsstatus**. Die Seite **Authentifizierungsstatus** wird angezeigt.

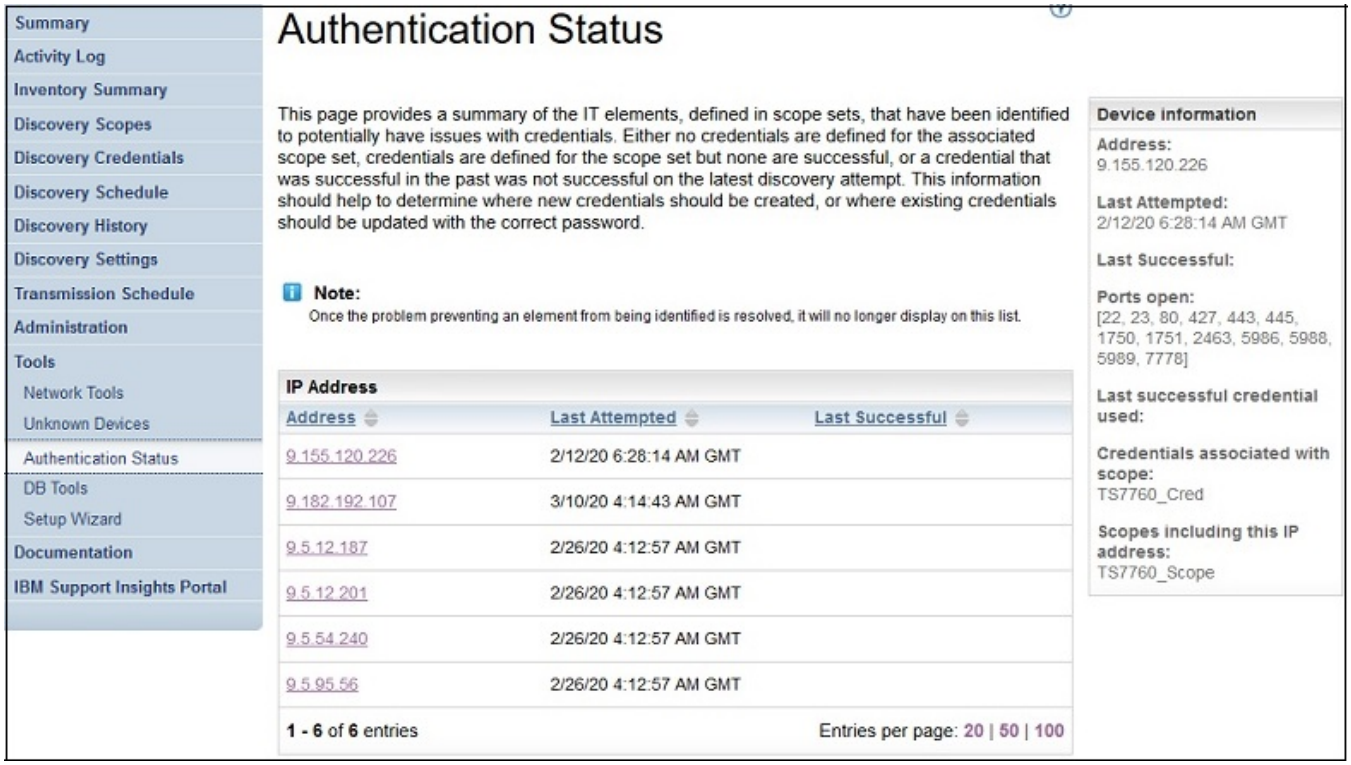

Abbildung 80. Authentifizierungsstatus

Die Statusanzeige enthält alle Geräte-IPs, für die Probleme mit Berechtigungsnachweisen gemeldet wurden. Die Probleme können folgende Ursachen haben:

- Für die zugehörige Bereichsgruppe wurden keine Berechtigungsnachweise definiert.
- Für die Bereichsgruppe wurden zwar Berechtigungsnachweise definiert, sie konnten jedoch nicht erfolgreich angewendet werden.
- Berechtigungsnachweise, die in der Vergangenheit ordnungsgemäß funktioniert haben, konnten beim letzten Erkennungsversuch nicht erfolgreich angewendet werden.

Klicken Sie auf den betreffenden IP-Adressenlink, um Gerätedaten wie *Zuletzt versucht*, *Zuletzt erfolgreich*, *Offene Ports*, *Letzter erfolgreich verwendeter Berechtigungsnachweis*, *Datum der letzten Änderung des Berechtigungsnachweises*, *Berechtigungsnachweis für Bereich* und *Bereiche mit dieser IP-Adresse* anzuzeigen. Diese Informationen sind hilfreich, um zu entscheiden, ob neue Berechtigungsnachweise erstellt werden müssen oder ob es genügt, die vorhandenen Berechtigungsnachweise mit dem richtigen Kennwort zu aktualisieren.

Anmerkung: – Wenn das Berechtigungsnachweisproblem bei einem Gerät behoben ist, wird die betreffende Geräte-ID von der Liste entfernt.

Unbekannte Einheiten

Sie können Informationen zu Geräten anzeigen, die von der TSA erkannt wurden, aber nicht genau identifiziert werden konnten.

Zum Anzeigen dieser unbekannten Geräte klicken Sie im Navigationsbereich auf **Tools** > **Unbekannte Einheiten**. Die Seite **Unbekannte Einheiten** wird angezeigt.

Durch Klicken auf einen Eintrag in der Liste "Unbekannte IPs" können Sie weitere Informationen zu dem betreffenden Gerät anzeigen.

Kapitel 6. Verwaltungsaufgaben einrichten

Statusinformationen

Die TSA bietet eine Übersicht über Informationen, Protokolle und Berichte, um Ihnen zu helfen, schnell Informationen zu Jobs, erkannten Beständen und Produktdaten zu finden.

Sie können die zusammenfassenden Informationen zu Jobs, Beständen und Produktdaten anzeigen, indem Sie im Navigationsbereich auf **Zusammenfassung** klicken. Die Seite **Zusammenfassung** wird laufend aktualisiert, damit die angezeigten Übersichtsinformationen stets auf dem neuesten Stand sind. Die Seite **Zusammenfassung** enthält folgende Informationen:

- **Systemstatus**

  Auf der Seite **Systemstatus** wird der Status der aktuell ausgeführten Services und Aufgaben angezeigt. Die Seiten für die einzelnen Services können Sie anzeigen, indem Sie im Fensterbereich **Systemstatus** auf den Namen des Services klicken.
- **Jobzusammenfassung**

  Im Fensterbereich **Jobzusammenfassung** wird eine Übersicht über die aktuellen Jobs angezeigt.
- **Bestandszusammenfassung**

  Im Fensterbereich **Bestandszusammenfassung** wird eine Übersicht über die erkannten Bestände angezeigt.
- **Produktinformationen**

  Im Fensterbereich **Produktinformation** werden der Hostname und die ID der TSA angezeigt.

Aktivitätenprotokoll anzeigen

Im Aktivitätenprotokoll werden Protokollnachrichten im Zusammenhang mit den Erkennungs- und Übertragungsprozessen angezeigt. Durch Klicken auf einen Eintrag im Aktivitätenprotokoll können Sie weitere Informationen dazu anzeigen.

Sie können das Aktivitätenprotokoll anzeigen, indem Sie im Navigationsbereich auf **Aktivitätenprotokoll** klicken. Eine Liste mit Protokolleinträgen wird angezeigt. Für jeden Eintrag ist die Nachricht, der Schweregrad und der Zeitpunkt der Aktivität aufgeführt.

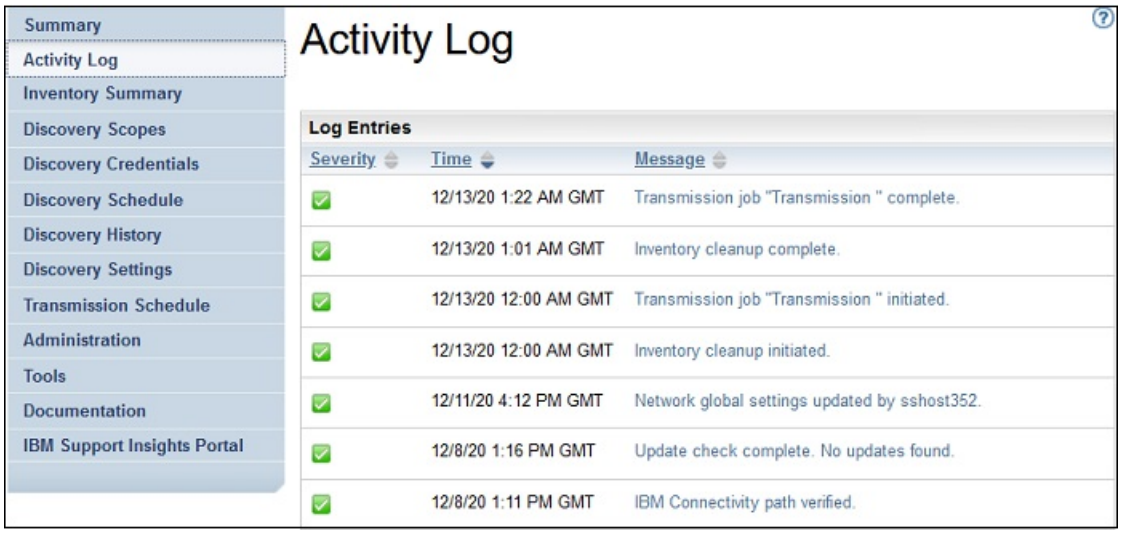

Abbildung 81. Aktivitätenprotokoll

Anmerkung: Da Erkennungsvorgänge jeweils an einer einzelnen Bereichsgruppe ausgeführt werden, können bei einer vollständigen Erkennung mehrere Protokolleinträge vorhanden sein.

Um nähere Einzelheiten zu einem Eintrag im Aktivitätenprotokoll anzuzeigen, klicken Sie auf die Nachricht in diesem Eintrag.

Um die Protokolldateien auf Ihrem Computer zu speichern, klicken Sie auf **Alle Protokolle herunterladen**.

Um das Protokoll zu löschen, klicken Sie auf **Protokoll löschen**.

Bestandsbereinigungsarchiv anzeigen

Sie können die Bestände anzeigen, die nach Ablauf der im **Zeitplan für Bestandsbereinigung** festgelegten Aufbewahrungsdauer bereinigt wurden.

Informationen zu diesem Vorgang

Führen Sie zum Anzeigen der gelöschten Bestände die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie auf der Seite **Zeitplan für Bestandsbereinigung** auf **Bereinigungsarchiv anzeigen**. Die Seite **Bestandsbereinigungsarchiv** wird angezeigt.

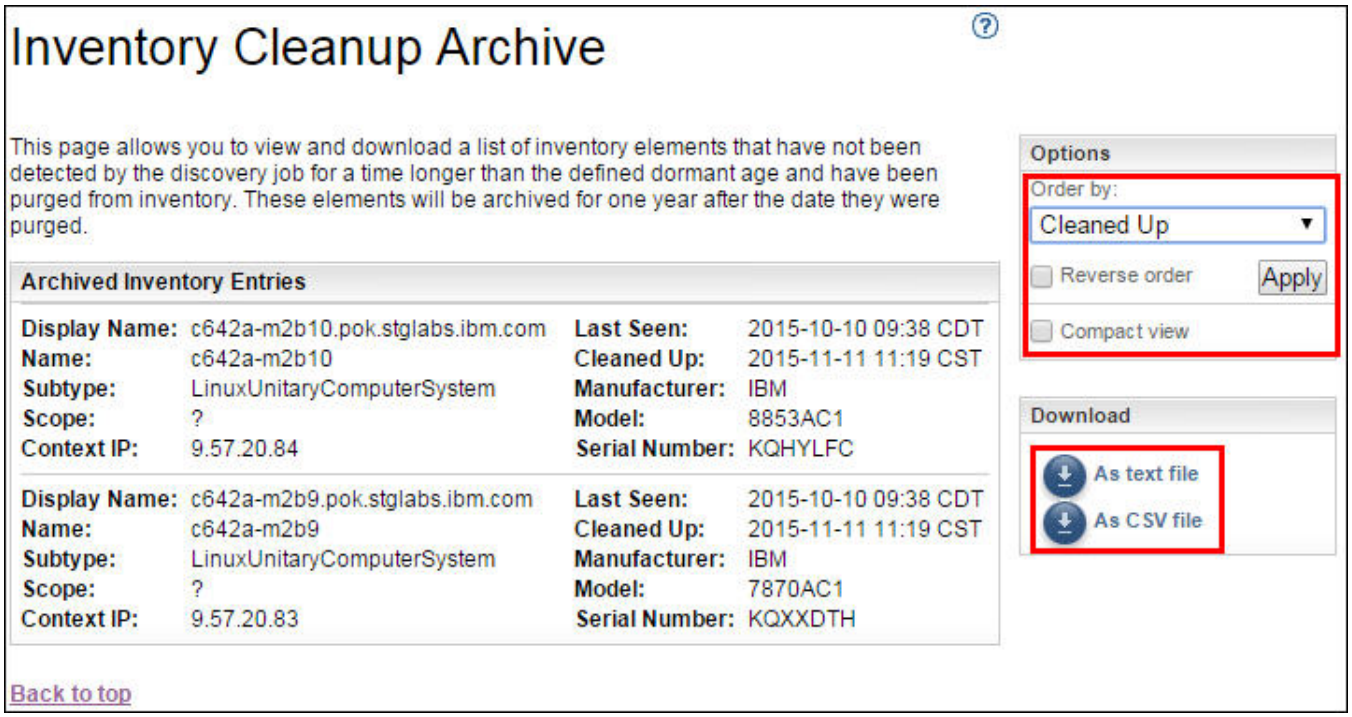

Abbildung 82. Bestandsbereinigungsarchiv

2. Auf der Seite **Bestandsbereinigungsarchiv** können Sie nachsehen, welche Elemente im Rahmen von Bereinigungsprozessen aus dem Bestand gelöscht wurden.

   Anmerkung:

   - Die Bestandsinformationen in diesem Archiv bleiben nur ein Jahr lang verfügbar. Nach einem Jahr werden die Archivinformationen gelöscht.
   - Das Archiv ist leer (keine bereinigten Objekte), wenn alle definierten Ziele innerhalb des letzten Jahres aktiv erkannt wurden.

3. Im Fensterbereich **Optionen** können Sie die Reihenfolge der Bestandsdetails ändern.

a) Wählen Sie unter **Reihenfolge nach** im Fensterbereich **Optionen** eine Eigenschaft aus und klicken Sie auf **Anwenden** um die Ansicht der Bestandsdetails dementsprechend anzuordnen.

b) Aktivieren Sie die Option **Reihenfolge umkehren**, um die Details in der umgekehrten Reihenfolge der ausgewählten Eigenschaft anzuzeigen.

c) Aktivieren Sie die Option **Kompaktansicht**, um eine Zusammenfassung der Bestände anzuzeigen.

4. Klicken Sie zum Herunterladen der Bestandsdetails auf **Als Textdatei** oder auf **Als CSV-Datei**. Speichern Sie die Bestandsdetails, wenn Sie die Daten lokal bearbeiten und/oder für einen längeren Zeitraum (mehr als ein Jahr) auf Ihrem Computer behalten möchten. Im Archiv gespeicherte Daten werden nach einem Jahr gelöscht.

Kennwörter

Zum Schutz der TSA-Benutzerkonten werden Kennwörter verwendet.

Kennwort ändern

Vorgehensweise zum Ändern des TSA-Benutzerkennworts.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Kennwort**.
   Die Seite **Kennwort** wird angezeigt.
2. Geben Sie im Feld **Aktuelles Kennwort** Ihr derzeitiges Kennwort ein.
3. Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.

   Das Kennwort muss folgenden Regeln entsprechen:

   - Es muss mindestens 8 Zeichen lang sein.
   - Es muss mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthalten.
   - Der Benutzername darf nicht enthalten sein.
   - Es darf nicht mit einem der acht vorherigen Kennwörter identisch sein.
   - Es muss mindestens alle 90 Tage (Standard) geändert werden, jedoch nicht öfter als einmal pro Tag.
4. Geben Sie im Feld **Kennwort bestätigen** das neue Kennwort erneut ein.
   Bevor das Kennwort gespeichert wird, werden die beiden von Ihnen eingegebenen Kennwörter verglichen, um zu bestätigen, dass sie übereinstimmen.
5. Klicken Sie auf **Speichern**.

Nächste Schritte

Wichtig: Es ist nicht möglich, ein Kennwort wiederzuerlangen. Falls Sie Ihr Kennwort verlieren oder vergessen, können Sie sich nicht mehr in der TSA anmelden, um das Kennwort zu ändern. Bei Verlust des Kennworts für ein Benutzerkonto oder Administratorkonto (falls mehrere Konten vorhanden sind) wenden Sie sich bitte an Ihren TSA-Administrator. Bei Verlust des Kennworts für das Standardadministratorkonto (Werkseinstellung der TSA) rufen Sie den IBM Support an.Weitere Informationen hierzu finden Sie im Abschnitt „Bei der Technical Support Appliance anmelden” auf Seite 21.

Sicherheit

Sie können Sicherheitsfunktionen und Dienstprogramme für die TSA aufrufen und ändern.

Die verfügbaren Sicherheitsdienstprogramme werden auf der Seite **Sicherheit** aufgelistet. Auf dieser Seite können Sie die Einstellungen für das Sitzungszeitlimit ändern oder die maximale Kennwortgültigkeitsdauer für alle Benutzerkonten ändern.

Einstellungen für das Sitzungszeitlimit ändern

Aus Sicherheitsgründen wird der Benutzer nach einer gewissen Zeit der Inaktivität von der TSA abgemeldet. Sie können die automatische Benutzerabmeldung durch die TSA verhindern oder die Zeitdauer ändern, nach der die Benutzerabmeldung erfolgt.

Sitzungszeitlimit inaktivieren

Sie können die automatische Abmeldung des Benutzers von der TSA verhindern, indem Sie das Sitzungszeitlimit inaktivieren.

Vorgehensweise

1. Aktivieren Sie das Kontrollkästchen **Sitzungszeitlimit inaktivieren**.
2. Klicken Sie auf **Einstellungen für Sitzungszeitlimit ändern**.

Sitzungszeitlimitwert ändern

Standardmäßig wird der Benutzer nach 20 Minuten Inaktivität abgemeldet. Sie können die Zeitdauer bis zur Abmeldung des Benutzers verlängern, indem Sie den Sitzungszeitlimitwert ändern.

Vorgehensweise

1. Inaktivieren Sie das Kontrollkästchen **Sitzungszeitlimit inaktivieren**.
2. Geben Sie im Feld **Sitzungszeitlimit** die Zeitdauer in Sekunden an, bevor der Benutzer von der TSA abgemeldet wird.

   Anmerkung: Der Sitzungszeitlimitwert darf nicht kleiner als 20 Minuten sein.
3. Klicken Sie auf **Einstellungen für Sitzungszeitlimit ändern**.

Gültigkeitsdauer des Kennworts ändern

Als Sicherheitsmaßnahme müssen alle Benutzer ihr TSA-Anmeldekennwort nach einer bestimmten Anzahl von Tagen ändern. Standardmäßig ist die maximale Gültigkeitsdauer für ein Kennwort 90 Tage, Sie können jedoch die Gültigkeitsdauer stattdessen auch auf 30 oder 60 Tage festlegen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Sicherheit**. Die Seite **Sicherheit** wird angezeigt.
2. Blättern Sie auf der Seite **Sicherheit** abwärts bis zum Fensterbereich **Maximale Gültigkeitsdauer des Kennworts**.
3. Wählen Sie im Fensterbereich **Maximale Gültigkeitsdauer des Kennworts** die gewünschte Gültigkeitsdauer (30 Tage, 60 Tage oder 90 Tage) aus der Dropdown-Liste **Maximale Gültigkeitsdauer** aus.
4. Klicken Sie auf **Maximale Gültigkeitsdauer des Kennworts ändern**, um die Einstellung zu aktualisieren. Die Bestätigungsnachricht *Maximale Gültigkeitsdauer des Kennworts wurde aktualisiert* wird angezeigt.

Sicherung und Wiederherstellung

Sie können die TSA-Konfiguration sichern und wiederherstellen.

Wichtig: Es wird dringend empfohlen, regelmäßig eine Sicherung durchzuführen. Außerdem sollte eine Sicherung durchgeführt werden, nachdem Änderungen an Bereichsgruppen oder Berechtigungsnachweisen vorgenommen wurden.

Sicherungszeitpunkt

Zeigt das Datum und die Uhrzeit an, zu der die neueste Sicherung erfolgte.

Konfigurationszusammenfassung

Verwenden Sie diese Option, um eine Übersicht über die aktuelle TSA-Konfiguration anzuzeigen, bevor Sie sie speichern.

Führen Sie zum Anzeigen der TSA-Konfigurationszusammenfassung die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Sicherung und Wiederherstellung**. Die Seite **Sicherung und Wiederherstellung** wird angezeigt.
2. Klicken Sie auf **Zusammenfassung anzeigen**, um eine Zusammenfassung der aktuellen TSA-Konfiguration anzuzeigen. Daraufhin werden die Konfigurationseinstellungen angezeigt, die bei einer Sicherung der TSA gespeichert werden.

   Anmerkung: Die Informationen werden in einem Popup-Fenster angezeigt. Falls Ihr Web-Browser Popup-Fenster blockiert, müssen Sie zunächst die Anzeige von Popup-Fenstern der TSA in Ihrem Browser zulassen.

   Auf der Seite **Zusammenfassung** werden im Abschnitt **Sicherung** die Informationen zum Sicherungsstatus mit folgenden Hinweisen angezeigt:

   - Das Symbol *OK* (), wenn die letzte Sicherung innerhalb der letzten 60 Tage vorgenommen wurde.
   - Das Symbol *Warnung* (), wenn die letzte Sicherung mehr als 60 Tage, aber höchstens 90 Tage zurückliegt.
   - Das Symbol *Fehler* (), wenn länger als 90 Tage keine Sicherung durchgeführt wurde.

Sicherung

Verwenden Sie diese Option, um eine Kopie der TSA-Konfiguration zu sichern.

Führen Sie zum Sichern der TSA-Konfiguration die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Sicherung und Wiederherstellung**. Die Seite **Sicherung und Wiederherstellung** wird angezeigt.

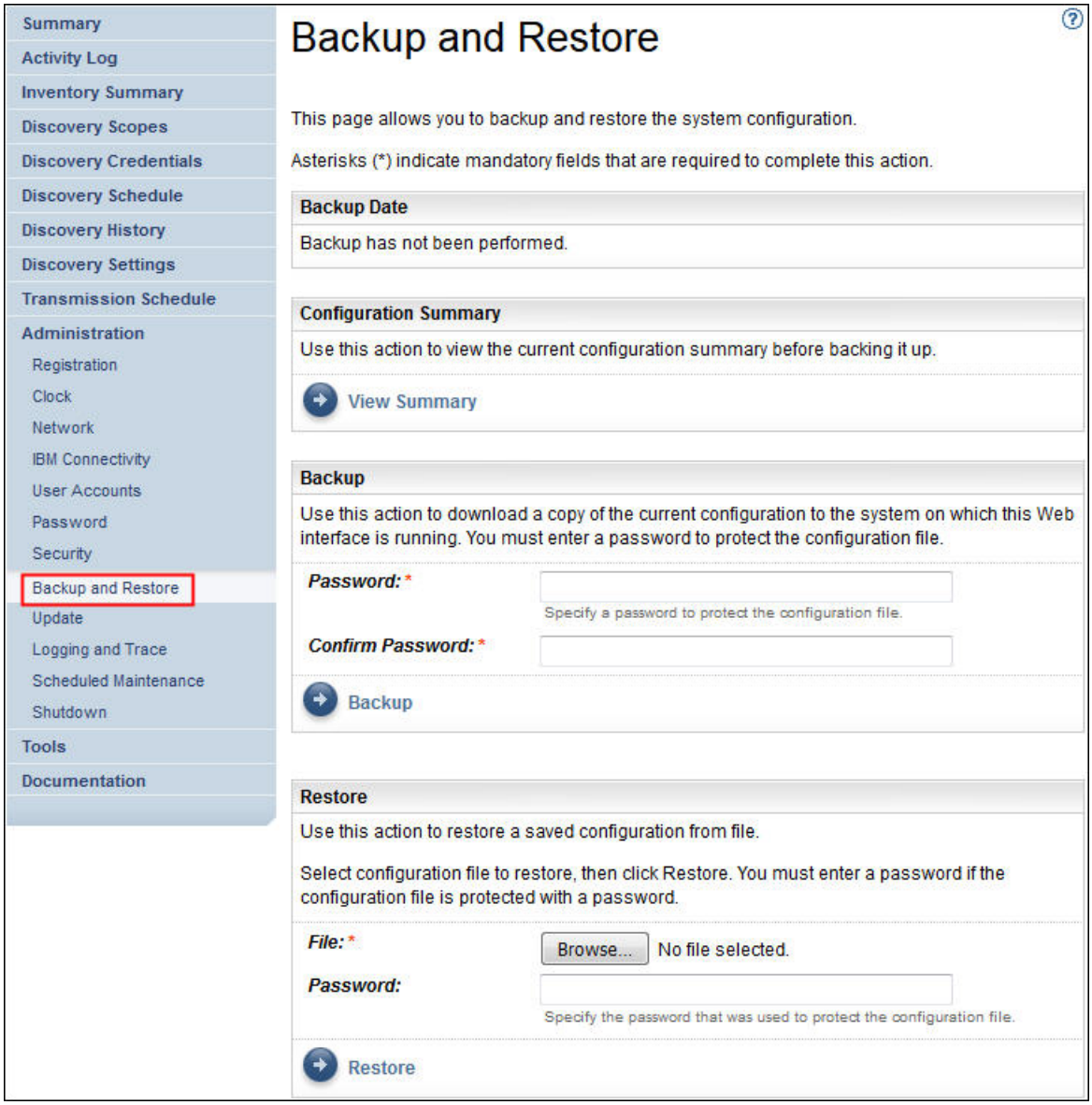

Abbildung 83. Sicherung und Wiederherstellung

2. Geben Sie im Fenster **Sicherung** zum Schutz der Konfigurationsdatei ein Kennwort ein.
3. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein. Bevor das Kennwort gespeichert wird, werden die beiden von Ihnen eingegebenen Kennwörter verglichen, um zu bestätigen, dass sie übereinstimmen.

   Anmerkung: Bewahren Sie das Kennwort sicher auf, da Sie es beim Wiederherstellungsvorgang benötigen.
4. Klicken Sie auf **Sicherung** und speichern Sie die Backup-Konfigurationsdatei komprimiert auf dem System.

   Anmerkung: Die erzeugte Backup-Konfigurationsdatei kann nur von der TSA geöffnet werden.

   Anmerkung: Falls Sie Ihr Administratorkennwort kürzlich geändert haben, erstellen Sie nach der Kennwortänderung eine Sicherung und verwenden Sie zur Wiederherstellung die neueste Sicherungsdatei.

Wiederherstellung

Verwenden Sie diese Option, um eine zuvor gespeicherte Kopie der Konfiguration wiederherzustellen.

Führen Sie zum Wiederherstellen der TSA-Konfiguration die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Sicherung und Wiederherstellung**. Die Seite **Sicherung und Wiederherstellung** wird angezeigt.
2. Klicken Sie auf **Datei auswählen**, um die wiederherzustellende Konfigurationsdatei zu suchen und auszuwählen.
3. Geben Sie das Kennwort ein, das beim Sichern der Konfigurationsdatei verwendet wurde.
4. Klicken Sie auf **Wiederherstellen**.

   Der Wiederherstellungsjob wird im Fensterbereich "Jobzusammenfassung" der Seite **Zusammenfassung** angezeigt. Nach Abschluss der Wiederherstellung werden Sie aufgefordert, das System neu zu starten.

   Anmerkung: Durch das Wiederherstellen einer Sicherung wird die vorhandene Konfiguration gelöscht. Alle Konfigurationseinstellungen einschließlich Bereichsdefinitionen und Berechtigungsnachweisen werden durch diejenigen aus der Sicherungsdatei ersetzt.

Anmerkung: Vergewissern Sie sich bei Sicherungs- und Wiederherstellungsoperationen, dass der Discovery Manager-Status auf der Seite **Zusammenfassung** als "OK" (✅) angezeigt wird. Falls Discovery Manager inaktiv ist, erhalten Sie eine Meldung wie: "`Discovery Manager wird nicht ausgeführt. Bevor Sie die Aktivität fortsetzen, warten Sie ab, bis der Discovery Manager-Status in der Anzeige 'Zusammenfassung' mit einem grünen Häkchen dargestellt wird (normalerweise bis zu 10 Minuten).`" Wenn Discovery Manager nach 10 Minuten noch nicht ausgeführt wird, wenden Sie sich bitte an den IBM Support.

Update

Sie können Updates für die TSA suchen und herunterladen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Update**.
   Die Seite **Update** wird angezeigt.

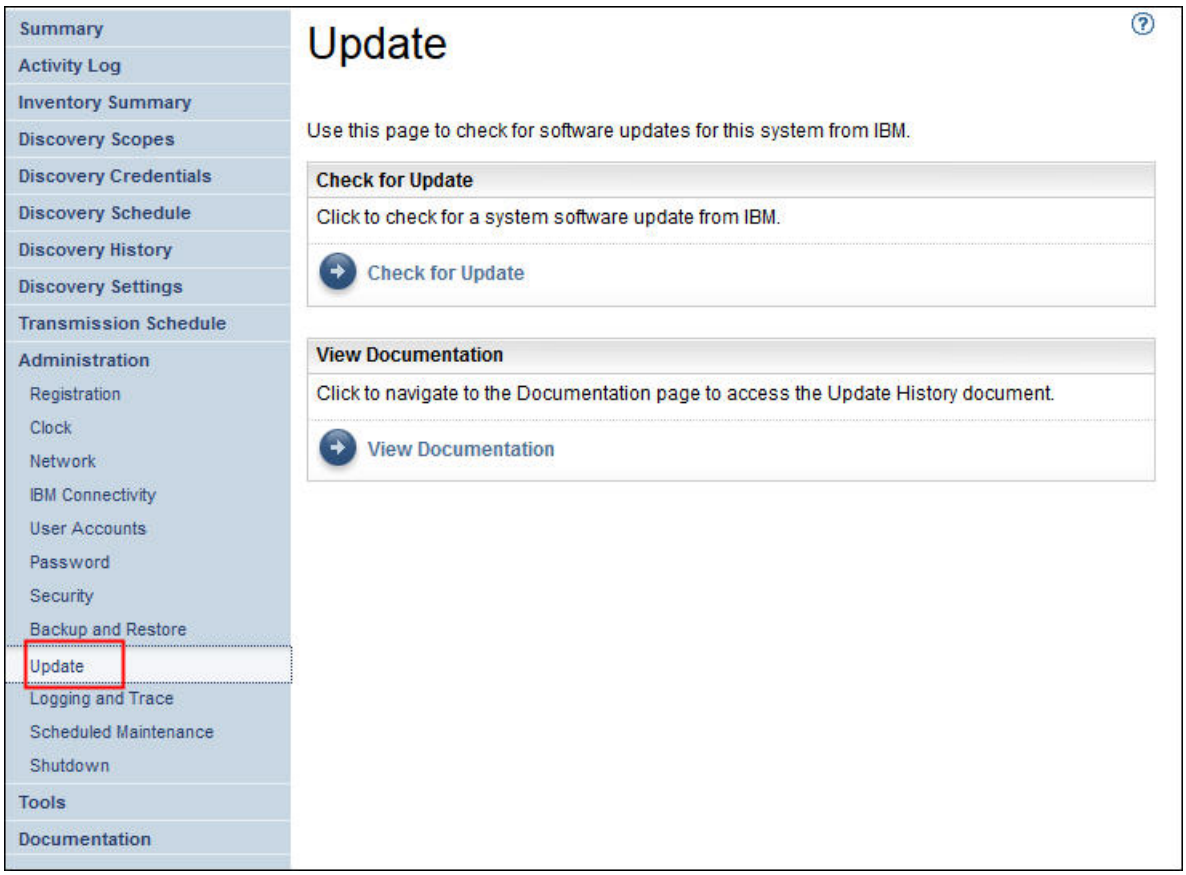

Abbildung 84. Update

2. Klicken Sie auf **Auf Update prüfen**.
   Auf der Seite **Updateverfügbarkeit** werden alle verfügbaren Updates aufgelistet.

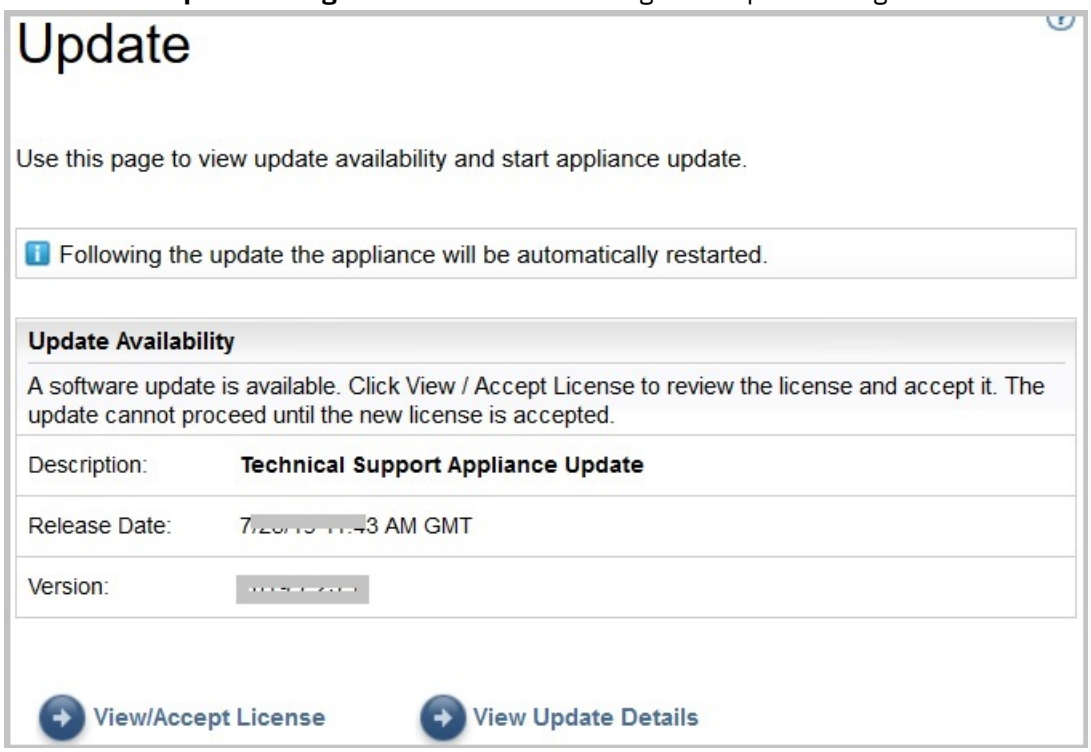

Abbildung 85. Updateverfügbarkeit

a) Bei manchen neuen Releases der TSA müssen Sie eine neue Lizenzvereinbarung akzeptieren, bevor Sie mit der Aktualisierung fortfahren können. Falls eine neue Lizenzvereinbarung vorliegt, klicken Sie auf die Schaltfläche **Lizenz anzeigen/akzeptieren**. Die Seite **Lizenzvereinbarung** wird angezeigt.

b) Klicken Sie auf die Schaltfläche **Akzeptieren** auf der Seite **Lizenzvereinbarung**, um die neue Lizenzvereinbarung zu akzeptieren. Daraufhin wird die Seite **Update** nun mit der Schaltfläche **Update jetzt ausführen** angezeigt. Falls keine neue Lizenzvereinbarung akzeptiert werden muss, erscheint die Schaltfläche **Lizenz anzeigen/akzeptieren** nicht, sondern Sie können direkt auf **Update jetzt ausführen** klicken.

Anmerkung:

- Nachdem Sie die Lizenz akzeptiert haben, wird die Schaltfläche **Lizenz anzeigen/akzeptieren** nicht mehr angezeigt.
- Klicken Sie im Navigationsfenster auf **Verwaltung** > **Lizenz**, um die aktuelle Lizenzvereinbarung, die Sie akzeptiert haben, anzusehen.

c) Klicken Sie zum Installieren des Updates auf **Update jetzt ausführen**.

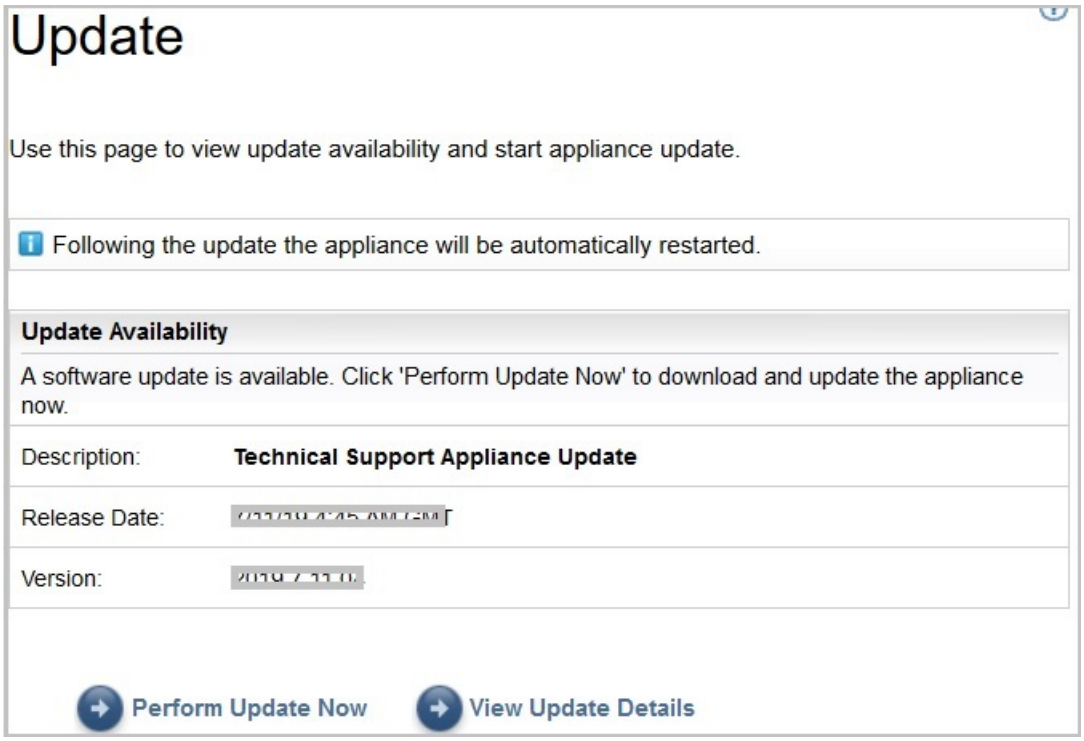

Abbildung 86. Update jetzt ausführen

Nach Abschluss der Aktualisierung wird die TSA automatisch neu gestartet.

d) Um Informationen zu den Inhalten des Updates anzuzeigen, klicken Sie auf **Updatedetails anzeigen**.

Planmäßige Wartung aktivieren

Damit die TSA dauerhaft mit optimaler Leistung arbeitet, empfehlen wir, die Funktion zur planmäßigen Wartung zu aktivieren.

Informationen zu diesem Vorgang

Durch planmäßige Wartung wird die optimale Leistung der TSA gesichert. Sie können diese Funktion jederzeit aktivieren oder inaktivieren. Wenn Sie die planmäßige Wartung aktivieren, können Sie den Tag und

die Uhrzeit für die automatische Ausführung der Wartung festlegen. Der Status der planmäßigen Wartung wird im Abschnitt **Systemstatus** der Seite **Zusammenfassung** angezeigt.

Nach der Ausführung eines planmäßigen Wartungsjobs wird das System automatisch neu gestartet und Sie erhalten eine Stunde vorher eine Nachricht über den Neustart des Systems, z. B. `Ein Systemneustart im Rahmen der planmäßigen Wartung erfolgt in 59 Minute(n).`

Wichtig: Planen Sie die Appliance-Wartung nicht mit weniger als 30 Minuten Abstand zu anderen geplanten Jobs wie Erkennung, Übertragung oder Bestandsbereinigung. Bei weniger als 30 Minuten Abstand zu anderen geplanten Jobs können diese Jobs nicht ausgeführt werden.

Vorgehensweise

Führen Sie zum Bearbeiten der Wartungsplanung die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Planmäßige Wartung**.

   Auf der Seite **Planmäßige Wartung** werden im Bereich **Zeitplan** die nächste geplante Ausführung und der definierte Ausführungszeitpunkt angezeigt. Im Abschnitt **Verlauf** sind der Status und weitere Details des aktuell ausgeführten und der vorherigen Übertragungsjobs aufgeführt.
2. Klicken Sie auf der Seite **Planmäßige Wartung** auf **Zeitplan bearbeiten**.
   a) Im Fensterbereich **Zeitplan aktivieren** können Sie die planmäßige Wartung aktivieren oder inaktivieren.
   b) Wenn Sie die planmäßige Wartung aktivieren, wählen Sie mithilfe der Dropdown-Listen **Stunde** und **Minute** einen neuen Zeitpunkt aus.
   c) Legen Sie den **Tagauswahlmodus** fest. Um die Wartung für bestimmte Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus. Um die Wartung für einen bestimmten Tag im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.
   d) Aktivieren Sie die jeweiligen Kontrollkästchen im Feld **Tage**, um andere oder zusätzliche Tage in der Woche oder im Monat auszuwählen.

      Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.
3. Klicken Sie auf **Speichern**.

   Die Seite **Planmäßige Wartung** wird mit dem neuen Zeitplan angezeigt.

Protokollierung und Trace

Sie können die TSA-Diagnosetrace-Einstellungen anzeigen und ändern. Außerdem können Sie die Einstellungen für die Discovery Manager-Tracestufen ändern. Da Änderungen an diesen Einstellungen das Leistungsverhalten beeinflussen können, sollten Sie solche Änderungen nur auf Anweisung durch den IBM Support vornehmen.

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Protokollierung und Trace**. Die Seite **Protokollierung und Trace** wird angezeigt. Im Abschnitt **Tracestufe für TSA** sind die aktuellen Traceeinstellungen (Fehler, Warnung, Information, Debug oder Trace) aufgeführt.

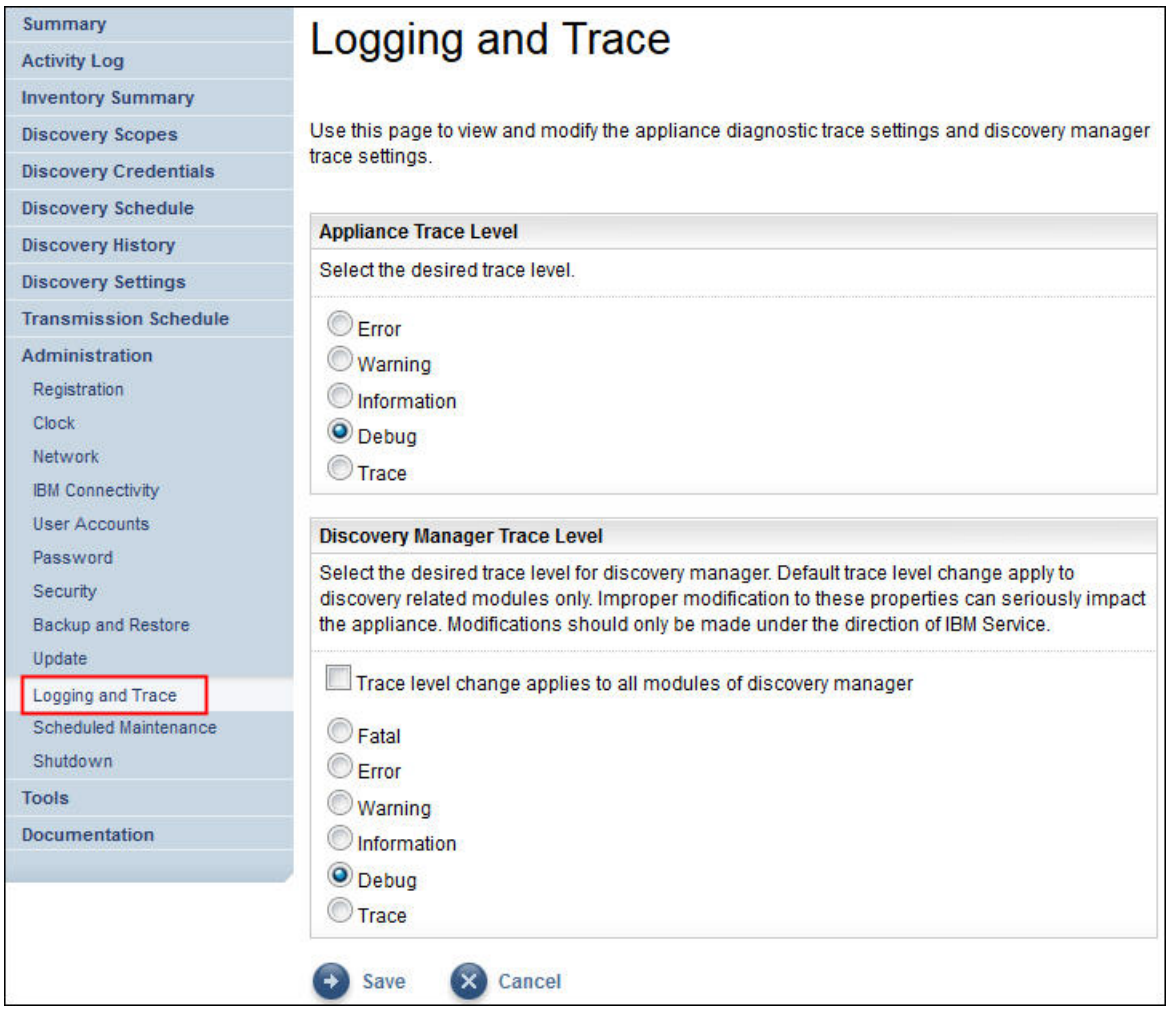

Abbildung 87. Protokollierung und Trace

2. Falls erforderlich, können Sie die Traceeinstellung im Fensterbereich **TSA-Tracestufe** ändern, indem Sie auf das Optionsfeld neben der gewünschten Tracestufe klicken.
3. Klicken Sie auf **Speichern**.

Anmerkung: Standardmäßig ist für die Fensterbereiche *TSA-Tracestufe* und *Discovery Manager-Tracestufe* die Stufe **Debug** festgelegt.

Die Einstellungen für die **Discovery Manager-Tracestufe** können Sie mit folgenden Schritten anzeigen und ändern:

Wichtig: Nehmen Sie Änderungen in diesem Abschnitt nur auf Anweisung durch den IBM Service vor.

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Protokollierung und Trace**. Die Seite **Protokollierung und Trace** wird geöffnet und zeigt die aktuelle Traceeinstellung an.
2. Aktivieren Sie die Option **Änderung der Tracestufe gilt für alle Module von Discovery Manager**, wenn die Tracestufe auf alle Discovery Manager-Module angewendet werden soll.
3. Klicken Sie auf das Optionsfeld neben der gewünschten Traceeinstellung.
4. Klicken Sie auf **Speichern**.

Herunterfahren

Sie können Operationen der TSA aussetzen und wiederaufnehmen sowie die TSA herunterfahren und erneut starten oder ausschalten.

Das Herunterfahren kann mehrere Minuten dauern.

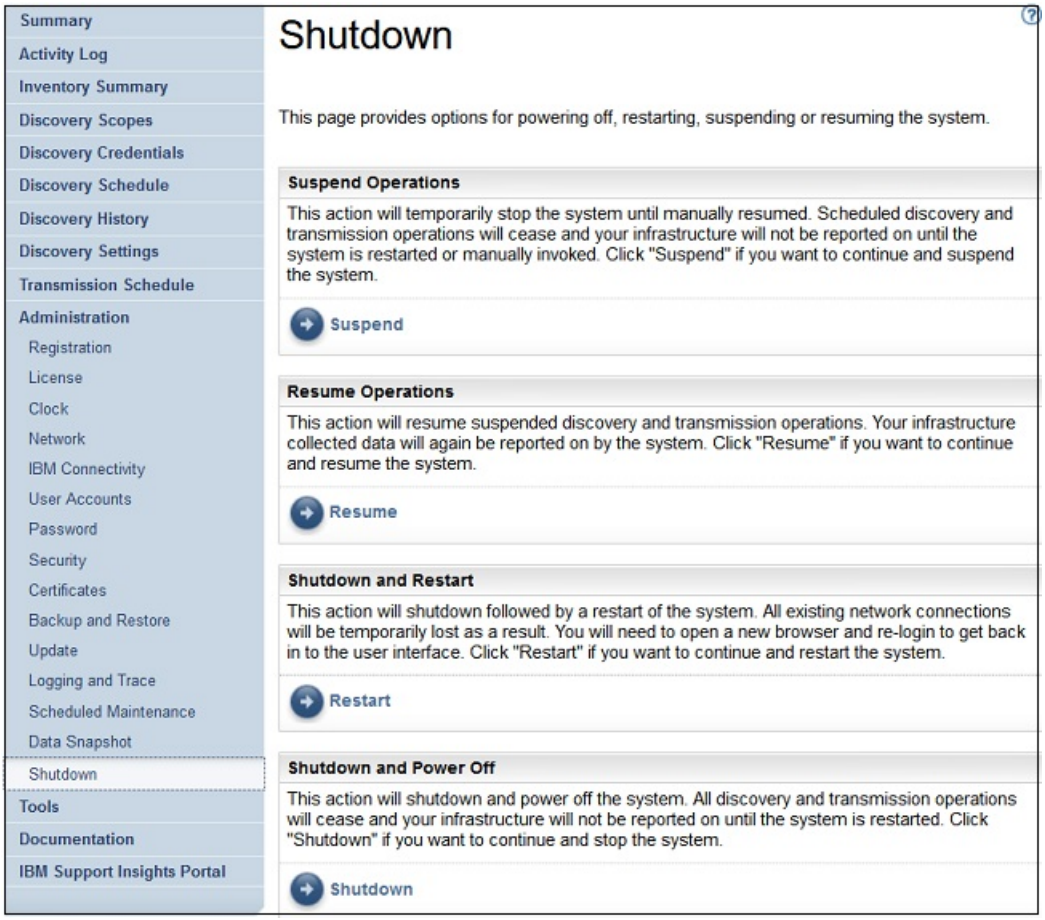

Abbildung 88. Herunterfahren

Betrieb aussetzen

Durch diese Aktion wird die TSA temporär angehalten. Alle Erkennungs- und Übertragungsoperationen werden gestoppt, und es werden keine Informationen an IBM übermittelt, bis der Betrieb wieder fortgesetzt wird.

Führen Sie zum Aussetzen der TSA-Operationen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Herunterfahren**. Die Seite **Herunterfahren** wird angezeigt.
2. Klicken Sie auf **Aussetzen**.

   Anmerkung: Sie können den Status von TSA in der **Übersichtsseite** überprüfen. Wenn TSA den Status "Ausgesetzt" aufweist, wird im Fensterbereich **Systemstatus** angezeigt, dass TSA ausgesetzt wurde.

Betrieb fortsetzen

Durch diese Aktion wird der Betrieb der temporär angehaltenen TSA wiederaufgenommen. Alle Erkennungs- und Übertragungsoperationen werden fortgesetzt, und die Informationen werden wie geplant an IBM übermittelt.

Führen Sie zum Fortsetzen der TSA-Operationen die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Herunterfahren**. Die Seite **Herunterfahren** wird angezeigt.
2. Klicken Sie auf **Fortsetzen**.

Herunterfahren und erneut starten

Durch diese Aktion wird die TSA heruntergefahren und erneut gestartet. Alle bestehenden Netzverbindungen werden unterbrochen. Nach dem Neustart müssen Sie einen Browser starten und sich erneut anmelden.

Führen Sie zum Herunterfahren und erneuten Starten der TSA die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Herunterfahren**. Die Seite **Herunterfahren** wird angezeigt.
2. Klicken Sie auf **Erneut starten**.

Herunterfahren und Ausschalten

Durch diese Aktion wird die TSA heruntergefahren und ausgeschaltet. Alle Erkennungs- und Übertragungsoperationen werden eingestellt, und es wird kein Infrastruktur-Reporting mehr durchgeführt, bis das System wieder gestartet wird.

Führen Sie zum Herunterfahren und Ausschalten der TSA die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Herunterfahren**. Die Seite **Herunterfahren** wird angezeigt.
2. Klicken Sie auf **Herunterfahren**.

Anmerkung: Nachdem die TSA heruntergefahren wurde, müssen Sie sie über die VMware ESXi-Webschnittstelle oder den Hyper-V Manager wieder einschalten.

Tools

Die TSA verfügt über Tools, die Ihnen das Einrichten der TSA-Umgebung erleichtern.

Klicken Sie zum Aufrufen dieser Tools im Navigationsbereich auf **Tools**.

Netztools

Die Seite **Netztools** beinhaltet Diagnosetools und Informationen zu den von der TSA verwendeten Netzprotokollen.

Zum Aufrufen der Diagnosetools klicken Sie im Navigationsbereich auf **Tools** > **Netztools**. Die Seite **Netztools** wird angezeigt.

Die Seite "Netztools" besteht aus mehreren Registerkarten. Durch Klicken auf eine Registerkarte wird die entsprechende Seite angezeigt.

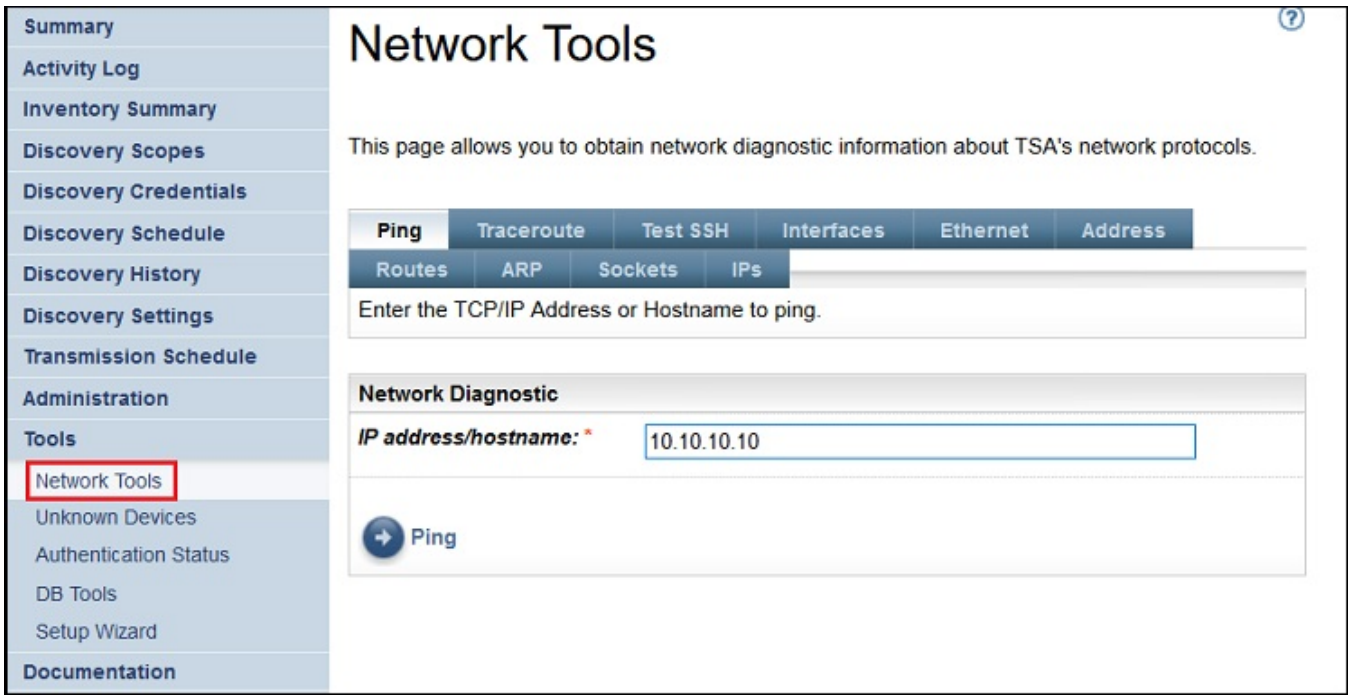

Abbildung 89. Netztools

Ping
Verwenden Sie diese Seite zum Senden einer Echoanforderung an einen Remote-Host, um zu überprüfen, ob der Host erreichbar ist. Auf dieser Seite finden Sie auch den Hostnamen bzw. die TCP/IP-Adresse.

Traceroute
Verwenden Sie diese Seite, um den Pfad anzuzeigen, über den Pakete an einen Remote Host gesendet werden.

SSH testen
Auf dieser Seite können Sie testen, ob ein Remote Host per SSH mit den Erkennungsberechtigungsnachweisen, die für diesen Host definiert sind, aufrufbar ist.

Schnittstellen
Verwenden Sie diese Seite, um Statistikdaten zu den aktuell konfigurierten Netzschnittstellen anzuzeigen.

Ethernet
Verwenden Sie diese Seite, um die Einstellungen zu den aktuell konfigurierten Ethernet-Karten anzuzeigen.

Adresse
Verwenden Sie diese Seite, um die IP-Adressen für die aktuell konfigurierten Netzschnittstellen anzuzeigen.

Routen
Verwenden Sie diese Seite, um die Kernel-IP-Routingtabellen und entsprechenden Netzschnittstellen anzuzeigen.

ARP
Verwenden Sie diese Seite, um die Inhalte der ARP-Verbindungen (Address Resolution Protocol) anzuzeigen.

Sockets
Verwenden Sie diese Seite, um Informationen zu TCP/IP-Sockets anzuzeigen.

IPs
Verwenden Sie diese Seite, um Informationen zu den IP-Paketfilterregeln anzuzeigen.

Anmerkung: Der eingegebene Hostname darf keinen Unterstrich ("_") enthalten.

Datenbanktools

Auf der Seite **Datenbanktools** lassen sich verschiedene Datenpflegeoperationen ausführen. Es wird jedoch empfohlen, diese Funktionen nur auf Anweisung durch den IBM Support zu verwenden.

Sie können folgende Operationen an der Datenbank ausführen:

Bestandsdatenbank erneut erstellen

Wenn Sie die Bestandsdatenbank erneut erstellen, gehen sämtliche Bestandsdaten verloren. Falls das Kontrollkästchen **Berechtigungsnachweise beibehalten** inaktiviert oder Discovery Manager nicht verfügbar ist, werden die Berechtigungsnachweise ebenfalls gelöscht.

Führen Sie zur Neuerstellung der Datenbank die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Tools** > **DB-Tools**.
2. Aktivieren Sie das Kontrollkästchen **Berechtigungsnachweise und Bereiche beibehalten** im Abschnitt **Bestandsdatenbank erneut erstellen**, um alle Erkennungsberechtigungsnachweise zu behalten. Wenn Sie **Berechtigungsnachweise und Bereiche beibehalten** nicht auswählen, werden alle Berechtigungsnachweise und Bereiche gelöscht und müssen neu erstellt werden. Weitere Informationen zu Erkennungsberechtigungsnachweisen finden Sie im Abschnitt „Erkennungsberechtigungsnachweise” auf Seite 76.

   Anmerkung: Die Berechtigungsnachweise und Bereiche können nur beibehalten werden, wenn Discovery Manager ausgeführt wird (Status "grün").
3. Klicken Sie auf **Bestandsdatenbank erneut erstellen**. Daraufhin wird der folgende Warnhinweis angezeigt: `Taking this action will temporarily shutdown the Discovery Manager. Are you sure you want to recreate the inventory database?`
4. Klicken Sie auf **OK**, um die Bestandsdatenbank erneut zu erstellen. Die folgende Nachricht wird angezeigt: `Recreate Database Started`. Die Neuerstellung der Datenbank kann ungefähr 6 Stunden lang dauern. In der Zwischenzeit wird auf der Seite "Zusammenfassung" die folgende Nachricht angezeigt: `dbinit starting`. Überprüfen Sie nach 6 Stunden, ob im **Aktivitätenprotokoll** der Status `Neuerstellung der Bestandsdatenbank erfolgreich` angezeigt wird.

   Anmerkung: Während der Neuerstellung der Bestandsdatenbank wird Discovery Manager vorübergehend heruntergefahren und das *Bestandsbereinigungsarchiv* wird gelöscht.

RUNSTATS ausführen

Führen Sie zum Ausführen des Befehls **RUNSTATS** die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Tools** > **DB-Tools**.
2. Klicken Sie auf **RUNSTATS ausführen**. Daraufhin wird der folgende Warnhinweis angezeigt: `Are you sure you want to perform RUNSTATS on the inventory database tables?`
3. Klicken Sie auf **OK**. Die folgende Nachricht wird angezeigt: `RUNSTATS Started`. Überprüfen Sie nach 30 Minuten das Aktivitätenprotokoll. Wenn der Job abgeschlossen ist, wird die folgende Nachricht dem Aktivitätenprotokoll hinzugefügt: `RUNSTATS für Bestandsdatenbank erfolgreich`.

REORG ausführen

Führen Sie zum Ausführen des Befehls **REORG** die folgenden Schritte durch:

1. Klicken Sie im Navigationsbereich auf **Tools** > **DB-Tools**.
2. Klicken Sie auf **REORG ausführen**. Daraufhin wird der folgende Warnhinweis angezeigt: `Are you sure you want to perform REORG on the inventory database tables?`
3. Klicken Sie auf **OK**. Die folgende Nachricht wird dem Aktivitätenprotokoll hinzugefügt: `REORG Started`. Überprüfen Sie nach 30 Minuten das Aktivitätenprotokoll. Wenn der Job abgeschlossen ist, wird die folgende Nachricht dem Aktivitätenprotokoll hinzugefügt: `REORG für Bestandsdatenbank erfolgreich`.

Dokumentation

Auf der Seite **Dokumentation** finden Sie hilfreiche Informationen zu den ersten Schritten mit der IBM Technical Support Appliance. Sie können auf Installationshandbücher und sicherheitsspezifische Dokumentation zugreifen, Beispielberichte anzeigen und den TSA-Installationscode von der TSA-Website unter https://ibm.biz/TSAdemo herunterladen.

Vorgehensweise

Führen Sie zum Anzeigen der Dokumentation und Kennenlernen der Technical Support Appliance die folgenden Schritte durch:

1. Klicken Sie im Navigationsmenü auf der linken Seite auf **Dokumentation**.

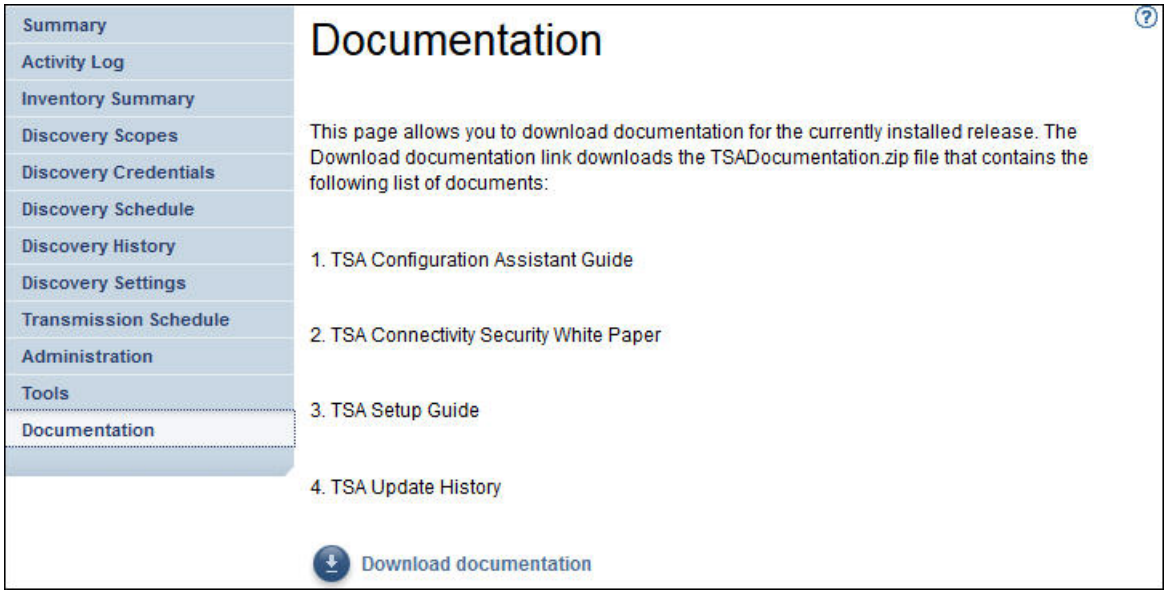

Abbildung 90. Dokumentation

2. Weitere Informationen zur Technical Support Appliance finden Sie durch Klicken auf den folgenden Link: https://ibm.biz/TSAdemo
3. Auf der Seite **TSA installieren** finden Sie weitere Links zum TSA-Image, Installationshandbuch, Konfigurationshandbuch und zu den zugehörigen Lernprogrammen.

Kapitel 7. IBM Support für die Technical Support Appliance (TSA) kontaktieren

Der IBM Support ist montags bis freitags während der üblichen Geschäftszeiten Ihrer Zeitzone erreichbar.

Informationen zu diesem Vorgang

Sie können den IBM Support auf zwei verschiedene Weisen kontaktieren:

1. Fall im IBM Support Portal öffnen
2. Serviceanforderung über das IBM Call Center erstellen

Fall im IBM Support Portal öffnen

Vorgehensweise

1. Melden Sie sich an https://www.ibm.com/mysupport/s/ an.

   Anmerkung: Sie müssen zuerst ein Konto erstellen, um auf das IBM Support Portal zuzugreifen.
2. Klicken Sie oben rechts im Portal auf **Fall öffnen**. Die Seite **Fall öffnen** wird angezeigt.
3. Wählen Sie den **Supporttyp** aus.
4. Geben Sie **Titel**, **Hersteller** und **Produkt** ein.

   Anmerkung: Damit Ihre Anforderung direkt an das für die Technical Support Appliance zuständige Team weitergeleitet wird, geben Sie im Feld **Produkt** `Technical Support Appliance` ein.
5. Wählen Sie den **Schweregrad** aus.
6. Geben Sie unter **Beschreibung** die Beschreibung ein und wählen Sie Ihre bevorzugte Sprache aus.
7. Falls kein Mitarbeiter verfügbar ist, der Ihre Sprache spricht, und Sie auf Englisch kommunizieren möchten, klicken Sie auf **Ja**.
8. Klicken Sie auf **Fall einreichen**.

Serviceanforderung über das IBM Call Center erstellen

Vorgehensweise

1. Wählen Sie die für Ihr Herkunftsland geltende Telefonnummer (siehe https://www.ibm.com/planetwide)
2. Wählen Sie die Sprache aus.
3. Wählen Sie 1 (IBM Produkte).
4. Wählen Sie 2 (Software Support).
5. Nennen Sie die Produkt-ID *5621IZX01* oder den Produktnamen *Technical Support Appliance*.
6. Sie werden um folgende Angaben gebeten:
   - Unternehmensnummer/Region
   - Kunden-/Firmenname
   - Adresse/Postleitzahl/Ort/Bundesland
   - Gebäude/Stockwerk/Raum
   - Telefonnummer am Standort der TSA
   - Name/E-Mail/Telefonnummer der Kontaktperson
   - Problembeschreibung

- Schweregrad

Anhang A. Die Technical Support Appliance konfigurieren

Falls Sie die Konfiguration der Einstellungen im **Installationsassistenten** beenden oder überspringen, können Sie die Einstellungen über das Navigationsmenü der TSA auf der linken Seite manuell konfigurieren.

Technical Support Appliance registrieren

Bei der Registrierung werden Informationen gesammelt, die zur Identifizierung der TSA erforderlich sind, wenn Daten zur Analyse an IBM übermittelt werden.

Informationen zu diesem Vorgang

Führen Sie zum Registrieren die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Registrierung**.
   Die Seite **Registrierung** wird angezeigt.

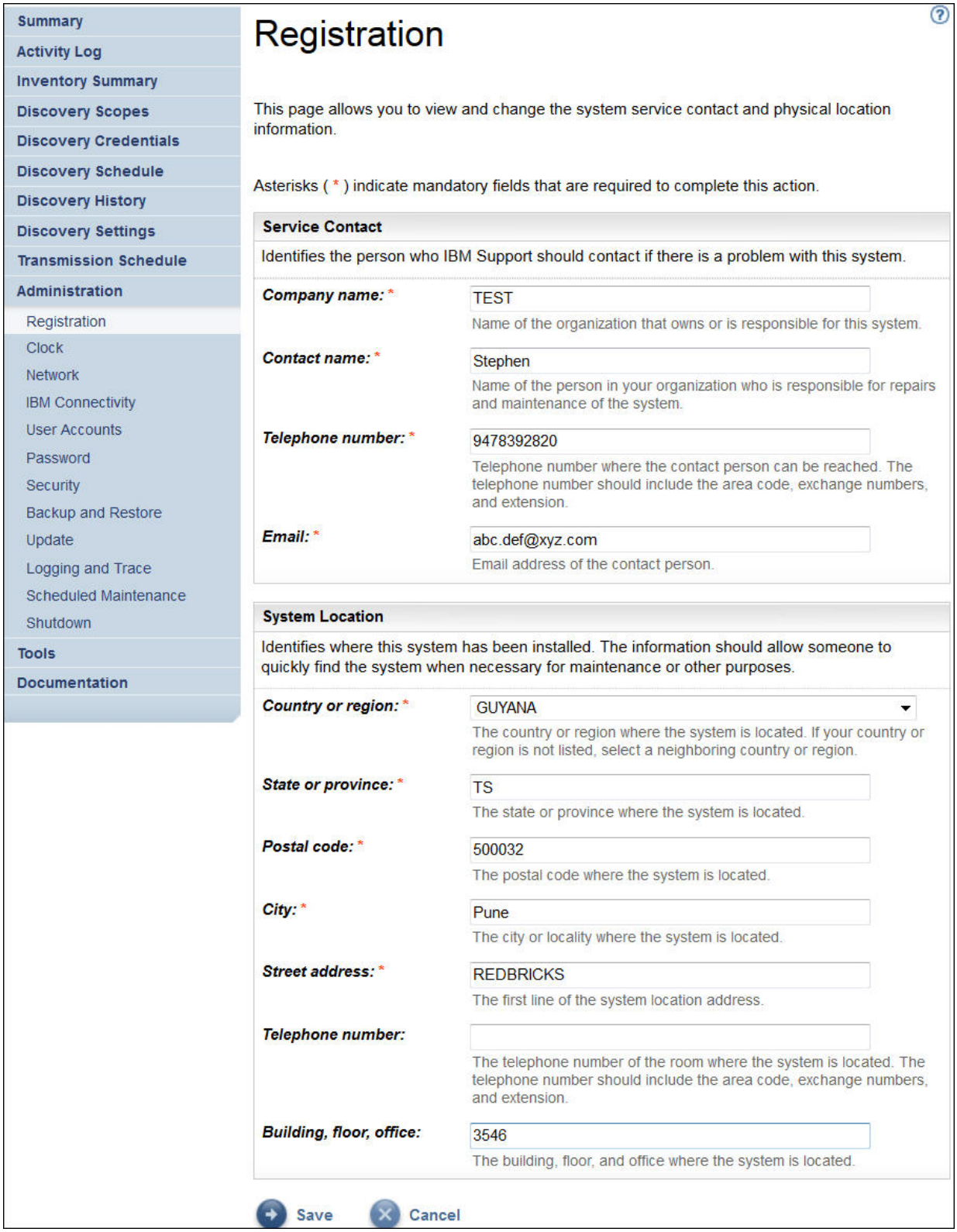

Abbildung 91. Registrierung

2. Geben Sie die Servicekontaktinformationen in folgenden Feldern an:

Firmenname
Der Name des Unternehmens, das die TSA verwendet.

Kontaktname
(Optional) Der Name der Person im Unternehmen, die für die TSA verantwortlich ist.

Telefonnummer
(Optional) Die Telefonnummer, unter der die Kontaktperson erreicht werden kann. Die Telefonnummer muss Vorwahl, Telefonzentrale und Durchwahlnummer enthalten. In der Telefonnummer dürfen keine Klammern enthalten sein.

E-Mail
(Optional) Die E-Mail-Adresse der Kontaktperson.

IBMid
(Optional) Die IBMid der Person, die Sie zum Anzeigen der Berichte im IBM Client Insights Portal autorisieren möchten.

Anmerkung: Mit Ihrer zugewiesenen IBMid können Sie sich unter https://clientinsightsportal.ibm.com/ an, um Ihre TSA-Berichte innerhalb von 1-2 Tagen nach jeder Datenübertragung herunterzuladen. Um eine IBMid zu beantragen, rufen Sie die Seite https://www.ibm.com/account auf.

Anmerkung: Der Servicekontakt ist die Person, die vom IBM Support bei einem Problem mit dem System zu kontaktieren ist. Die Kontaktinformationen werden von IBM verwendet, um Ihrem Unternehmen die Ergebnisse der Analyse der Technical Support Appliance zu übermitteln.

3. Geben Sie den Standort der TSA in folgenden Feldern an:

Land oder Region
Das Land oder die Region, wo sich die TSA befindet.

Bundesland oder Provinz
Das Bundesland oder die Provinz, wo sich die TSA befindet. Falls Ihnen das Bundesland nicht bekannt ist, geben Sie *Unbekannt* ein.

Postleitzahl
Die Postleitzahl des Standorts, an dem sich die TSA befindet.

Ort
Die Stadt oder der Ort, wo sich die TSA befindet.

Straßenadresse
Die Adresse des TSA-Standorts.

Telefonnummer
(Optional) Die Telefonnummer des Raums, in dem sich die TSA befindet. Die Telefonnummer muss Vorwahl, Telefonzentrale und Durchwahlnummer enthalten. In der Telefonnummer dürfen keine Klammern enthalten sein.

Gebäude, Stockwerk, Büro
(Optional) Das Gebäude, Stockwerk und Büro, in dem sich die TSA befindet.

4. Klicken Sie auf **Speichern**, um die Registrierungsinformationen zu speichern.

IBM Konnektivität einrichten

Geben Sie die Internetverbindungsdaten an, die für die Verbindung mit IBM verwendet werden sollen.

Vorbereitende Schritte

Stellen Sie sicher, dass Ihre Firewall Verbindungen zu Hostnamen und IP-Adressen von IBM Servern zulässt, wie in der Tabelle Tabelle 1 auf Seite 6 erläutert. Falls Ihr Netz den Zugriff auf die IBM Server nicht erlaubt, schlagen TSA-Transaktionen mit dem IBM Support fehl.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **IBM Konnektivität**.

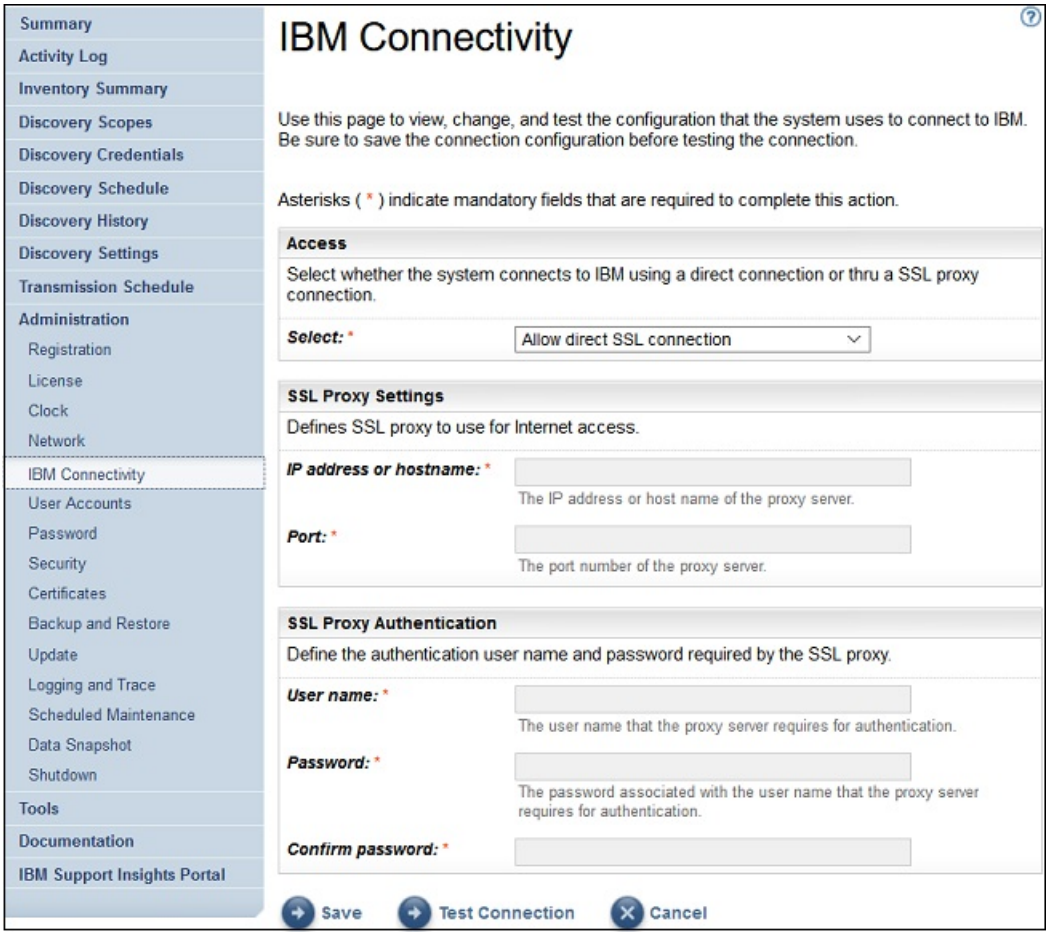

Abbildung 92. IBM Konnektivität

2. Wählen Sie im Fenster **Zugang** eine der folgenden Internetzugangsarten aus:

   SSL-Direktverbindung ermöglichen
   TSA stellt die Verbindung zu IBM über eine Direktverbindung her.

   SSL-Proxyverbindung verwenden
   TSA stellt die Verbindung zu IBM über eine SSL-Proxyverbindung her.

   SSL-Proxyverbindung mit Authentifizierung verwenden
   TSA stellt die Verbindung zu IBM über eine authentifizierende SSL-Proxyverbindung her.

3. Wenn Sie **Use SSL proxy connection** oder **Use authenticating SSL proxy connection** ausgewählt haben, geben Sie die folgenden Informationen zum Proxyserver an.

   IP-Adresse oder Hostname
   Die IP-Adresse oder der Hostname des Proxyservers.

   Anmerkung: Der eingegebene Hostname darf keinen Unterstrich ("_") enthalten.

   Port
   Die Portnummer des Proxyservers.

4. Wenn Sie **Use authenticating SSL proxy connection** ausgewählt haben, geben Sie die folgenden Informationen zum Proxyserver an:

   Benutzername
   Der Benutzername, den der Proxyserver zur Authentifizierung benötigt.

   Kennwort
   Das Kennwort zum Benutzernamen, das der Proxyserver zur Authentifizierung benötigt.

Kennwort bestätigen
Geben Sie das Kennwort erneut ein. Die beiden Kennwörter werden verglichen und auf Übereinstimmung geprüft, bevor das Kennwort gespeichert wird.

5. Klicken Sie auf **Speichern**, um die IBM Verbindungsinformationen zu speichern.
6. Klicken Sie auf **Verbindung testen**, um die angegebene Verbindung zu testen.

Wichtig:

- Speichern Sie die Verbindungseinstellungen, bevor Sie mit dem Testen der Verbindung beginnen.
- Ohne funktionierende Verbindung zu IBM sind die TSA-Funktionen nicht ausführbar.

Zugehörige Konzepte

Konfigurationsanforderungen für Verbindungen zum IBM Support

Die TSA kann mit dem IBM Support entweder per Direktverbindung oder über einen benutzerseitigen Proxy-Server in Verbindung treten, der für die Kommunikation mit IBM konfiguriert werden muss. Bei Verwendung eines Proxy wird die TLS/SSL-Prüfung nicht unterstützt. Alle über einen Proxy gesendeten Anforderungen müssen ohne TLS/SSL-Abschluss direkt an IBM fließen können.

Systemzeit einstellen

Während der Einrichtung müssen Sie die Systemzeit für die TSA, das Datum und die örtliche Zeitzone festlegen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Systemzeit**.
   Die Seite **Systemzeit** wird angezeigt.

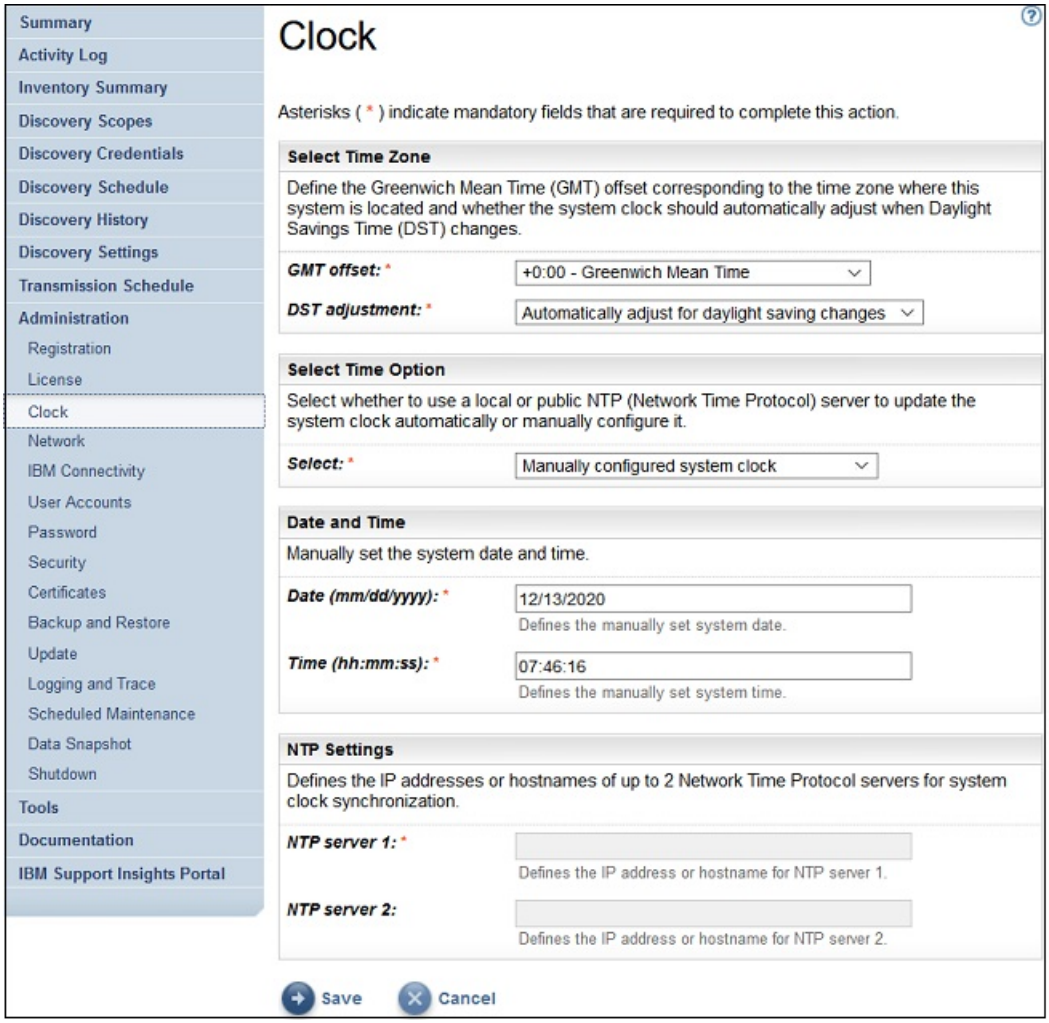

Abbildung 93. Systemzeit

2. Wählen Sie in der Dropdown-Liste **GMT-Abweichung** Ihre örtliche Zeitzone aus.
3. Wählen Sie in der Dropdown-Liste **Sommerzeitanpassung** die Anpassung für die Sommerzeit aus.

   Anmerkung: Die Sommerzeit gilt nicht in allen Zeitzonen. Wenn Sie diese Option für eine Zeitzone ohne Sommerzeit auswählen, wird eine Fehlernachricht angezeigt.
4. Wählen Sie in der Dropdown-Liste **Zeitoption auswählen** eine Methode für die Aktualisierung der Systemuhr aus.

   Die Systemuhr kann entweder automatisch durch Synchronisierung mit einem NTP-Server (Network Time Protocol) aktualisiert oder manuell eingestellt werden.

   a) Wenn Sie festgelegt haben, die Systemuhr manuell zu konfigurieren, stellen Sie das Datum und die Uhrzeit für das System ein. Geben Sie Datum und Uhrzeit in die Felder **Datum** und **Uhrzeit** ein.

   b) Wenn Sie festgelegt haben, die Systemuhr automatisch durch Synchronisierung mit einem NTP-Server zu aktualisieren, müssen Sie die IP-Adresse und den Hostnamen des NTP-Servers angeben. Tragen Sie in den **NTP-Server**-Feldern die IP-Adressen oder Hostnamen für bis zu zwei Server ein.

      Anmerkung: Vergewissern Sie sich, das der NTP-Server für die TSA über das Netz erreichbar ist.
5. Klicken Sie auf **Speichern**, um die Angaben zur Systemzeit zu speichern.

Ergebnisse

Anmerkung: Bei einigen Änderungen ist ein Neustart erforderlich, damit die Änderungen wirksam werden. Beispielsweise werden Sie aufgefordert, das System neu zu starten, wenn Sie das Datum oder die

Uhrzeit eingestellt haben oder von der manuellen Konfiguration zur NTP-Server-Konfiguration umgestiegen sind.

Übertragungszeitplan einrichten

In der TSA ist ein Standardzeitplan definiert, nach dem der Übertragungsprozess zu bestimmten Zeiten ausgeführt wird. Sie können diesen Zeitplan gemäß Ihren Anforderungen ändern.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Übertragungszeitplan**.
   Die Seite **Übertragungszeitplan** wird angezeigt.

   Im Fensterbereich **Zeitplan** werden die nächste geplante Ausführung und die definierten Ausführungszeitpunkte angezeigt. Im Bereich **Verlauf** sind der Status und weitere Details des aktuell ausgeführten und der vorherigen Übertragungsjobs aufgeführt.
2. Klicken Sie auf **Zeitplan bearbeiten**.
   Die Seite **Übertragungszeitplan** wird angezeigt.

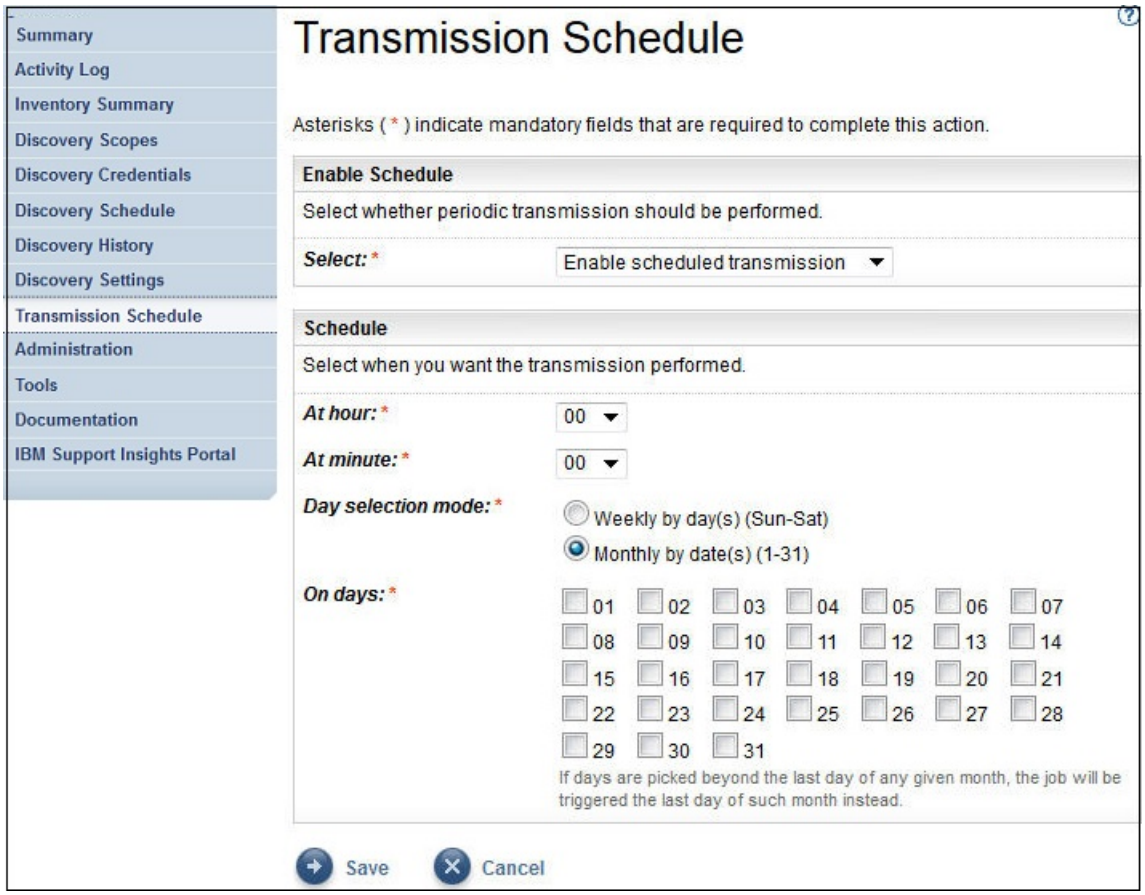

Abbildung 94. Übertragungszeitplan bearbeiten

a) Wählen Sie mithilfe der Dropdown-Listen **Stunde** und **Minute** einen neuen Zeitpunkt aus.

b) Legen Sie den **Tagauswahlmodus** fest.

Wöchentlich nach Tag(en) (So-Sa)
Um die Übertragung für einen bestimmten Tag oder mehrere Tage der Woche zu planen, wählen Sie die Option **Wöchentlich nach Tag(en) (So-Sa)** aus.

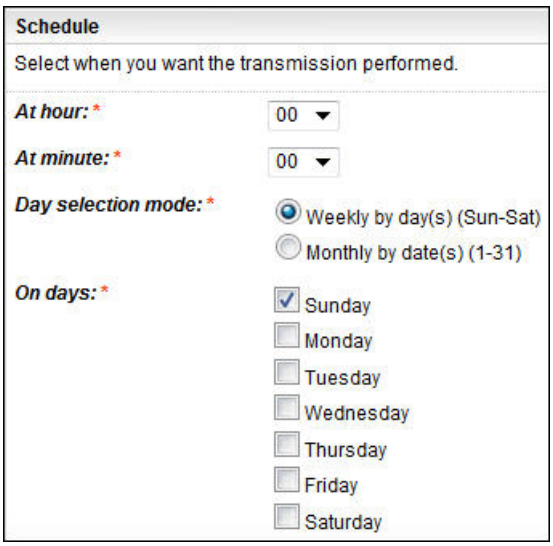

Abbildung 95. Wöchentlich nach Tag(en) (So-Sa)

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Wochentage aus.

Monatlich nach Datum (1-31)

Um die Übertragung für bestimmte Tage im Monat zu planen, wählen Sie die Option **Monatlich nach Datum (1-31)** aus.

Wählen Sie mithilfe der Kontrollkästchen unter **Tage** einen oder mehrere Tage im Monat aus.

Anmerkung: Wenn Tage über den letzten Tag eines Monats hinaus ausgewählt werden, wird der Job am letzten Tag dieses Monats ausgeführt.

3. Klicken Sie auf **Speichern**.
   Die Seite **Übertragungszeitplan** wird mit dem neuen Zeitplan angezeigt.

Update

Sie können Updates für die TSA suchen und herunterladen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Update**.
   Die Seite **Update** wird angezeigt.

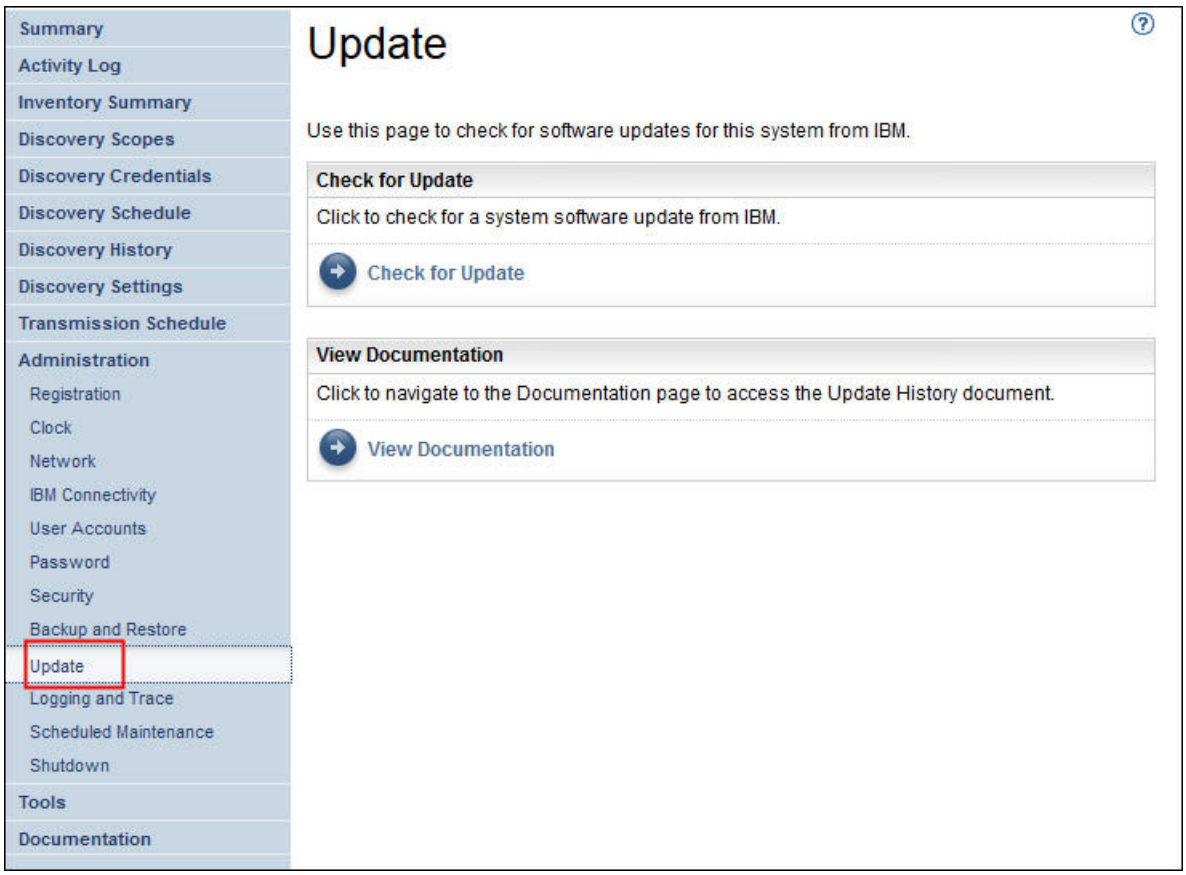

Abbildung 96. Update

2. Klicken Sie auf **Auf Update prüfen**.
   Auf der Seite **Updateverfügbarkeit** werden alle verfügbaren Updates aufgelistet.

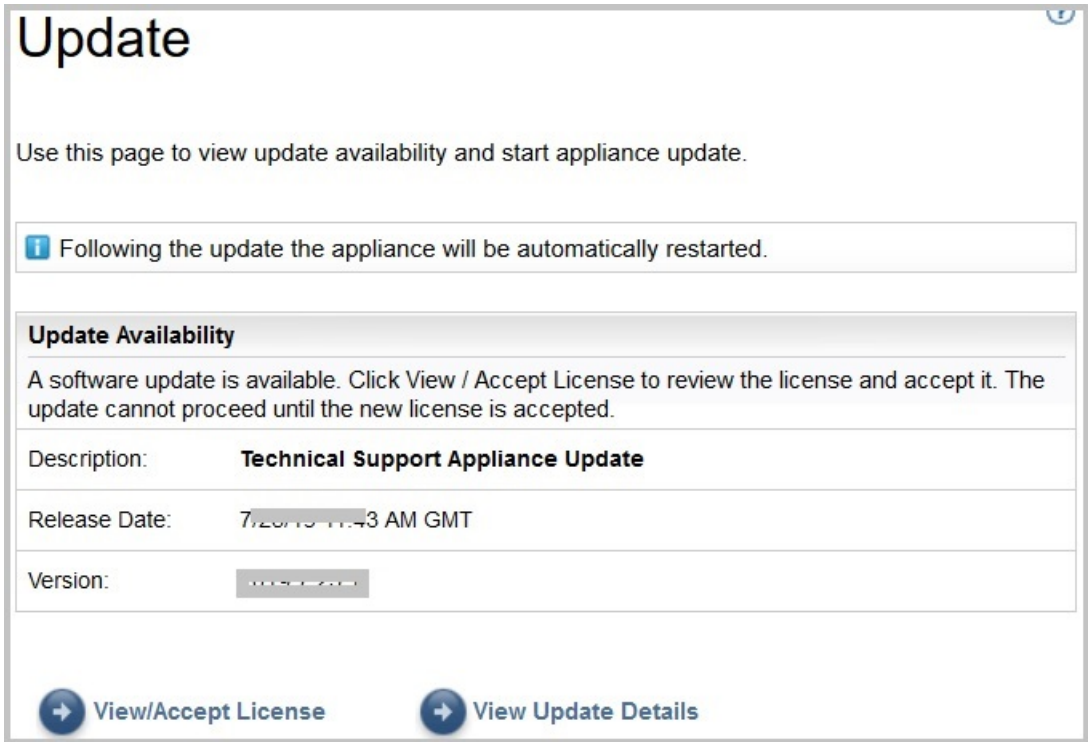

Abbildung 97. Updateverfügbarkeit

a) Bei manchen neuen Releases der TSA müssen Sie eine neue Lizenzvereinbarung akzeptieren, bevor Sie mit der Aktualisierung fortfahren können. Falls eine neue Lizenzvereinbarung vorliegt, klicken Sie auf die Schaltfläche **Lizenz anzeigen/akzeptieren**. Die Seite **Lizenzvereinbarung** wird angezeigt.

b) Klicken Sie auf die Schaltfläche **Akzeptieren** auf der Seite **Lizenzvereinbarung**, um die neue Lizenzvereinbarung zu akzeptieren. Daraufhin wird die Seite **Update** nun mit der Schaltfläche **Update jetzt ausführen** angezeigt. Falls keine neue Lizenzvereinbarung akzeptiert werden muss, erscheint die Schaltfläche **Lizenz anzeigen/akzeptieren** nicht, sondern Sie können direkt auf **Update jetzt ausführen** klicken.

Anmerkung:

- Nachdem Sie die Lizenz akzeptiert haben, wird die Schaltfläche **Lizenz anzeigen/akzeptieren** nicht mehr angezeigt.
- Klicken Sie im Navigationsfenster auf **Verwaltung** > **Lizenz**, um die aktuelle Lizenzvereinbarung, die Sie akzeptiert haben, anzusehen.

c) Klicken Sie zum Installieren des Updates auf **Update jetzt ausführen**.

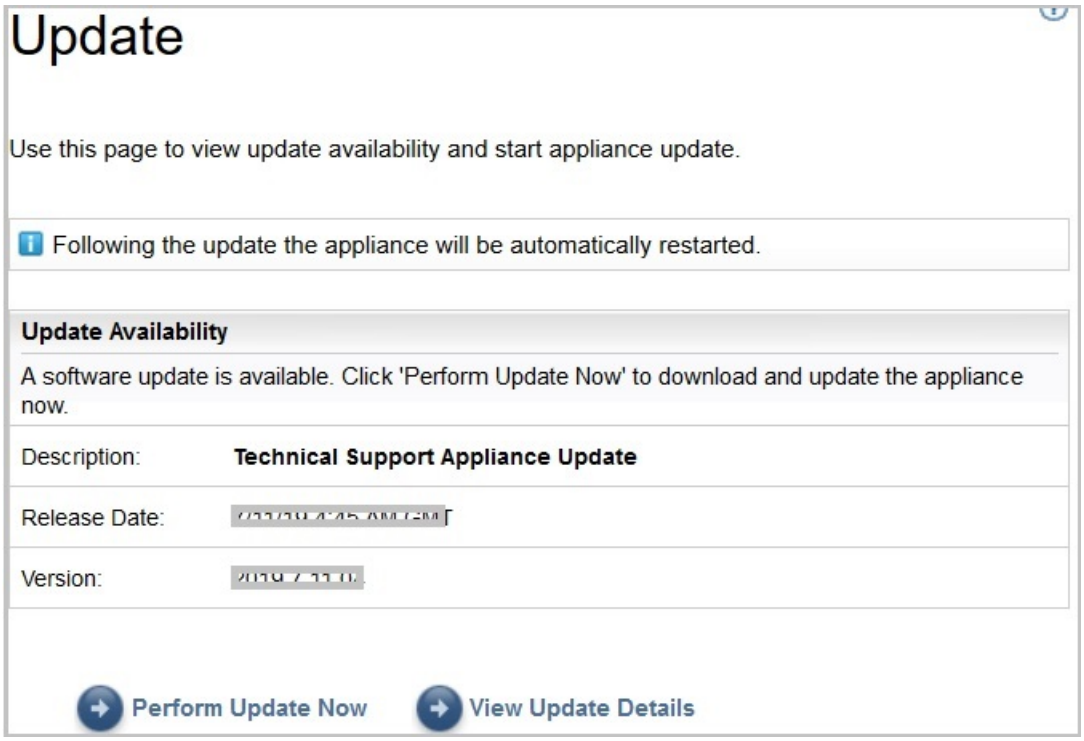

Abbildung 98. Update jetzt ausführen

Nach Abschluss der Aktualisierung wird die TSA automatisch neu gestartet.

d) Um Informationen zu den Inhalten des Updates anzuzeigen, klicken Sie auf **Updatedetails anzeigen**.

Anhang B. DHCP-Netzdetails konfigurieren

Führen Sie zum Konfigurieren der DHCP-Netzdetails die folgenden Schritte durch:

Vorgehensweise

1. Wählen Sie im **TSA-Konfigurationsmenü** die Option **1) Setup network configuration** aus.

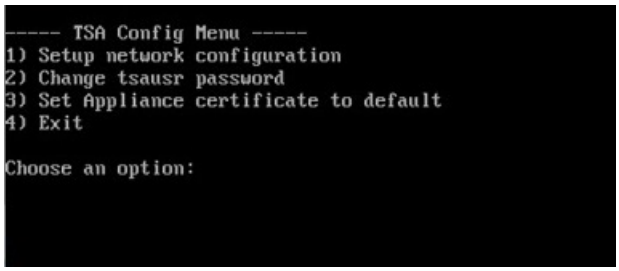

Abbildung 99. Netzkonfiguration einrichten

2. Geben Sie die folgenden Netzkonfigurationsdetails ein.

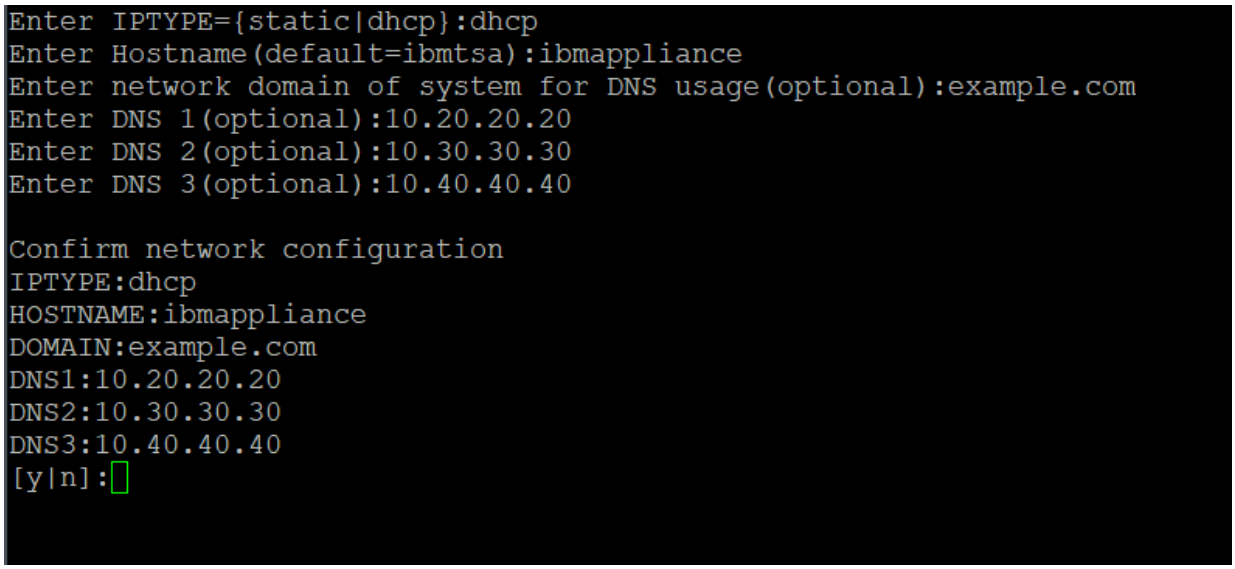

Abbildung 100. Netzkonfiguration

a) **Enter IPTYPE = {static|dhcp}**. Geben Sie dhcp ein.

IPTYPE: dhcp

Enter Hostname(default=ibmtsa). Sie können den Standardhostnamen ändern. Stellen Sie sicher, dass der Hostname eindeutig ist.

Enter network domain of system for DNS usage (optional).

Enter DNS 1(optional), **Enter DNS 2(optional)** und **Enter DNS 3(optional)**.

Die angegebenen Netzkonfigurationsdetails werden zur Bestätigung angezeigt.

b) Geben Sie **[y|n]** ein, um die Netzkonfiguration zu bestätigen oder zu verwerfen. Durch Eingabe von **y** wird die Netzkonfiguration gespeichert und das System automatisch neu gestartet.

Anmerkung: Falls die Konfiguration nicht korrekt ist können Sie die Details ändern. Geben Sie **n** ein, um die aktuellen Einstellungen zu ignorieren und die Konfiguration ab Schritt „2.a" auf Seite 131 neu zu starten.

c) Das System wird nach 15 Sekunden neu gestartet, damit die neue Netzkonfiguration wirksam wird.

d) Melden Sie sich nach dem Systemneustart im Virtualization Manager an und notieren Sie sich die **IP-Adresse**, die auf der Registerkarte **Zusammenfassung** angezeigt wird.

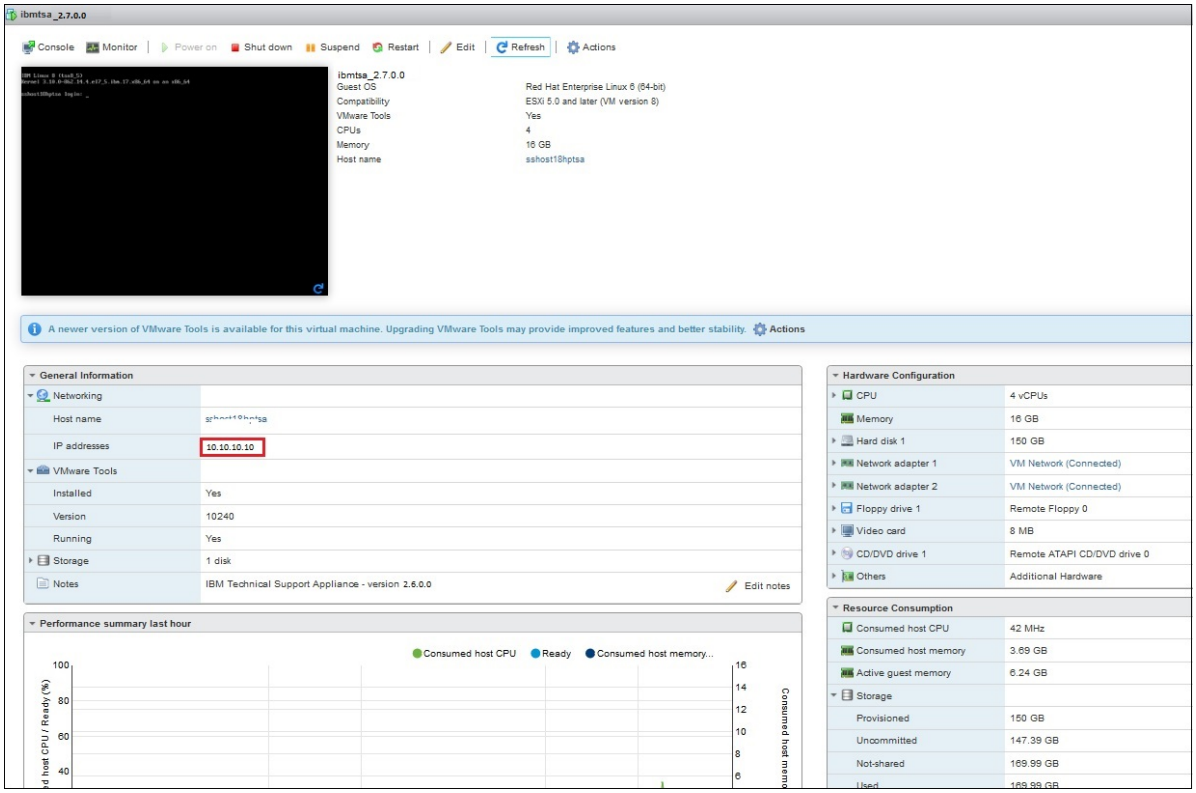

Abbildung 101. DHCP-IP-Adresse

e) Greifen Sie über den Browser mit der URL, die Sie im vorherigen Schritt erhalten haben, auf die TSA zu.
Beispiel: `https://newhost1.new.abclabs.example.com`

Anmerkung: Beim erstmaligen Verbindungsaufbau wird in Ihrem Browser eventuell eine Sicherheitsausnahmebedingung angezeigt. Akzeptieren Sie das Sicherheitszertifikat und setzen Sie die Anmeldung bei der TSA fort.

Anhang C. Benutzerkonten und Benutzergruppen

Sie können Benutzerkonten und Benutzergruppen hinzufügen, um den Zugriff auf TSA-Funktionen zu steuern.

Vorbereitende Schritte

TSA wird mit dem Benutzerkontonamen **admin** installiert. Dieses Konto hat die Berechtigung zur Ausführung jeder TSA-Funktion. Sie können auch Benutzerkonten aus den folgenden Gründen hinzufügen:

- Einem anderen Benutzer ermöglichen, als Vertretung für den **Benutzer mit Administratorberechtigung** zu agieren.
- Einigen Benutzern den Zugriff auf eine begrenzte Anzahl von TSA-Funktionen ermöglichen.

Informationen zu diesem Vorgang

Die Ausführung einer TSA-Funktion setzt eine bestimmte Berechtigungsstufe voraus. Wenn ein authentifizierter Benutzer versucht, eine Funktion auszuführen, ohne über die erforderliche Berechtigungsstufe zu verfügen, wird ein Fehler angezeigt und die Ausführung der Funktion verhindert.

In der TSA werden Berechtigungsstufen an Benutzergruppen vergeben. Benutzern wird die Mitgliedschaft in einer oder mehreren Benutzergruppen zugeordnet, wodurch sie die Berechtigungsstufe zur Ausführung bestimmter Funktionen erhalten.

In der TSA sind eine Benutzergruppe **Administrator** und ein **Benutzerkonto mit Administratorberechtigung** vorkonfiguriert. Die Benutzergruppe **Administrator** verfügt über uneingeschränkten Zugriff auf alle Systemfunktionen. Das **Benutzerkonto mit Administratorberechtigung** ist der Benutzergruppe **Administrator** zugeordnet.

Benutzerkonten und Benutzergruppen anzeigen

Sie können die vorhandenen Benutzerkonten und Benutzergruppen anzeigen.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.
   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Zum Anzeigen der vorhandenen Benutzerkonten klicken Sie auf die Registerkarte **Konten**.
   Die Benutzerkonten sind in der Tabelle "Benutzerkonten" aufgeführt.

   Tipp: Um Details zu einem bestimmten Benutzerkonto anzuzeigen, klicken Sie auf den Namen des Benutzerkontos. Der Fensterbereich auf der rechten Seite **Allgemein** enthält den Benutzernamen, den vollständigen Namen und eine Beschreibung zu dem ausgewählten Benutzerkonto. Klicken Sie auf den Fensterbereich auf der rechten Seite **Mitglied von**, um die Benutzergruppen anzuzeigen, zu denen dieses Benutzerkonto gehört.
3. Zum Anzeigen der vorhandenen Benutzergruppen klicken Sie auf die Registerkarte **Gruppen**.
   Die Benutzergruppen sind in der Tabelle "Benutzergruppen" aufgeführt.

   Tipp: Um Details zu einer bestimmten Benutzergruppe anzuzeigen, klicken Sie auf den Namen der Benutzergruppe. Der Fensterbereich auf der rechten Seite **Allgemein** enthält den Namen der Benutzergruppe und die ihr zugeordnete Berechtigungsstufe. Klicken Sie auf den Fensterbereich auf der rechten Seite **Bereichsbeschränkungen**, um die Bereichsgruppen anzuzeigen, in denen die ausgewählte Benutzergruppe Erkennungen ausführen kann. Klicken Sie auf den Fensterbereich **Mitglieder**, um die Benutzerkonten anzuzeigen, die zu dieser Benutzergruppe gehören.

Benutzerkonten und Benutzergruppen hinzufügen

Sie können Benutzerkonten und -gruppen hinzufügen, um den Zugriff auf TSA-Funktionen zu steuern.

Zugehörige Konzepte

Erkennungsbereiche und Bereichsgruppen

Durch Erkennungsbereiche wird festgelegt, welche Ressourcen die TSA erkennen soll. Die Erkennungsbereiche sind in Erkennungsbereichsgruppen gegliedert.

Benutzergruppe hinzufügen

Sie können Benutzergruppen hinzufügen, um den Zugriff auf TSA-Funktionen zu steuern.

Informationen zu diesem Vorgang

Führen Sie zum Hinzufügen einer Benutzergruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.
   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Gruppen**.

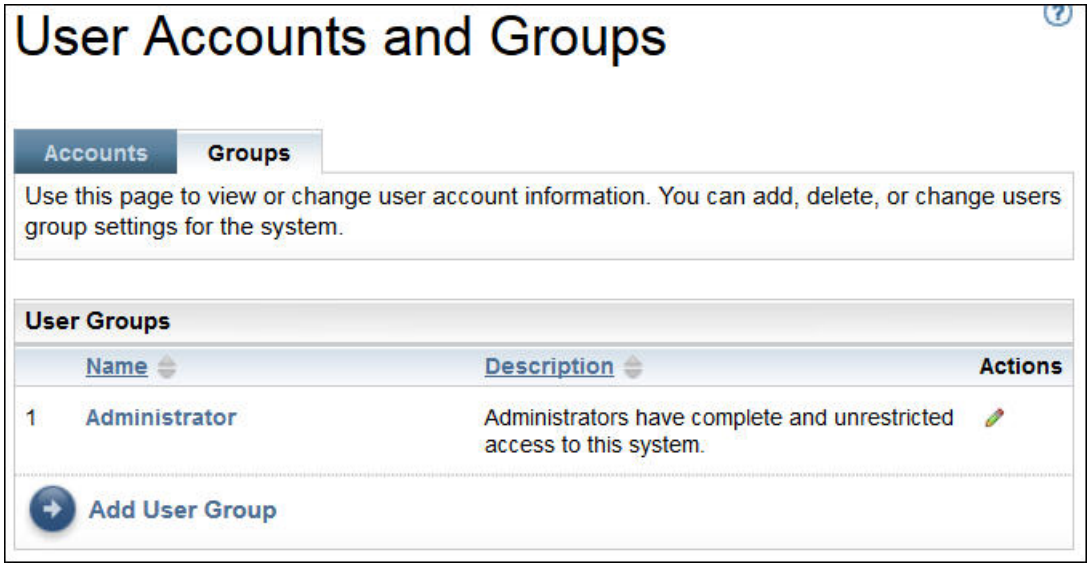

Abbildung 102. Gruppen

3. Klicken Sie auf **Benutzergruppe hinzufügen**.
   Die Seite **Benutzergruppe** wird angezeigt.

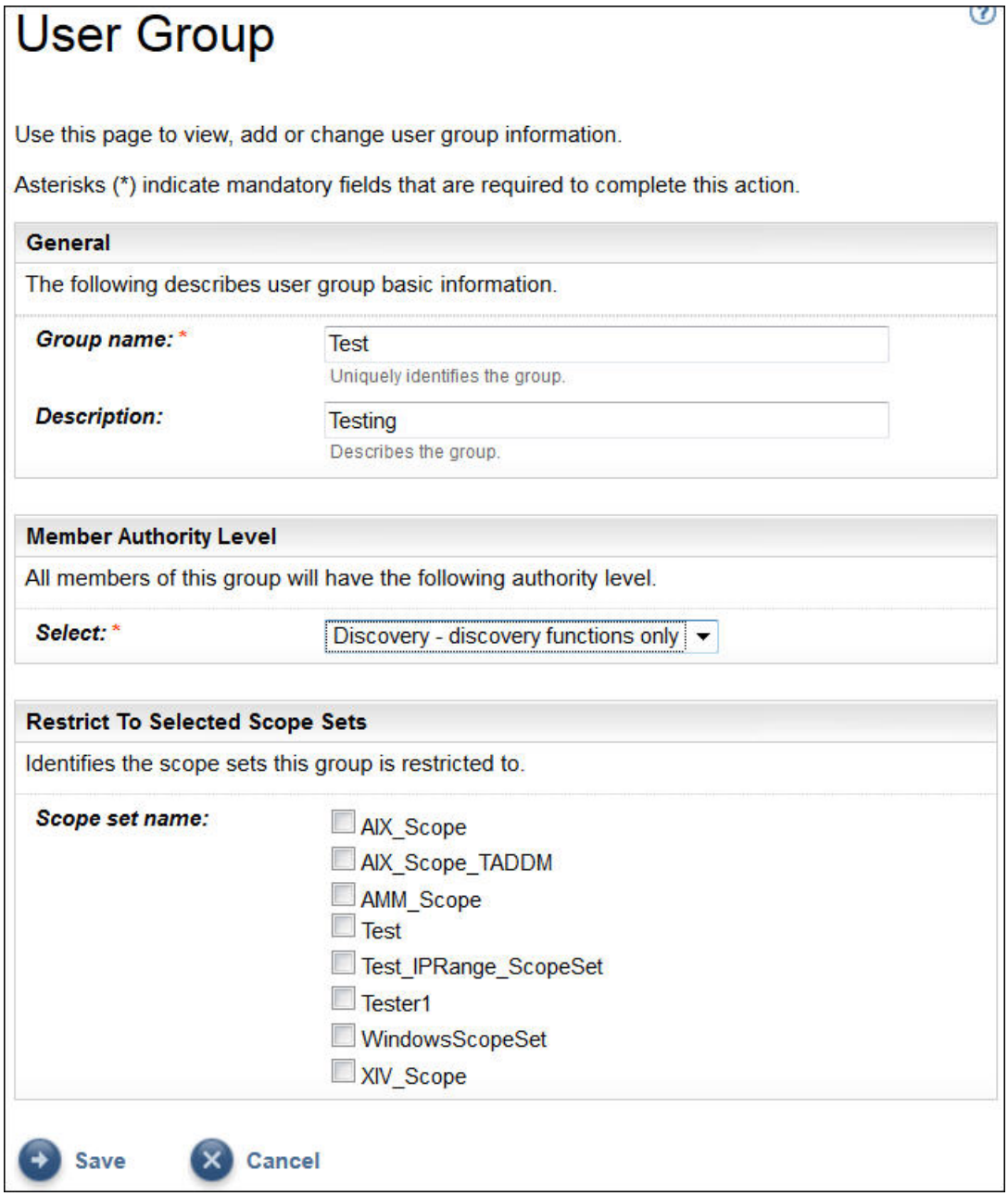

Abbildung 103. Benutzergruppe hinzufügen

4. Geben Sie im Feld **Gruppenname** einen eindeutigen Namen für die Benutzergruppe ein.
5. Optional: Geben Sie im Feld **Beschreibung** eine Beschreibung für die Benutzergruppe ein.
6. Wählen Sie die Berechtigungsstufe aus, die Sie der Benutzergruppe zuweisen möchten.

   Die TSA definiert die folgenden Berechtigungsstufen für Gruppen:

   - **Administrator** – keine Einschränkungen
   - **Erkennung** – nur Erkennungsfunktionen
   - **Besucher** – nur Lesezugriff
7. Wenn Sie für die Benutzergruppe die Berechtigungsstufe *Erkennung* festlegen, müssen Sie mindestens eine Bereichsgruppe auswählen, die auf diese Benutzergruppe beschränkt ist.

   Weitere Informationen zu Bereichsgruppen finden Sie im Abschnitt „Erkennungsbereiche und Bereichsgruppen” auf Seite 2.
8. Klicken Sie auf **Speichern**, um die Benutzergruppe zu speichern.

Die Seite **Benutzerkonten und -gruppen** wird mit der neuen Gruppe in der Liste angezeigt.

Benutzerkonto hinzufügen

Sie können Benutzerkonten hinzufügen, um den Zugriff auf TSA-Funktionen zu steuern.

Informationen zu diesem Vorgang

Führen Sie zum Hinzufügen eines Benutzerkontos die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.
   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.

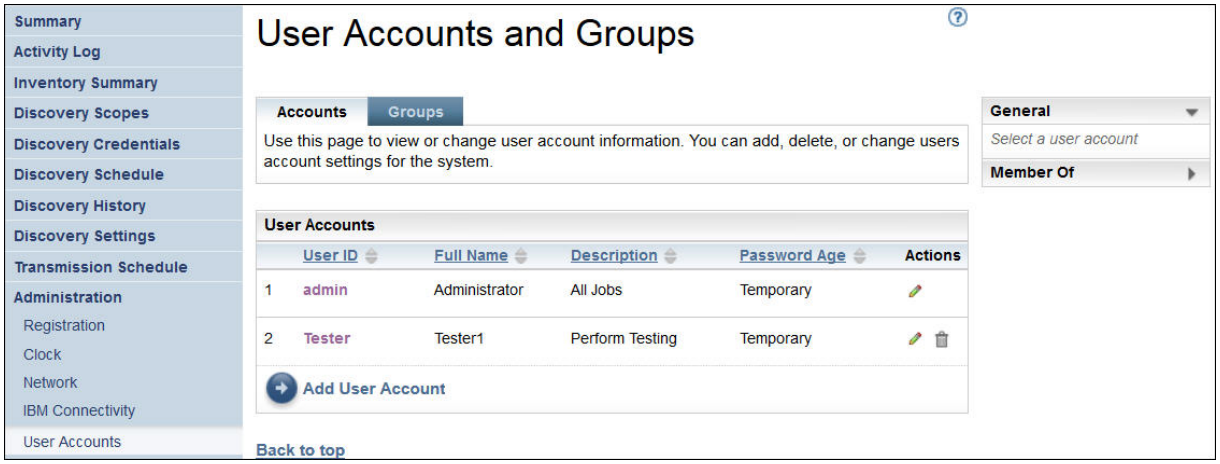

Abbildung 104. Benutzerkonten und -gruppen

2. Um ein neues Benutzerkonto zu definieren, klicken Sie auf **Benutzerkonto hinzufügen**.
   Die Seite **Benutzerkonto** wird angezeigt.

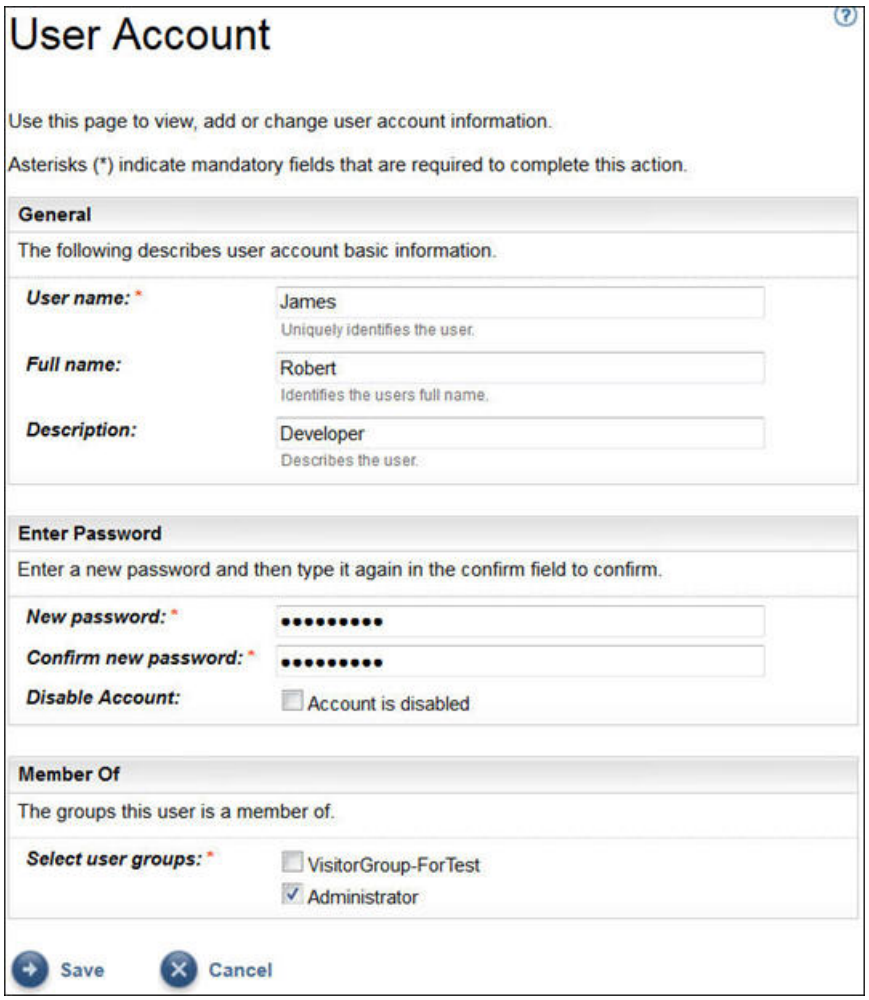

Abbildung 105. Benutzerkonto hinzufügen

3. Geben Sie im Feld **Benutzername** einen Namen für das Benutzerkonto ein.
4. Optional: Geben Sie im Feld **Vollständiger Name** den vollständigen Namen des Benutzers dieses Kontos ein.
5. Optional: Geben Sie im Feld **Beschreibung** eine Beschreibung für das Benutzerkonto ein.
6. Geben Sie im Feld **Neues Kennwort** ein Kennwort für das Benutzerkonto ein.

   Das Kennwort muss folgenden Regeln entsprechen:

   - Es muss mindestens 8 Zeichen lang sein.
   - Es muss mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthalten.
   - Der Benutzername darf nicht enthalten sein.
   - Es darf nicht mit einem der acht vorherigen Kennwörter identisch sein.
   - Es muss mindestens alle 30 Tage (Standard) oder entsprechend der Angabe im Abschnitt „Gültigkeitsdauer des Kennworts ändern” auf Seite 106 geändert werden, jedoch nicht öfter als einmal pro Tag.
7. Geben Sie im Feld **Kennwort bestätigen** erneut das Kennwort für dieses Benutzerkonto ein.

   Die beiden Kennwörter werden verglichen und auf Übereinstimmung geprüft, bevor das Kennwort gespeichert wird.

   Anmerkung: Das Kennwort muss bei der erstmaligen Anmeldung in diesem Benutzerkonto geändert werden.
8. Wenn Sie dieses Benutzerkonto inaktivieren möchten, wählen Sie das Kontrollkästchen **Konto ist inaktiviert** aus.

Durch Inaktivieren des Kontos können Sie verhindern, dass das Konto verwendet wird, ohne das Konto zu löschen.

Anmerkung: Sie können jedoch weder das **Administrator**konto inaktivieren noch die Gruppe des **Administrator**kontos ändern.

9. Wählen Sie die Benutzergruppen für dieses Benutzerkonto aus. Es muss mindestens eine Benutzergruppe ausgewählt werden. Die Benutzer erhalten die Berechtigungsstufe, die jeweils für die ausgewählten Gruppen definiert ist.
10. Klicken Sie auf **Speichern**, um das Benutzerkonto zu speichern.

    Die Seite **Benutzerkonten und -gruppen** wird mit dem neuen Benutzerkonto in der Liste angezeigt.

Benutzerkonten und Benutzergruppen ändern

Sie können vorhandene Benutzerkonten und Benutzergruppen ändern.

Benutzerkonten ändern

Sie können vorhandene Benutzerkonten ändern.

Informationen zu diesem Vorgang

Führen Sie zum Andern eines Benutzerkontos die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.

   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Konten**und dann auf das Symbol **Bearbeiten** ( ) neben dem Benutzerkonto.

   Die Seite **Benutzerkonto** wird angezeigt.
3. Im Fensterbereich **Allgemein** können Sie die Basisinformationen für dieses Benutzerkonto ändern.
4. Im Bereich **Kennwort eingeben** können Sie das Kennwort und die zugehörigen Verwaltungsinformationen ändern. Sie können dieses Benutzerkonto auch inaktivieren.

   Das Kennwort muss folgenden Regeln entsprechen:

   - Es muss mindestens 8 Zeichen lang sein.
   - Es muss mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthalten.
   - Der Benutzername darf nicht enthalten sein.
   - Es darf nicht mit einem der acht vorherigen Kennwörter identisch sein.
   - Es muss mindestens alle 90 Tage (Standard) geändert werden, jedoch nicht öfter als einmal pro Tag.

   Anmerkung: Das Kennwort muss bei der erstmaligen Anmeldung in diesem Benutzerkonto geändert werden.
5. Wenn Sie dieses Benutzerkonto inaktivieren möchten, wählen Sie **Konto ist inaktiviert** aus.

   Durch Inaktivieren des Kontos können Sie verhindern, dass das Konto verwendet wird, ohne das Konto zu löschen.Weitere Informationen zum Löschen eines Benutzerkontos finden Sie im Abschnitt „Benutzerkonten und Benutzergruppen löschen” auf Seite 140.

   Anmerkung: Sie können jedoch weder das **Administrator**konto inaktivieren noch die Gruppe des **Administrator**kontos ändern.

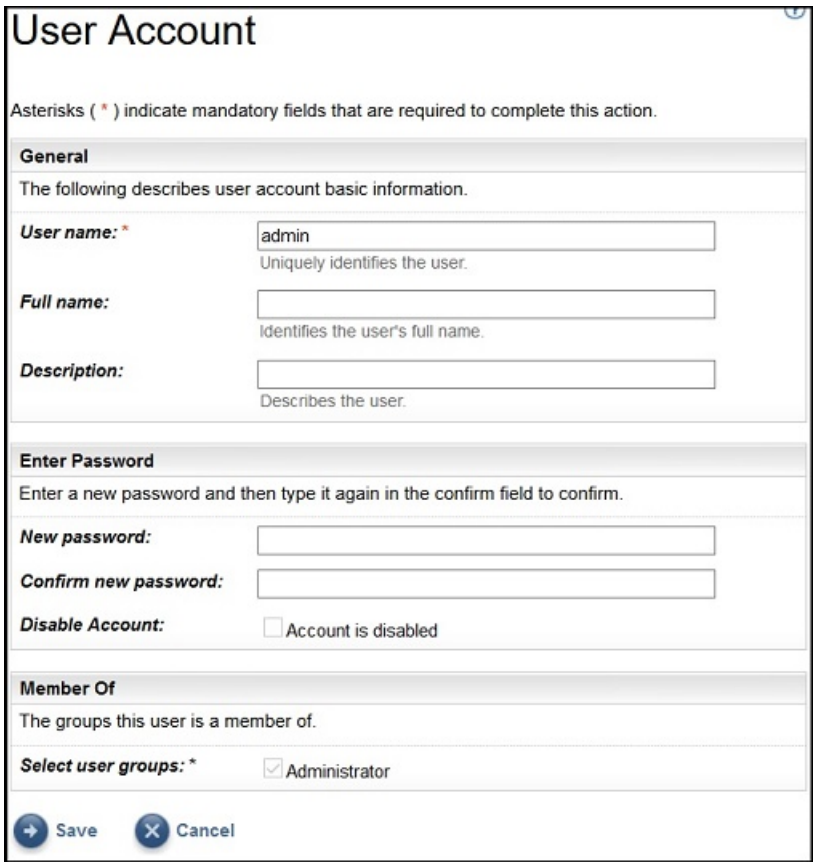

Abbildung 106. Administratorkonto ändern

6. Im Abschnitt **Mitglied von** können Sie die Benutzergruppen ändern, zu denen dieses Benutzerkonto gehört. Das Benutzerkonto muss Mitglied von mindestens einer Benutzergruppe sein.
7. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.
   Die geänderten Informationen werden auf der Seite **Benutzerkonten und -gruppen** angezeigt.

Benutzergruppen ändern

Sie können vorhandene Benutzergruppen ändern.

Vorbereitende Schritte

Anmerkung: Sie können die Gruppe **Administrator** nicht ändern.

Informationen zu diesem Vorgang

Führen Sie zum Ändern einer Benutzergruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.
   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Gruppen** und dann auf das Symbol **Bearbeiten** ( ) neben dem Benutzerkonto.
   Die Seite **Benutzergruppe** wird angezeigt.
3. Im Fensterbereich **Allgemein** können Sie die Basisinformationen für diese Benutzergruppe ändern.
4. Im Fensterbereich **Mitgliederberechtigungsstufe** können Sie ändern, ob die Benutzergruppe die Berechtigungsstufe *Administrator*, *Erkennung* oder *Lesen* erhält.

5. Wenn Sie im Fensterbereich **Auf ausgewählte Bereichsgruppen beschränken** die Berechtigungsstufe *Erkennung* in der **Mitgliederberechtigungsstufe** festgelegt haben, können Sie die Bereichsgruppen ändern, die diese Benutzergruppe erkennen darf.
6. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

   Die geänderten Informationen werden auf der Seite **Benutzerkonten und -gruppen** angezeigt.

Benutzerkonten und Benutzergruppen löschen

Sie können vorhandene Benutzerkonten und Benutzergruppen löschen.

Benutzerkonten löschen

Sie können vorhandene Benutzerkonten löschen.

Informationen zu diesem Vorgang

Anmerkung: Das Benutzerkonto **Administrator** kann nicht gelöscht werden.

Führen Sie zum Löschen eines Benutzerkontos die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf **Verwaltung** > **Benutzerkonten**.

   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Konten** und dann auf das Symbol **Löschen** ( ) neben dem zu löschenden Benutzerkonto.
3. Klicken Sie auf **OK**, um zu bestätigen, dass das Benutzerkonto gelöscht werden soll.

Benutzergruppen löschen

Sie können vorhandene Benutzergruppen löschen.

Informationen zu diesem Vorgang

Anmerkung: Die Benutzergruppe **Administrator** kann nicht gelöscht werden.

Führen Sie zum Löschen einer Benutzergruppe die folgenden Schritte durch:

Vorgehensweise

1. Klicken Sie auf **Verwaltung** > **Benutzerkonten**.

   Die Seite **Benutzerkonten und -gruppen** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Gruppen** und dann auf das Symbol **Löschen** ( ) neben der zu löschenden Benutzergruppe.
3. Klicken Sie auf **OK**, um zu bestätigen, dass die Benutzergruppe gelöscht werden soll.

   Anmerkung: Eine Benutzergruppe kann nur gelöscht werden, wenn ihr keine Benutzer zugeordnet sind.

Barrierefreiheit

Die Technical Support Appliance behindert nicht die Barrierefreiheitsfunktionen der unterstützten Browser. Eine umfassende Liste der Barrierefreiheitsfunktionen finden Sie auf der Barrierefreiheits-Informationsseite des von Ihnen verwendeten Browsers. Eine Liste der unterstützten Browser erhalten Sie unter „Erforderliche Web-Browser” auf Seite 5.

Die Veröffentlichungen zu diesem Produkt sind im Adobe Portable Document Format (PDF) und sollten den einschlägigen Barrierefreiheitsstandards entsprechen. Falls Sie Schwierigkeiten bei der Verwendung der PDF-Dateien haben, können Sie die betreffende Publikation in einem webbasierten Format anfordern, indem Sie eine E-Mail an folgende Adresse senden:

icfeedbk@us.ibm.com

Alternativ können Sie die Anforderung auch per Post an folgende Adresse senden:

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

Geben Sie in der Betreffzeile der Anforderungs-E-Mail den Titel der Publikation an, in diesem Fall "IBM Technical Support Appliance Installationshandbuch".

Durch das Einsenden von Informationen an IBM gewähren Sie IBM ein nicht ausschließliches Recht, die betreffenden Informationen in jeder als angemessen erachteten Weise weiterzugeben, ohne dass dadurch eine Verpflichtung gegenüber Ihnen entsteht.

Bemerkungen

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. Informationen über die gegenwärtig in Ihrem Land verfügbaren Produkte und Services erhalten Sie bei Ihrem örtlichen IBM Ansprechpartner. Die Bezugnahme auf bestimmte IBM Produkte, Programme oder Services bedeutet oder impliziert nicht, dass nur diese IBM Produkte, Programme oder Services verwendet werden können. Stattdessen können auch andere funktionsäquivalente Produkte, Programme oder Services verwendet werden, solange dadurch keine IBM Schutzrechte verletzt werden. Es obliegt jedoch dem Benutzer, den Betrieb aller Produkte, Programme oder Services anderer Anbieter zu überprüfen und zu bewerten.

IBM ist möglicherweise im Besitz von Patenten oder Patentanmeldungen in Bezug auf die in diesem Dokument beschriebenen Inhalte. Durch die Bereitstellung dieses Dokuments wird keinerlei Lizenz für diese Patente gewährt. Lizenzanforderungen sind schriftlich zu richten an:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Für Lizenzanforderungen mit Doppelbyte-Informationen (DBCS) wenden Sie sich bitte an das IBM Intellectual Property Department in Ihrem Land oder senden Sie Ihre Fragen schriftlich an:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Das folgende Abschnitt ist nicht zutreffend für das Vereinigte Königreich und alle andere Länder, in denen diese Bestimmungen nicht den lokalen Gesetzen entsprechen: INTERNATIONAL BUSINESS MACHINES CORPORATION STELLT DIESE PUBLIKATION AUF DER GRUNDLAGE DES GEGENWÄRTIGEN ZUSTANDS ("AS-IS") UND OHNE JEDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK ZUR VERFÜGUNG. Da in manchen Staaten der Ausschluss von ausdrücklichen oder stillschweigenden Gewährleistungen bei bestimmten Transaktionen nicht zulässig ist, trifft diese Aussage für Sie möglicherweise nicht zu.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann jederzeit ohne vorherige Ankündigung Verbesserungen bzw. Änderungen an dem/den in dieser Publikation beschriebenen Produkt(en) und/oder Programm(en) vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Sys-

temen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corp. in den USA und/oder anderen Ländern. Sonstige Produkt- und Servicenamen können ebenfalls Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Hyper-V und das Windows Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

VMware, das VMware-Logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server und VMware vSphere sind Marken oder eingetragene Marken der VMware, Inc., oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Teilenummer:

(1P) P/N: