HP SiteScope

Softwareversion: 11.30

Handbuch zur Bereitstellung

Datum der Dokumentveröffentlichung: Mai 2015
Datum des Software-Release: März 2015

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212; kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

Marken

Adobe® und Acrobat® sind Marken von Adobe Systems Incorporated.

Intel®, Pentium® und Intel® Xeon® sind Marken der Intel Corporation in den Vereinigten Staaten und anderen Ländern.

iPod ist eine Marke der Apple Computer, Inc.

Java ist eine eingetragene Marke von Oracle und/oder den Tochtergesellschaften.

Microsoft®, Windows®, Windows NT® und Windows® XP sind in den Vereinigten Staaten eingetragene Marken der Microsoft Corporation.

Oracle ist eine eingetragene Marke der Oracle Corporation und/oder ihren Tochterunternehmen.

UNIX® ist eine eingetragene Marke von The Open Group.

Dokumentationsaktualisierungen

Auf der Titelseite dieses Dokuments befinden sich die folgenden bezeichnenden Informationen:

- Software-Versionsnummer zur Angabe der Version der Software
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten:
https://softwaresupport.hp.com

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Um sich für eine HP Passport-ID zu registrieren, wechseln Sie zu: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Oder klicken Sie oben auf der Seite des HP Software-Supports auf den Link **Register**.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HP-Händler.

Support

Besuchen Sie die HP Software Support Online-Website von HP unter: **https://softwaresupport.hp.com**

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Support-Leistungen von HP Software.

HP Software-Unterstützung stellt Kunden online verschiedene Tools zur eigenständigen Problemlösung zur Verfügung. interaktiver technischer Support-Werkzeuge die Möglichkeit, ihre Probleme intern zu lösen. Als Kunde mit Supportvertrag stehen Ihnen beim Support folgende Optionen zur Verfügung:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Support-Verträgen
- Nachschlagen von HP-Supportkontakten
- Einsehen von Informationen über verfügbare Services

- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Für die meisten Support-Bereiche müssen Sie sich als Benutzer mit einem HP Passport registrieren und anmelden. In vielen Fällen ist zudem ein Support-Vertrag erforderlich. Hier können Sie sich für eine HP Passport-ID registrieren:

https://hpp12.passport.hp.com/hppcf/createuser.do

Weitere Informationen zu Zugriffsebenen finden Sie unter:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now greift auf die Website des HPSW-Lösungs- und Integrationsportals zu. Auf dieser Website finden Sie Informationen zu den HP Product Solutions, die Ihnen Lösungen zum Erreichen Ihrer Geschäftsziele bieten, eine vollständige Liste mit Integrationen für Ihre HP-Produkte sowie eine Auflistung der ITIL Processes. Die URL der Website lautet **http://h20230.www2.hp.com/sc/solutions/index.jsp**.

Inhalt

Teil 1: Einführung in SiteScope

Kapitel 1: SiteScope – Übersicht

HP SiteScope ist eine agentlose Überwachungslösung zur Gewährleistung der Verfügbarkeit und Leistung verteilter IT-Infrastrukturen, wie z. B. Server, Betriebssysteme, Netzwerkgeräte, Netzwerkdienste, Applikationen und Applikationskomponenten.

Diese webbasierte Lösung für die Infrastrukturüberwachung ist leicht, umfassend anpassbar und erfordert keine Installation von Agents zur Datenerfassung auf Ihren Produktionssystemen. Mit SiteScope erhalten Sie die notwendigen Echtzeitinformationen, um Infrastrukturoperationen zu überprüfen, stets über Probleme informiert zu sein und Engpässe zu beheben, bevor diese kritisch werden.

Site Scope stellt verschiedene Werkzeuge bereit, darunter Vorlagen, einen Assistenten zum Veröffentlichen von Vorlagenänderungen und eine automatische Vorlagenbereitstellung. Mit diesen Werkzeugen können Sie einen Standardsatz von Monitortypen und -konfigurationen in einer einzigen Struktur entwickeln. SiteScope-Vorlagen lassen sich im gesamten Unternehmen schnell bereitstellen und aktualisieren, um sicherzustellen, dass die Überwachungsinfrastruktur mit den in der Vorlage festgelegten Standards kompatibel ist.

SiteScope beinhaltet auch Warnungstypen, die Sie zum Kommunizieren und Aufzeichnen von Ereignisinformationen in einer Vielzahl von Medien verwenden können. Sie können Warnungsvorlagen nach den Anforderungen Ihres Unternehmens anpassen.

SiteScope dient auch als Überwachungsgrundlage für andere HP-Produkte wie Business Service Management (BSM), Network Node Manager i (NNMi), HP Software-as-a-Service und LoadRunner/Performance Center. Indem Sie mit SiteScope beginnen und später weitere HP-Lösungen wie Service Level Management von BSM hinzufügen, können Sie eine solide Infrastrukturüberwachung erstellen, mit deren Hilfe Sie Ihre IT-Infrastruktur und Servicelevel aus Unternehmenssicht verwalten können.

SiteScope kann auch zusammen mit HP Operations Manager-Produkten (HPOM) verwendet werden, um so eine leistungsstarke Infrastrukturverwaltung mit agentlosen und agentbasierten Komponenten bereitzustellen. SiteScope-Ziele fungieren als Agent für HPOM und werden den Operations Manager Service-Ansichten automatisch hinzugefügt, sodass HPOM übergangslos SiteScope-Daten und den Überwachungsstatus anzeigen kann. Für die Ereignisintegration werden SiteScope-Warnungen und Statusänderungen der Überwachungsmetriken direkt an HPOM gesendet. Die kombinierten Funktionen der agentlosen und agentbasierten Überwachung bietet eine leistungsstarke und umfassende Überwachungslösung. Weitere Details zur Verwendung von HPOM-Produkten finden Sie in der HPOM-Dokumentation.

Kapitel 2: SiteScope-Editionen

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über SiteScope-Editionen

SiteScope ist in verschieden Editionen mit jeweils unterschiedlichem Funktionsumfang erhältlich.

SiteScope wird mit einer integrierten Lizenz für die **Community**-Edition installiert, mit der für einen unbegrenzten Zeitraum ein eingeschränkter Funktionsumfang genutzt werden kann. Außerdem gibt es eine kostenlose, einmalig verwendbare Testversion, mit der der volle Funktionsumfang von SiteScope während eines Zeitraums von dreißig Tagen zur Verfügung steht.

Um SiteScope über die in der Community-Edition verfügbaren Funktionen hinaus zu erweitern, müssen Sie ein Upgrade auf eine der kommerziellen Editionen ausführen: **Premium**, **Ultimate** oder **System Collector**. Es gibt darüber hinaus eine kostenlose **Lasttest**-Edition, die umgehend nach Installation von HP SiteScope für Lasttests zur Verfügung steht. Die Community-, Premium- und Ultimate-Editionen stehen allen Benutzern zur Verfügung, während die System Collector- und Lasttests-Editionen mit der HP Operations Manager-Integration bzw. HP Load Runner/Performance Center zur Verfügung gestellt werden.

Funktionsumfang und Kapazität von SiteScope lassen sich durch den Import von zusätzlichen Lizenzen erweitern. Das bedeutet, dass Sie eine SiteScope-Bereitstellung ganz flexibel skalieren können, damit diese den Anforderungen Ihres Unternehmens und Ihrer Infrastruktur gerecht wird. Bei Anfragen zum Erwerb von Lizenzen oder zusätzlicher Kapazität wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.

Weitere Informationen über die Lizenzierung finden Sie unter "SiteScope-Lizenzen" auf Seite 29.

Tabelle für den Funktionsvergleich

Die untenstehende Tabelle zeigt die Funktionen, die in den unterschiedlichen SiteScope-Editionen.

Funktion	SiteScope-Editionen			Nur mit HP-Produkten verfügbar	
	Community	**Test**	**Premium/ Ultimate**	**System-Collector**	**Lasttests**
Lizenzdauer	Instant-On (unbefristet)	30 Tage	Befristet oder unbefristet	Befristet oder dauerhaft	Instant-On (unbefristet)
Lizenz-anspruchsmodell	25 OSIs 25 URLs (Festgelegte Kapazität)	25 OSIs 25 URLs 10 Transaktionen (Festgelegte Kapazität)	OSIs, URLs, Transaktionen (Menge vom Benutzer festgelegt)	OSIs (Menge vom Benutzer festgelegt)	25 OSIs 25 URLs (Festgelegte Kapazität)
Knotengesperrt[1]	x	x	✔	✔	x
Supportmodell	SiteScope-Communities	Internet/Telefon	Internet/Telefon	Internet/Telefon	E-Mail
Benutzerkonten	1	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt
Datenrückhaltung	30 Tage [2]	30 Tage [2]	Unbegrenzt	Unbegrenzt	Unbegrenzt
Warnungen	Nur E-Mail, Ereigniskonsole	✔	✔	✔	✔
Reporterstellung	Nur Kurz-Reports	✔	✔	✔	✔
Multi-View, Ereigniskonsole	✔	✔	✔	✔	✔
Analytics	✔	✔	✔	✔	✔
Monitortypen	Alle Monitore bis auf die unter "Nicht in der Community-Edition enthaltene Monitore" auf Seite 17 aufgelisteten Monitore.	Alle Monitore	Alle Monitore	Alle Monitore	Alle Monitore außer Webskript- und Integrations-monitore

Funktion	SiteScope-Editionen			Nur mit HP-Produkten verfügbar	
	Community	**Test**	**Premium/ Ultimate**	**System-Collector**	**Lasttests**
Lösungsvorlagen	x	Alle Lösungsvorlagen	Alle Lösungsvorlagen	Alle Lösungsvorlagen	HP Quality Center, HP QuickTest Professional, HP Service Manager, HP Vertica, Operating System Host (AIX, Linux, Microsoft Windows, Solaris)
Benutzerdefinierte Vorlagen	✔ Außer für die Bereitstellung über CSV- oder XML-Datei	✔	✔	✔	✔
APIs	x	✔	✔	✔	✔
Integrationen	x	✔	✔	✔	Integrationen von generischen Daten
Hochverfügbarkeit (Failover)	x	x	✔	✔	x
Aktualisierungen und Patches	x	x (Aktualisierung über Patches möglich)	✔	✔	✔
Unterstützte Plattformen (Installation)	Verschiedene Windows- und Linux 64-Bit-Plattformen (siehe "Systemanforderungen" auf Seite 74 für eine Liste der unterstützten Versionen).				
Unterstützung einer mehrsprachigen Benutzeroberfläche	10 Sprachen (siehe Liste der unterstützten Sprachen im Abschnitt zur Internationalisierung im SiteScope-Benutzerhandbuch).				

[1] Einige Lizenzeditionen sind knotengesperrt, um Lizenzmissbrauch zu verhindern. Hierbei ist die Lizenz nur auf einem bestimmten Computer gültig.

[2] Das Konfigurieren der Anzahl der täglichen Protokolle in den Protokolleinstellungen wirkt sich nicht auf die Anzahl der aufbewahrten täglichen Protokolle aus.

Nicht in der Community-Edition enthaltene Monitore

- Active Directory-Replikations-Monitor
- Amazon-Webservices-Monitor
- COM+ Server-Monitor
- HP Vertica-JDBC-Monitor
- Integrationsmonitore
- Microsoft Exchange-Monitore - Microsoft Exchange 2007 Message Traffic, Microsoft Exchange, Microsoft Exchange-Basis (nicht mehr unterstützte Monitore: Microsoft Exchange 5.5/2000/2003 Message Traffic, Microsoft Exchange 2003 Mailbox, Microsoft Exchange 2003 Public Folder)
- Microsoft Lync-Monitore - Archivierungsserver, Server für A/V-Konferenzen, Director Server, Edgeserver, Front-End-Server, Vermittlungsserver, Monitoring und CDR Server, Registrierungsserver
- Oracle-Datenbank Lösungsvorlagen - Oracle 10g-Applikationsserver-, Oracle 9i-Applikationsserver-, Oracle-Datenbank-Monitor
- SAP-Monitore - SAP CCMS, SAP CCMS-Warnungen, SAP Java Web Application Server, SAP-Leistung, SAP-Arbeitsprozesse
- Siebel-Monitore - Siebel Applikationsserver, Siebel Protokoll, Siebel Webserver
- VMware-Datenspeicher-Monitor
- VMware Host-Monitore - VMware Host-CPU, VMware Host-Speicher, VMware Host-Netzwerk, VMware Host-Status, VMware Host-Speicher
- WebLogic-Applikationsserver-Monitor
- Webskript-Monitor
- WebSphere-Monitore - WebSphere-Applikationsserver-, WebSphare MQ-Status-, WebSphere Performance Servlet-Monitor

Community-Edition

Die Community-Edition ermöglicht es, kostenlos für einen unbegrenzten Zeitraum auf einige Funktionen von SiteScope zuzugreifen. Diese Edition wird automatisch aktiviert, nachdem eine reguläre SiteScope-Installation durchgeführt wurde.

Hinweis: Die Community-Edition wird nicht mit jeder Minor- oder Minor-Minor-Versionsfreigabe bereitgestellt. Weitere Informationen zu Versionstypen finden Sie unter "Installationsversionstypen" auf Seite 103.

In der Tabelle weiter unten werden einige der Hauptunterschiede zwischen der Community-Edition und den kommerziellen SiteScope-Editionen dargestellt.

Funktion	Beschreibung
Lizenzdauer	**Community-Edition:** Diese Edition läuft niemals ab. Sie kann mit einer beliebigen anderen Edition überschrieben werden, nachdem die Lizenzdatei importiert wurde, und sie wird wieder aktiviert, wenn keine andere kommerzielle Edition vorhanden oder gültig ist. **Kommerzielle Edition:** Befristet oder dauerhaft. Weitere Informationen zu den Folgen des Ablaufs einer kommerziellen Edition finden Sie unter "Lizenzablauf" auf Seite 40.
Kapazität	**Community-Edition:** Die Lizenz hat eine feste Kapazität für die Überwachung von bis zu 25 Betriebssysteminstanzen (OS-Instanzen) und 25 URLs (die Kapazität kann nicht erweitert werden). Wenn diese Kapazität während einer Monitorausführung überschritten wird, werden alle Monitore angehalten und es wird ein Fehler im Protokoll angezeigt. Beispielsweise kann sich die OSi-Kapazitätsnutzung für dynamische VMWare-Monitore während der Ausführung des Monitors je nach der Anzahl der erkannten VMs ändern. **Kommerzielle Edition:** Der Benutzer kann OS-Instanz-, URL- und Transaktionslizenzkapazitäten gemäß den Überwachungsanforderungen erwerben.
Benutzerverwaltung	**Community-Edition:** Ein Benutzerkonto (Administrator). **Kommerzielle Edition:** Unbegrenzte Benutzer, Benutzerrollen und Unterstützung für LDAP-Integration für Authentifizierung und Autorisierung.

Funktion	Beschreibung
Lösungsvorlagen und Monitore	**Community-Edition:** • Lösungsvorlagen und ihre jeweiligen Monitore sind nicht verfügbar. • Die unter "Nicht in der Community-Edition enthaltene Monitore" auf Seite 17 aufgeführten Monitore sind nicht verfügbar. • Alle anderen Monitore stehen zur Verfügung. **Kommerzielle Edition:** Alle Monitore und Lösungsvorlagen sind verfügbar.
Datenrückhaltung	**Community-Edition:** • Historische Überwachungsdaten werden nur für 30 Tage aufbewahrt (Protokolldateien werden jedoch nicht gelöscht). Das Konfigurieren der Anzahl der täglichen Protokolle in den Protokolleinstellungen wirkt sich nicht auf die Anzahl der aufbewahrten täglichen Protokolle aus. • Kurz-Reports zeigen Daten der letzten 30 Tage an. **Kommerzielle Edition**: Unbegrenzt
Warnungsaktionen	**Community-Edition:** Es werden nur Warnungsaktionen per E-Mail- und Ereigniskonsole aktiviert. **Kommerzielle Edition:** Alle Warnungsaktionen werden aktiviert.
APIs	**Community-Edition:** Nicht unterstützt. **Kommerzielle Edition:** Unterstützt
Integrationen	**Community-Edition:** Nicht unterstützt. **Kommerzielle Edition:** Unterstützt
Hochverfügbarkeit (Failover)	**Community-Edition:** Nicht unterstützt. Wenn Sie versuchen, eine Verbindung von SiteScope zu einem SiteScope Failover-Computer unter Verwendung der Community-Edition herzustellen, wird eine Ausnahme vom primären SiteScope- zum Failover-Computer zurückgegeben und auf der Benutzeroberfläche angezeigt. Ferner wird eine entsprechende Nachricht in das Protokoll **error.log** des primären SiteScope-Computers geschrieben. **Kommerzielle Edition:** Unterstützt

Funktion	Beschreibung
Vorlagenbereitstellung	**Community-Edition:** CSV-Vorlagenbereitstellung (über die Benutzeroberfläche) und automatische Vorlagenbereitstellung wird nicht unterstützt. **Kommerzielle Edition:** Vollständig unterstützt
Upgrade	Sie können die Community-Edition auf die Premium-, Ultimate- oder System-Collector-Edition aktualisieren. Weitere Informationen finden Sie unter "Importieren und Aktualisieren Ihrer Lizenz" auf Seite 34.

Testversion

Nachstehend werden die Spezifikationen für die Verwendung der Testversion von SiteScope aufgelistet.

Funktion	Beschreibung
Versionstyp	Eine kostenlose, einmalige Testlizenz.
Versionsdauer	30 Tage
Kapazität	Bei Aktivierung über die Community-Edition umfasst die Testlizenz eine Kapazität für die Überwachung von bis zu 25 OS-Instanzen, 25 URLs und 10 Transaktionen. **Hinweis:** Die Kapazität der Testlizenzen ist fest und kann nicht erweitert oder verlängert werden.
Funktionen	Vollständige SiteScope-Funktionen Weitere Informationen finden Sie unter "Tabelle für den Funktionsvergleich" auf Seite 15.
Knotengesperrt	Nein
Aktivierung	Verfügbar bei Verwendung der Community-Edition, wenn Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen > Testversion** auswählen. Die Testversion kann nur einmal gestartet werden, danach ist die Schaltfläche permanent deaktiviert.
Deaktivieren	Wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus. Wählen Sie in der Tabelle **Installierte Lizenzen** die Zeile **Test** aus und klicken Sie auf **Lizenz entfernen**. SiteScope wird auf die vorherige Edition (oder die Community-Edition) zurückgesetzt, wenn keine anderen Editionen erworben wurden.
Upgrade	Sie können die Testversion durch die Premium- Ultimate- oder System Collector-Edition ersetzen. Weitere Informationen finden Sie unter "Importieren und Aktualisieren Ihrer Lizenz" auf Seite 34.
Ablaufdatum	Die Lizenz läuft automatisch nach 30 Tagen ab und SiteScope kehrt zur Community-Edition zurück. Der Funktionsumfang entspricht nun wieder dem der derzeitig aktiven Lizenzedition.

Kommerzielle Editionen

SiteScope umfasst die folgenden kommerziellen Editionen: In den folgenden Tabellen werden die Spezifikationen für die Verwendung dieser Editionen aufgelistet.

Eine Liste der in den einzelnen Editionen verfügbaren Funktionen finden Sie unter "Tabelle für den Funktionsvergleich" auf Seite 15.

Premium/Ultimate-Edition

Funktion	Beschreibung
Versionstyp	Kommerzielle Edition.
Versionsdauer	Befristet oder dauerhaft
Kapazität	Erwerben Sie die benötigte Kapazität für OSi, URL und Transaktionen (es gibt keine Minimalkapazität). Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.
Funktionen	Vollständige SiteScope-Funktionen
Knotengesperrt	Ja (die Lizenz ist nur auf einem bestimmten Computer gültig)
Aktivierung	Nach dem Lizenzerwerb wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus und geben Sie den Pfad auf Ihre SiteScope-Lizenzdatei in das Feld **Lizenzdatei** ein oder klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie die Lizenzdatei aus.
Deaktivieren	Wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus. Wählen Sie in der Tabelle "Installierte Lizenzen" die Zeile **Premium/Ultimate** aus und klicken Sie auf **Lizenz entfernen**. Wenn Sie eine Lizenz für eine Premium- oder Ultimate-Edition löschen, sollten Sie gleichzeitig auch alle Zeilen mit den zugehörigen Kapazitätstypen (OSi, URL und Transaktion) löschen. SiteScope wird auf die vorherige Version oder die Community-Version zurückgesetzt, wenn keine anderen Versionen erworben werden.
Upgrade	Sie können die Premium-Edition durch die Ultimate- oder System Collector-Edition ersetzen. Weitere Informationen finden Sie unter "Importieren und Aktualisieren Ihrer Lizenz" auf Seite 34.
Ablaufdatum	Eine Lizenz läuft ab, wenn das Ablaufdatum für alle Kapazitätstypen innerhalb der aktiven Edition erreicht wird. SiteScope sendet sieben Tage vor Lizenzablauf eine Nachricht an den Benutzer und zeigt diese Mitteilung auch im Bereich "Lizenzen" an. Bei Ablauf stuft SiteScope die Version (und die Funktionen) automatisch auf die vorherige kommerziellen Version zurück, sofern in der Hierarchie vorhanden. Andernfalls wird die Community-Version die aktive Version.

Funktion	Beschreibung
Kapazitäts-Downgrade	Wenn die OSi-, URL- Transaktionskapazität überschritten wird, geht SiteScope wie folgt vor: 1. Öffnet ein Dialogfeld mit einer Warnmeldung. 2. Senden einer täglichen Meldung (für bis zu 7 Tage), mit der ein Benutzer darauf hingewiesen wird, die Extra-Monitore zu entfernen oder die Lizenzkapazität zu erhöhen. Wenn die Kapazität 7 Tage überschritten wurde, hält SiteScope alle Monitore an.

System Collector-Edition

Funktion	Beschreibung
Versionstyp	Eine SiteScope-Version, die mit der HP Operations Manager-Integration zur Verfügung gestellt wird.
Versionsdauer	Befristet oder dauerhaft
Kapazität	Erwerben Sie die benötigte Kapazität für OSi (es gibt keine Minimalkapazität). Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.
Funktionen	Vollständige SiteScope-Funktionen
Knotengesperrt	Ja (die Lizenz ist nur auf einem bestimmten Computer gültig)
Aktivierung	Nach dem Lizenzerwerb wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus und geben Sie den Pfad auf Ihre SiteScope-Lizenzdatei in das Feld **Lizenzdatei** ein oder klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie die Lizenzdatei aus.
Deaktivieren	Wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus. Wählen Sie in der Tabelle **Installierte Lizenzen** die Zeile **System Collector** aus und klicken Sie auf **Lizenz entfernen**. Wenn Sie eine Lizenz für eine System Collector-Edition löschen, sollten Sie gleichzeitig auch alle Zeilen mit den zugehörigen Kapazitätstypen (OSi, URL und Transaktion) löschen. SiteScope wird auf die vorherige Version oder die Community-Version zurückgesetzt, wenn keine anderen Versionen erworben werden.
Upgrade	Obwohl es nicht möglich ist, eine System Collector-Lizenz zu überschreiben, können Sie eine Lizenz für die Premium- oder Ultimate-Edition, um die URL- und Transaktionskapazität zu erhöhen. Weitere Informationen finden Sie unter "Importieren und Aktualisieren Ihrer Lizenz" auf Seite 34.
Ablaufdatum	Eine Lizenz läuft ab, wenn das Ablaufdatum für die OSi-Kapazität innerhalb der aktiven Edition erreicht wird. SiteScope sendet sieben Tage vor Lizenzablauf eine Nachricht an den Benutzer und zeigt diese Mitteilung auch im Bereich "Lizenzen" an. Bei Ablauf stuft SiteScope die Version (und die Funktionen) automatisch auf die vorherige kommerziellen Version zurück, sofern in der Hierarchie vorhanden. Andernfalls wird die Community-Version die aktive Version.

Funktion	Beschreibung
Kapazitäts-Downgrade	Wenn die OSi-, URL- Transaktionskapazität überschritten wird, geht SiteScope wie folgt vor: 1. Öffnet ein Dialogfeld mit einer Warnmeldung. 2. Senden einer täglichen Meldung (für bis zu 7 Tage), mit der ein Benutzer darauf hingewiesen wird, die Extra-Monitore zu entfernen oder die Lizenzkapazität zu erhöhen. Wenn die Kapazität 7 Tage überschritten wurde, hält SiteScope alle Monitore an.

Lasttests-Edition

Folgende Tabelle enthält die Spezifikationen für die Nutzung der SiteScope Lasttests-Edition in HP LoadRunner oder HP Performance Center.

Funktion	Beschreibung
Versionstyp	Kostenlos erhältliche Version von SiteScope, die mit HP LoadRunner und HP Performance Center zur Verfügung gestellt wird.
Versionsdauer	Unbefristet
Kapazität	25 Betriebssysteminstanzen, 25 URLs **Hinweis:** Diese Lizenz hat eine feste Kapazität, die sich nicht erweitern lässt.
Funktionen	Informationen hierzu finden Sie unter "Tabelle für den Funktionsvergleich" auf Seite 15.
Knotengesperrt	Nein
Aktivierung	Wird automatisch nach der Installation von SiteScope for Load Testing installiert.
Deaktivieren	Die Lizenz für die Lasttests-Edition kann vom Benutzer nicht entfernt werden.
Upgrade	Sie können die Lasttests-Edition auf die Premium-, Ultimate- oder System Collector-Edition aktualisieren. Weitere Informationen finden Sie unter "Importieren und Aktualisieren Ihrer Lizenz" auf Seite 34. **Hinweis:** Für das Upgrade einer Lasttests-Edition sind zusätzliche Konfigurationsschritte erforderlich. Eine Beschreibung finden Sie unter "Aktualisieren einer Lizenz von SiteScope für Lasttests auf die Premium-Edition" auf Seite 37.
Ablaufdatum	Nicht zutreffend (Lizenz ist permanent)
Kapazitäts-Downgrade	Bei Überschreiten der Lizenzkapazität führt SiteScope folgende Aktionen aus: 1. Öffnet ein Dialogfeld mit einer Warnmeldung. 2. Senden einer täglichen Meldung (für bis zu 7 Tage), mit der der Benutzer darauf hingewiesen wird, die zusätzlichen Monitore zu entfernen. Wenn die Kapazität 7 Tage überschritten wurde, hält SiteScope alle Monitore an.

Failover-Edition

Nachstehend werden die Spezifikationen für die Verwendung der SiteScope Failover-Edition aufgelistet.

Funktion	Beschreibung
Versionstyp	SiteScope bietet eine Failover-Unterstützung sowie zusätzliche Redundanz und einen automatischen Ausfallschutz für den Fall, dass bei einem SiteScope-Server Verfügbarkeitsprobleme auftreten. Die Failover-Edition wird mit den Premium, Ultimate- und System-Collector-Editionen ohne Aufpreis bereitgestellt.
Versionsdauer	Für SiteScope Failover ist eine primäre SiteScope-Instanz mit einer Premium-, Ultimate- oder System-Collector-Lizenz erforderlich.
Funktionen	Vollständige SiteScope-Funktionen
Aktivierung	Nach der Installation von SiteScope müssen Sie die Failover-Lizenz importieren. Die Funktion beginnt erst nach der Synchronisierung des Failover-Servers mit einem primären SiteScope-Server (mit einer Premium-, Ultimate- oder System-Collector-Lizenz).
Deaktivieren	Wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** aus. Wählen Sie in der Tabelle **Installierte Lizenzen** die Zeile **Failover** aus und klicken Sie auf **Lizenz entfernen**. Wenn Sie eine Lizenz für eine Failover-Editionslizenz löschen, sollten Sie gleichzeitig auch alle Zeilen mit den zugehörigen Kapazitätstypen (OSi, URL und Transaktion) löschen.
Ablauf-/ Kapazitäts-Downgrade	Für SiteScope Failover ist eine primäre SiteScope-Instanz mit einer Premium-, Ultimate- oder System-Collector-Lizenz erforderlich. Bei Ablauf der primären SiteScope-Editionslizenz läuft auch die Failover-Lizenz ab und es gibt keine aktive Edition auf dem SiteScope Failover-Computer.

Kapitel 3: SiteScope-Lizenzen

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über die SiteScope-Lizenzierung

Die SiteScope-Lizenzierung bestimmt, wie viele Monitore gleichzeitig erstellt werden und welche Monitortypen verwendet werden können. Erwerben Sie den Lizenztyp und die Kapazität je nach den Anforderungen Ihrer Überwachungsumgebung. Wie viele SiteScope-Monitore Sie erstellen können, ist abhängig von zwei Faktoren:

- Von der Überwachungskapazität, die Sie für die jeweiligen Lizenzkapazitätstypen erworben haben (OS-Instanz, URL, Transaktion).
- Welche SiteScope-Monitortypen Sie verwenden wollen.

Mit dem Erwerb einer SiteScope-Lizenz und Registrierung Ihrer SiteScope-Kopie erhalten Sie wichtige Rechte und Berechtigungen. Registrierte Benutzer haben zudem Zugriff auf technischen Support und Informationen zu allen HP-Produkten sowie das Recht auf kostenlose Aktualisierungen und Upgrades.

Außerdem erhalten Sie Zugriff auf die HP-Website zur Software-Unterstützung. Sie können diesen Zugriff für die Suche nach technischen Informationen in der Wissensdatenbank zum Lösen von Softwareproblemen sowie zum Herunterladen von Aktualisierungen der SiteScope -Dokumentation verwenden.

Neues Lizenzmodell für Monitore

Das Lizenzanspruchsmodell von SiteScope wurde von einem punktebasierten Modell in ein Kapazitätsmodell geändert, das davon abhängt, welche Arten von Objekten mit SiteScope überwacht werden. Es gibt drei Arten von Überwachungsobjekten: Betriebssysteminstanzen (OSi), Transaktionen für Monitore, die VuGen-Skripts ausfüren, und URLs.

Welche Lizenzkapazitätstypen zur Verfügung stehen, hängt vom Installationstyp und der gewählten SiteScope-Edition ab. Das bedeutet, dass Sie eine SiteScope-Bereitstellung ganz flexibel skalieren können, damit diese den Anforderungen Ihres Unternehmens und Ihrer Infrastruktur gerecht wird.

Weitere Informationen zur Benutzeroberfläche finden Sie unter:

- "Instant-On-Lizenz" unten
- "Lizenzedition " auf der nächsten Seite
- "Lizenzkapazitätstyp" auf Seite 32

Neues Lizenzmodell für Lösungsvorlagen

Für Lösungsvorlagen sind keine getrennten Lizenzen für jede einzelne Lösung mehr erforderlich. Stattdessen stehen nun mit einer Lizenz für die Premium-, Ultimate- und System Collector-Edition automatisch alle Lösungsvorlagen zur Verfügung. Der Lizenzverbrauch für die Lösungsvorlage hängt davon ab, wie viele Monitore aus der Lösungsvorlagen bereitgestellt werden.

Instant-On-Lizenz

Sie müssen über eine gültige Lizenz verfügen, um SiteScope verwenden zu können. Je nach gewähltem Installationstyp wird die zugehörige Lizenz umgehend aktiviert (Instant-On).

- **HP SiteScope.** Die *Community*-Edition ist nach einer regulären SiteScope-Installation sofort verfügbar. Diese kostenlose Edition ermöglicht es, für einen unbegrenzten Zeitraum auf einige der Funktionen von SiteScope zuzugreifen. Sie können Ihre SiteScope-Edition jederzeit aktualisieren, um die Überwachungsfunktionen der ursprünglichen Bereitstellung zu erweitern und alle Funktionen von SiteScope zu nutzen. Eine der Liste der verfügbaren SiteScope-Editionen finden Sie unter "Lizenzedition " auf der nächsten Seite.
- **HP SiteScope for Load Testing.** Die Lasttests-Edition steht umgehend nach Installation von HP SiteScope for Load Testing zur Verfügung. Dieser Installationstyp wird nur mit der Installation von HP LoadRunner oder HP Performance Center verwendet.

Hinweis: Bei einer SiteScope Failover-Installation steht die Lizenz für die *Failover*-Edition ohne zusätzliche Kosten für die Premium-, Ultimate- und System Collector-Editionen zur Verfügung. Nach der Installation von SiteScope müssen Sie die Failover-Lizenzdatei importieren.

Lizenzedition

Sie können Ihre ursprüngliche SiteScope-Bereitstellung aktualisieren, indem Sie je nach der gewünschten Umgebung, die überwacht werden soll, die entsprechende SiteScope-Edition und das jeweilige Kapazitätsmodell (siehe "Lizenzkapazitätstyp" auf der nächsten Seite) auswählen.

Folgende Editionen stehen zur Auswahl:

Lizenzedition	Beschreibung
Testversion	SiteScope bietet eine kostenlose, einmalige Testlizenz mit allen SiteScope-Funktionen für einen Zeitraum von 30 Tagen. Weitere Informationen finden Sie unter "Testversion" auf Seite 21.
Premium-/ Ultimate-Edition	Bietet alle Funktionen von SiteScope, einschließlich Integrationen, SiteScope-APIs, SiteScope-Failover und ermöglicht die Nutzung von Unternehmensmonitoren und -vorlagen. Die Premium- und Ultimate-Editionen sind funktionell identisch und unterscheiden sich lediglich durch die im Paket enthaltenen Integrationen. Weitere Informationen erhalten Sie bei Ihrem HP-Kundenbetreuer. Weitere Informationen finden Sie unter "Premium/Ultimate-Edition" auf Seite 23.
System-Collector	Eine mit HP Operations Manager Integration bereitgestellte Version von SiteScope, die es ermöglicht, SiteScope-Monitore für HPOM-Applikationen zu verwenden. Weitere Informationen finden Sie unter "System Collector-Edition" auf Seite 25.
Lasttests	Eine mit HP LoadRunner- oder HP Performance Center bereitgestellte SiteScope-Version, mit der Benutzer SiteScope-Monitore in einer LoadRunner- oder Performance Center-Applikation definieren und verwenden können. Weitere Informationen finden Sie unter "Lasttests-Edition" auf Seite 27.

Ein Vergleich der in den einzelnen Editionen verfügbaren Funktionen finden Sie unter "Tabelle für den Funktionsvergleich" auf Seite 15.

Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite. Wenn Sie eine Lizenz besitzen und eine Lizenzschlüsseldatei benötigen, sollten Sie das HP Softwarelizenzierungs-Portal verwenden.

Lizenzkapazitätstyp

Die folgende Tabelle enthält eine Erläuterung zu den unterschiedlichen Kapazitätstypen, die Regeln für die Berechnung der Lizenznutzung sowie die Monitore, die von den einzelnen Kapazitätstypen unterstützt werden:

Kapazitätstyp	Beschreibung
OSi-Lizenz	**Unterstützte Monitore:** Alle Monitore außer URL, URL-Inhalt, URL-Liste, URL-Sequenz, Webskript, Webservice, Linkprüfung und XML-Metriken und kostenlose Monitore (Verbund, Formelverbund, Amazon-Webservices, E-Business-Transaktion und Integrationsmonitore).
	Lizenzverbrauch: In der Regel wird eine OSi-Lizenzinstanz pro überwachtem Remoteserver belegt, unabhängig von der Anzahl der für diesen Remoteserver konfigurierten Monitore. Wenn Sie beispielsweise einen CPU-, Disk Space- und Memory-Monitor auf demselben Betriebssystem oder Host verwenden, wird dadurch eine einzige BS-Instanz der jeweiligen Lizenz verbraucht. **Ausnahmen:** • Benutzerdefinierte Monitore, SNMP-Trap- und Microsoft Windows DFÜ-Monitore verbrauchen eine OS-Instanz für je 15 Monitore. • Der HP Vertica-JDBC-Monitor verbraucht eine OS-Instanz pro überwachtem Server und eine OS-Instanz pro überwachtem Knoten. • Solaris Zones benötigt eine Betriebssysteminstanz für jede überwachte Servereigenschaft und eine Betriebssysteminstanz für jede überwachten Zone. • Der VMware-Datenspeicher-Monitor verwendet eine OS-Instanz pro Datenspeicher. • VMware Host-Monitore belegen eine OS-Instanzlizenz pro überwachtem Host und eine OS-Instanzlizenz für jeden überwachten virtuellen Computer. In den bewährten Vorgehensweisen für VMware wird empfohlen, dass Sie den Objektnamen (in vSphere) eines VM-Gasts entsprechend dem Servernamen oder Computernamen des Gasts festlegen. Wenn Sie die Namen auf diese Weise festlegen, nutzt SiteScope nur eine Betriebssysteminstanz für alle Monitore auf demselben Server. Wenn sich der vSphere-Objektname vom Gastservernamen unterscheidet, verwendet SiteScope eine Betriebssysteminstanz für alle VMware-Monitore mit dem Gastservernamen und eine Betriebssysteminstanz für alle Monitore mit dem vSphere-Objektnamen. **Hinweis:** OS-Instanzen aus verschiedenen Edition, werden nicht aggregiert, da sich die Kosten für eine OS-Instanz-Lizenz für die verschiedenen Editionen unterscheiden. Die OS-Instanzen aus OS-Lizenzen der gleichen Edition werden jedoch aggregiert (wenn Sie beispielsweise über mehrere Lizenzen für die Premium-Edition verfügen und jede OS-Instanzen enthält).

Kapazitätstyp	Beschreibung
URL-Lizenz	**Unterstützte Monitore:** URL, URL-Inhalt, URL-Liste, URL-Sequenz, Webservice, Linkprüfung, XML-Metriken. **Lizenzverbrauch:** • Jeder überwachte URL oder URL-Schritt nutzt eine URL-Lizenzinstanz. • URL-Lizenzen werden zwischen den Editionen aggregiert, ausgenommen sind Community-, Test- und Lasttests-Editionen, die eigene URL-Lizenzen enthalten.
Transaktionslizenz	**Unterstützte Monitore:** Webskript-Monitore, die VuGen-Skripttransaktionen nutzen. **Lizenzverbrauch:** • Es wird eine Transaktionslizenz-Instanz pro VuGen-Skripttransaktion verbraucht. • Transaktionslizenzen werden zwischen den Edition aggregiert; ausgenommen sind die Community- und Lasttests-Editionen, die die Transaktionsüberwachung nicht unterstützen.

Importieren und Aktualisieren Ihrer Lizenz

In der Installation von SiteScope ist eine kostenlose Community-Editionslizenz enthalten.

Wenn Sie SiteScope über die in der Community-Edition enthaltenen Funktionen hinaus erweitern möchten, müssen Sie die SiteScope-Edition mit den Kapazitätstypen (OSi, URL und Transaktion) erwerben, die Sie benötigen, und den Lizenzdateischlüssel in SiteScope importieren.

Sie haben folgenden Möglichkeiten zum Import einer SiteScope-Lizenz:

- Während der Installation mit dem SiteScope-Konfigurationsassistenten
- Nach der Installation mithilfe der Seite der allgemeinen Voreinstellungen (siehe "Importieren von SiteScope-Lizenzen" auf Seite 38), mithilfe einer API oder mit dem SiteScope Konfigurationswerkzeug (siehe "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151).

Wenn Sie eine Versionslizenz importieren, die in der Hierarchie höher gestellt ist, werden die Funktionen der aktiven Version entsprechend der Version der importierten Lizenz aktualisiert. Details zum Aktualisieren einer Lizenz finden Sie unter "Aktualisieren der SiteScope-Versionslizenz" auf Seite 36.

Sie können die Lizenzkapazität für die Premium-, Ultimate- und System-Collector-Version aktualisieren. Weitere Informationen finden Sie unter "Erhöhen der Lizenzkapazität" auf Seite 38.

Aktualisieren der SiteScope-Versionslizenz

Sie können Ihre vorhandene Versionslizenz jederzeit aktualisieren, indem Sie eine Lizenz mit einer höheren Version erwerben.

Durch die Aktualisierung von SiteScope Community auf SiteScope Premium oder Ultimate profitieren Sie von der zusätzlichen Funktion, die in SiteScope zur Verfügung steht. Einen Vergleich des Funktionsumfangs der SiteScope Community-Edition mit anderen Editionen von SiteScope finden Sie unter "Tabelle für den Funktionsvergleich" auf Seite 15.

Sie können Ihre Editionslizenz anhand der folgenden Hierarchie aktualisieren:

Installationstyp	Editionshierachie	Aktualisierung von Edition möglich			Mögliche Kapazitätserweiterung	
		Premium	Ultimate	System-Collector	Transaction/ URL	OSi
SiteScope	Community	✔	✔	✔		
	Test	✔	✔	✔		
	System Collector (Paket)					✔
	Premium		✔	✔	✔	✔
	Ultimate (Paket)			✔	✔	✔
SiteScope für Lasttests[1]	Lasttests	✔				
	Premium				✔	✔
SiteScope-Failover	Failover					
[1] Um die Lizenz für eine Installation von SiteScope für Lasttests auf die Premium-Edition zu aktualisieren, sind zusätzliche Konfigurationsschritte erforderlich (siehe "Aktualisieren einer Lizenz von SiteScope für Lasttests auf die Premium-Edition" auf der nächsten Seite).						

So aktualisieren Sie die Editionslizenz:

1. Erwerben Sie die gewünschte SiteScope-Edition. Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite. Wenn Sie eine Lizenz besitzen und eine Lizenzschlüsseldatei benötigen, sollten Sie das HP Softwarelizenzierungs-Portal verwenden.

2. Importieren Sie die Lizenzdatei. Weitere Informationen finden Sie unter "Importieren von SiteScope-Lizenzen" auf der nächsten Seite.

   Hinweis: Nach dem Upgrade auf SiteScope 11.30 kann es einen Moment dauern, bevor der Bereich **Lizenzierung** mit den aktuellen Lizenzen aktualisiert wird.

Aktualisieren einer Lizenz von SiteScope für Lasttests auf die Premium-Edition

Hinweis: Bei Verwendung einer Installation von SiteScope für Lasttests wird die Integration mit BSM nicht unterstützt.

Wenn Sie die Lizenz einer SiteScope für Lasttests-Installation auf die Premium-Edition aktualisieren, müssen Sie die folgenden Änderungen vornehmen, um die volle Funktionalität der Premium-Edition nutzen zu können:

1. Wählen Sie in SiteScope **Einstellungen > Infrastrukturvoreinstellungen > Benutzerdefinierte Einstellungen** aus, und legen Sie die Werte der folgenden Eigenschaften fest:

   - disableRepeatedSchedules=false
   - disableReports=false
   - MultiViewDashboardEnabled=true

   Hinweis: Alternativ können Sie die Eigenschaften `_disableRepeatedSchedules=true`, `_disableReports=true` und `_MultiViewDashboardEnabled=false` aus der Datei **<SiteScope-Stammverzeichnis>\groups\master.config** entfernen und SiteScope dann neu starten.

2. Starten Sie SiteScope neu.

Erhöhen der Lizenzkapazität

Wie viele SiteScope-Monitore Sie erstellen können, ist abhängig von zwei Faktoren:

- Von der Überwachungskapazität, die Sie für den jeweiligen Lizenzkapazitätstyp erworben haben (OS-Instanz, URL, Transaktion).
- Welche SiteScope-Monitortypen Sie verwenden wollen.

Sie können die Lizenzkapazität für die Premium-, Ultimate- und System-Collector-Edition aktualisieren, je nach den Anforderungen Ihrer Überwachungsumgebung. Die Test-, Community- und Lasttests-Editionen verfügen über eine feste Kapazität, die nicht erhöht werden kann.

Hinweis: Beim Erwerb und Import von zusätzlichen Kapazitäten:

- Der OSi-Kapazitätstyp gilt nur für die aktuelle Edition. Die Lizenzkapazität wird nicht mit der OSi-Kapaziät aus früheren Editionen aggregiert.
- Der URL-Kapazitätstyp wird mit der URL-Kapazität aus vorherigen Editionen aggregiert, wenn er in die aktuelle Premium-, Ultimate- oder System-Collector-Edition importiert wird.
- Der Transaktionskapazitätstyp wird mit der Transaktionskapazität aus vorherigen Editionen aggregiert, wenn er in die aktuelle Premium-, Ultimate- oder System-Collector-Edition importiert wird.

So erhöhen Sie die Lizenzkapazität:

1. Erwerben Sie die erforderliche OS-Instanz-, URL- und Transaktionskapazität. Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.
2. Importieren Sie die Lizenzdatei. Weitere Informationen finden Sie unter "Importieren von SiteScope-Lizenzen" unten.

Importieren von SiteScope-Lizenzen

Sobald Sie Ihre Lizenzdatei von HP erhalten, importieren Sie den Lizenzschlüssel über die SiteScope-Benutzeroberfläche in SiteScope.

So importieren Sie eine Lizenz in SiteScope:

1. Öffnen Sie über einen Webbrowser die SiteScope-Instanz, die Sie ändern möchten. Der SiteScope-Dienst bzw. -Prozess muss gerade ausgeführt werden.

2. Wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen** aus und erweitern Sie den Bereich **Lizenzen**.

3. Geben Sie den Pfad der SiteScope-Lizenzdatei in das Feld **Lizenzdatei** ein oder klicken Sie auf die Schaltfläche **Auswählen** und wählen Sie die Lizenzdatei aus.

4. Klicken Sie auf **Importieren**. Nachdem die Lizenz erfolgreich importiert wurde, werden Informationen über die importierte Lizenz in der Tabelle der installierten Lizenzen aufgeführt. Dazu gehören die Lizenzversion, der Kapazitätstyp und die Details (verfügbare, verbrauchte und verbleibende Kapazität), Ablaufdatum und der Lizenzstatus.

   Hinweis: Nach dem Upgrade auf SiteScope 11.30 kann es einen Moment dauern, bevor der Bereich **Lizenzierung** mit den aktuellen Lizenzen aktualisiert wird.

Lizenzablauf

Ablauf der Editionslizenz

Bei zeitlich befristeten Lizenzen sendet SiteScope eine Warnungsmeldung sieben Tage vor Ablauf der Lizenz an die Benutzer.

Wenn eine Editionslizenz abläuft, wird die Lizenz automatisch auf die vorher gültige Lizenz in der Editionshierarchie heruntergestuft (siehe "Aktualisieren der SiteScope-Versionslizenz" auf Seite 36). Andernfalls wird die Community-Edition die aktive Version. Es kann auch vorkommen, dass ein Benutzer die Lizenz entfernt.

Die SiteScope-Funktionen werden sofort entsprechend der Funktionen, die mit der aktiven Editionsdefinition verfügbar sind, reduziert.

Hinweis: Ein Benutzer kann nicht die Community- oder Lasttests-Editionslizenz aus der Tabelle der installierten Lizenzen unter **Voreinstellungen > Allgemeine Voreinstellungen > Lizenzen** entfernen.

Kapazitätslizenz läuft ab

Wenn die Kapazität einer OSi-, URL- Transaktionslizenz überschritten wird, geht SiteScope wie folgt vor:

1. Es wird ein Dialogfeld mit einer Warnmeldung geöffnet.
2. Der Benutzer erhält eine Nachricht, dass die Lizenzkapazität überschritten wurde. SiteScope sendet sieben Tage lang täglich eine Nachricht.

Wenn der Benutzer die zusätzlichen Monitore nicht entfernt oder die Lizenzkapazität innerhalb dieses Zeitraums nicht erhöht, hält SiteScope alle Monitore an, auch die Monitortypen, für die die Kapazität nicht überschritten wurde. Wenn Monitore angehalten werden, können Sie weiterhin Monitore aus SiteScope entfernen.

Herunterstufen auf die Community-Lizenz

Wenn eine kommerzielle Lizenz abläuft und keine andere kommerzielle Editionslizenz vorliegt oder gültig ist, wird die Community-Edition automatisch zur aktiven Lizenz. Alle Funktionen, die nicht in der Community-Edition unterstützt werden, werden sofort deaktiviert.

In der Tabelle weiter unten wird gezeigt, wie sich ein Herunterstufen der Lizenz auf die Funktionen auswirkt:

Funktion	Beschreibung
Monitore	Wenn die Lizenzkapazität der Community-Editionslizenz überschritten wird, werden alle Monitore angehalten und es wird eine Meldung auf der Benutzeroberfläche angezeigt. Alle erstellten Monitore, die in der Community-Edition nicht zulässig sind, werden angehalten und deaktiviert (z. B. Unternehmensmonitore und Amazon-Webservices-Monitor).
Benutzerkonten	Benutzer können sich nicht mehr mit anderen Benutzerkonten anmelden (regulär oder mit LDAP) oder andere Benutzerkonten bearbeiten. Dies gilt nicht für das SiteScope-Administratorkonto.
Datenrückhaltung	Während alle täglichen Protokolle auf dem System behalten werden, können Benutzer Report- und Analysedaten nur für die letzten 30 Tage anzeigen.
Warnungen	Warnungsaktionen, die nicht in der Community-Edition zulässig sind, werden angehalten und deaktiviert (es sind nur Warnungsaktionen über E-Mail und die Ereigniskonsole zulässig).
Reports	Geplante Reports werden nicht gesendet und nur Kurz-Reports können über die Benutzeroberfläche aktiviert werden.
APIs	Alle öffentlichen und privaten SiteScope-APIs werden blockiert.
Integrationen	Alle Integrationen werden angehalten und deaktiviert.
SiteScope-Failover	SiteScope Failover erhält eine Fehlermeldung und beendet das Synchronisieren von Daten aus der primären SiteScope-Instanz.

Hinweise und Einschränkungen zur Lizenzierung

Community-Edition

Die Community-Edition wird nicht mit jeder Minor- oder Minor-Minor-Versionsfreigabe bereitgestellt. Weitere Informationen zu Versionstypen finden Sie unter "Installationsversionstypen" auf Seite 103.

SiteScope-Integration in BSM

- Wenn SiteScope für den Versand von Daten an BSM konfiguriert wurde und Ihre SiteScope-Lizenz abläuft, beendet SiteScope den Versand aller Daten (einschließlich Topologiedaten) an BSM. Nachdem Sie die SiteScope-Lizenz erneuert haben, müssen Sie das Kontrollkästchen **Alle Anmeldungen bei Business Service Management deaktivieren** unter **Voreinstellungen > Integrationsvoreinstellungen > BSM-Integration > Haupteinstellungen für BSM-Integration**

deaktivieren, um Protokollierung und Datenübertragung an BSM wieder zu aktivieren, da diese von SiteScope bei Ablauf der Lizenz automatisch deaktiviert werden.

- Wenn Sie in SiteScope einen Monitor löschen, nachdem Ihre Lizenz für SiteScope Premium, Ultimate oder System Collector abgelaufen ist (und deshalb die Integration mit BSM deaktiviert wurde), wird der Monitor nicht aus BSM entfernt. Sie müssen den Monitor in BSM unter **RTSM Administration > IT Universe Manager** manuell aus der Ansicht **SiteScope Topology Upgrade Compliancy** entfernen.

Kapitel 4: Roadmap für die ersten Schritte

Dieses Kapitel enthält eine grundlegende und ausführliche Roadmap für Ihre ersten Schritte mit SiteScope.

1. **Registrieren Sie Ihre Kopie von SiteScope.**

   Registrieren Sie Ihre Kopie von SiteScope, um Zugriff auf technischen Support und Informationen zu allen HP-Produkten zu erhalten. Ihnen stehen auch Aktualisierungen und Upgrades zu. Sie können Ihre SiteScope-Kopie auf der HP-Website zur Software-Unterstützung registrieren.

2. **Erfahren Sie, wo Sie Hilfe bekommen.**

   Informieren Sie sich über Möglichkeiten der Unterstützung, z.B. Services und HP Software-Support sowie die SiteScope-Hilfe.

3. **Planen Sie Ihre SiteScope-Bereitstellung.**

   Erstellen Sie vor der Installation der SiteScope-Software einen vollständigen Bereitstellungsplan. Verwenden Sie "Bereitstellungsmethodik und -planung" auf Seite 45 zur Unterstützung. Weiter gehende Informationen zu bewährten Methoden bei der Bereitstellungsplanung erhalten Sie beim zuständigen HP-Mitarbeiter.

4. **Installieren Sie SiteScope.**

   Grundlegende Informationen zu den für die Bereitstellung der SiteScope-Applikation erforderlichen Schritten finden Sie unter "Übersicht über die Installation" auf Seite 72. Informationen zur sicheren Bereitstellung von SiteScope finden Sie unter "Optimieren der Sicherheit der SiteScope-Plattform" auf Seite 181.

5. **Melden Sie sich bei SiteScope an und starten Sie die Systemverwaltung.**

   Melden Sie sich mit einem Webbrowser an der Weboberfläche von SiteScope an. Verwenden Sie die Prüfliste unter "Verwaltung nach der Installation" auf Seite 237 als Leitfaden für grundlegende Plattform- und Monitorverwaltungsaufgaben, um SiteScope für die Bereitstellung im Betrieb vorzubereiten.

6. **Stellen Sie SiteScope den Unternehmens- und Systembenutzern zur Verfügung.**

   Nachdem das SiteScope-System mit definierten Benutzern und eingehenden Monitordaten eingerichtet wurde, können Sie damit beginnen, Unternehmens- und Systembenutzern den Zugriff

auf und die Verwendung der SiteScope-Monitore sowie der Report- und Warnungsfunktionen zu erläutern.

Vollständige Details zur Verwendung und Verwaltung von SiteScope finden Sie in der SiteScope-Hilfe.

Kapitel 5: Bereitstellungsmethodik und -planung

Dieses Kapitel umfasst die folgenden Themen:

Eine Methodik für die Überwachung von Unternehmenssystemen

Für die Bereitstellung von SiteScope ist Ressourcenplanung, der Entwurf einer Systemarchitektur und eine gut durchdachte Bereitstellungsstrategie erforderlich. Dieses Kapitel gibt einen Überblick über die Methodik und Überlegungen, die für eine erfolgreiche Bereitstellung und Verwendung von SiteScope erforderlich sind.

Hinweis: Die unten stehenden Informationen sind Ihnen bei den Vorbereitungen vor Beginn der Installation behilflich. Tiefer gehende Informationen zu bewährten Methoden bei der Bereitstellungsplanung erhalten Sie beim zuständigen Mitarbeiter von HP Professional Services.

Eine konsistente Methodik ist wesentlich, um eine effektive Systemüberwachung zu gewährleisten. Es ist jedoch nicht immer klar, wie der Ansatz für eine Lösung zur Überwachung in Unternehmen sowie deren Entwicklung und Bereitstellung aussehen sollte. Die Lösung muss die Rolle der IT-Infrastruktur und deren Beitrag am Erfolg des Unternehmens berücksichtigen. Die Systemüberwachung ist ein Werkzeug zur Gewährleistung der Verfügbarkeit und Funktion von Diensten, die vom Unternehmen zur Erreichung der wichtigsten Zielvorgaben verwendet werden. Nachfolgend finden Sie einige Richtlinien für die Planung der Systemüberwachung.

Was überwacht werden sollte

Für ein effektives Unternehmenssystemmanagement ist ein mehrstufiger Überwachungsansatz erforderlich. SiteScope bietet Ihnen die dazu erforderlichen Werkzeuge. Auf einer Ebene können Sie einzelne Hardwareelemente in der Infrastruktur überwachen, um zu gewährleisten, dass diese ausgeführt werden und verfügbar sind. Als Ergänzung können Sie wichtige Dienste und Prozesse auf diesen Systemen überwachen. Dazu gehören systemnahe Betriebssystemprozesse sowie Prozesse, die auf den Zustand und die Leistung wichtiger Applikationen schließen lassen. Darüber hinaus soll eine Transaktionsüberwachung von Geschäftsprozessen erstellt werden, um zu gewährleisten, dass wichtige Applikationen und Dienste verfügbar sind und erwartungsgemäß funktionieren.

Welcher Schwellenwert ein Ereignis darstellt

Die Verfügbarkeit und Leistung von Informationssystemen ist wesentlich für den Unternehmenserfolg. Die Schwellenwerte, die Sie für Monitore festlegen, richten sich nach der Art des Systems oder Geschäftsprozesses, das bzw. der überwacht wird.

Wie häufig das System überprüft werden sollte

Die Häufigkeit, mit der ein System überprüft wird, kann ebenso wichtig sein wie der von Ihnen festgelegte Ereignisschwellenwert. Die Verfügbarkeit unternehmenskritischer Informationssysteme sollte während der Zeiten, in denen der Zugriff möglich ist, regelmäßig überprüft werden. In vielen Fällen müssen System rund um die Uhr an allen Wochentagen verfügbar sein. Sie bestimmen, wie häufig SiteScope ein System überprüft, indem Sie für jeden Monitor die **Häufigkeit** einstellen. Ein zu großer Zeitraum zwischen den Überprüfungen kann dazu führen, dass Probleme zu spät erkannt werden. Eine zu häufige Überprüfung kann ein bereits stark ausgelastetes System unnötig überlasten.

Welche Aktionen bei Entdecken eines Ereignisses durchzuführen sind

Als Überwachungsapplikation gibt Ihnen SiteScope die erforderlichen Werkzeuge an die Hand, um Probleme zu erkennen. Mithilfe von SiteScope-Warnungen können Sie eine rechtzeitige Benachrichtigung senden, wenn eine Ereignisschwelle ausgelöst wurde. Eine E-Mail-Benachrichtigung ist eine verbreitete Warnungsaktion. SiteScope beinhaltet weitere Warnungstypen, die mit anderen Systemen kombiniert werden können.

Sie können ein Eskalationsschema für Warnungen entwickeln, indem Sie mehrere Warnungsdefinitionen mit unterschiedlichen Warnungsauslösungskriterien festlegen. Mithilfe der

Warnungseinstellungen in **When** können Sie die Beziehung zwischen erkannten Ereignissen und Warnungsaktionen anpassen.

Eine weitere Ereignisaktion kann darin bestehen, die Überwachung und Warnung für Systeme zu deaktivieren, die von einem nicht mehr verfügbaren System abhängig sind. Mithilfe der SiteScope-Optionen für die Gruppierung und Überwachung von Abhängigkeiten können Sie eine Überlappungsserie von Warnungen verhindern.

Welche Antworten automatisiert erfolgen können

Werden Probleme erkannt, ist eine automatisierte Antwort zur Problemlösung ideal. Dies ist nicht für alle Systeme möglich, doch der Script Alert-Typ von SiteScope bietet ein flexibles, leistungsstarkes Werkzeug zur Automatisierung von Fehlerbehebungsaktionen in einer Vielzahl von Situationen. Überlegen Sie, welche möglicherweise in Ihrer Umgebung auftretenden Probleme sich über eine automatisierte Antwort beheben lassen.

Infrastrukturbewertung von Unternehmenssystemen

1. Sammeln Sie Informationen zu technischen und Unternehmensanforderungen, bevor Sie Entscheidungen zu Architektur und Bereitstellung treffen. Dieses Stadium umfasst folgende Aktionen:

   - Erstellen Sie eine Liste aller zu überwachenden Unternehmensapplikationen. Diese sollte End-to-End-Dienste wie Auftragsverarbeitung, Kontozugriffsfunktionen, Datenabfragen, Aktualisierungen und Report-Generierung berücksichtigen.

   - Erstellen Sie eine Liste der Server, die die Unternehmensapplikationen unterstützen. Diese muss Server enthalten, die Front-End-Weboberflächen, Back-End-Datenbanken und Applikationsserver unterstützen.

   - Erstellen Sie eine Liste der Netzwerkgeräte, die die Unternehmensapplikationen unterstützen. Dazu gehören Netzwerkappliances und Authentifizierungsdienste.

   - Identifizieren Sie zu überwachende Taktelemente. Taktelemente sind Dienste, die als grundlegende Indikatoren für die Verfügbarkeit eines bestimmten Unternehmenssystems oder einer Ressource dienen.

   - Entwerfen Sie Monitorvorlagen, die die zu überwachenden Ressourcen für die einzelnen Systeme darstellen.

2. Identifizieren Sie die wichtigsten Beteiligten und Projektleistungen der Unternehmenssystemüberwachung. Zu den Projektleistungen gehören:
   - Welche Reports generiert werden sollen.
   - Welche Warnungsaktionen bei der Erkennung von Ereignissen durchgeführt werden sollen.
   - An wen Warnungen gesendet werden sollen.
   - Welche Benutzer Anzeige- und Verwaltungszugriff auf SiteScope benötigen.
   - Welche SiteScope-Elemente für welche Beteiligte zugänglich sein müssen.
   - Wie die Schwellenwerte für etwaige Vereinbarungen zum Servicelevel (SLA) lauten (falls anwendbar).
3. Machen Sie sich mit den Beschränkungen vertraut, denen die Ausführung der Systemüberwachungsfunktion unterliegt. Dazu gehören Einschränkungen der Protokolle, die verwendet werden können, Benutzerauthentifizierungsanforderungen, der Zugriff auf Systeme mit unternehmenskritischen Daten sowie Einschränkungen des Netzwerkverkehrs.

SiteScope-Serverdimensionierung

Die Grundlage einer erfolgreichen Überwachungsbereitstellung besteht in der richtigen Dimensionierung des Servers, auf dem SiteScope ausgeführt werden soll. Die Serverdimensionierung ist von verschiedenen Faktoren abhängig:

- Die Anzahl der Monitorinstanzen, die auf der SiteScope-Installation ausgeführt werden sollen.
- Die durchschnittliche Ausführungsfrequenz der Monitore.
- Die zu überwachenden Protokoll- und Applikationstypen.
- Wie viele Monitordaten zur Report-Erstellung auf dem Server verbleiben müssen.

Ausgangspunkt für die Schätzung der Anzahl benötigter Monitore bildet die Kenntnis der Anzahl von Servern in der Umgebung, der jeweiligen Betriebssysteme und der zu überwachenden Applikation.

Eine Tabelle mit Empfehlungen zur Serverdimensionierung auf der Grundlage von Schätzungen der Anzahl auszuführender Monitore finden Sie unter "Anpassen von SiteScope auf Windows-Plattformen" auf Seite 57 bzw. unter "Anpassen von SiteScope auf Linux-Plattformen" auf Seite 60.

Netzwerkstandort und -umgebung

Ein Großteil der SiteScope-Überwachung erfolgt über die Emulation von Web- oder Netzwerkclients, die Anforderungen an Server und Applikationen der Netzwerkumgebung senden. Aus diesem Grund muss SiteScope auf Server, Systeme und Applikationen im gesamten Netzwerk zugreifen können. Dies hilft bei der Entscheidung, wo SiteScope installiert werden sollte.

Die von SiteScope verwendeten Methoden zur Überwachung von Systemen, Servern und Applikationen lassen sich in zwei Kategorien unterteilen:

- **Standardbasierte Netzwerkprotokolle.** Dazu gehören HTTP, HTTPS, SMTP, FTP und SNMP.
- **Plattformspezifische Netzwerkdienste und -befehle.** Dazu gehören NetBIOS, telnet, rlogin und Secure Shell (SSH).

Die Überwachung der Infrastruktur beruht auf plattformspezifischen Diensten. Als agentlose Lösung erfordert die Überwachung, dass SiteScope immer wieder bei zahlreichen Servern in der Infrastruktur angemeldet und authentifiziert werden muss. Aus Leistungs- und Sicherheitsgründen sollte SiteScope innerhalb derselben Domäne und so nah wie möglich an den zu überwachenden Systemelementen bereitgestellt werden. Außerdem ist es ratsam, dass sich SiteScope im selben Subnet befindet wie der entsprechende Netzwerkauthentifizierungsdienst (z. B. Active Directory, NIS oder LDAP). Der Zugriff auf sowie die Verwaltung von SiteScope kann nach Bedarf remote über HTTP oder HTTPS erfolgen.

Hinweis: Stellen Sie SiteScope möglichst nicht an einem Standort bereit, an dem ein beträchtlicher Anteil der Überwachungsaktivität die Kommunikation über ein Wide Area Network (WAN) erfordert.

Tipp: Aus Sicherheitsgründen ist davon abzuraten, SiteScope zur Überwachung von Servern über eine Firewall zu verwenden, da für die Überwachung der Serververfügbarkeit verschiedene Protokolle und Ports erforderlich sind. Die SiteScope-Lizenzierung ist nicht serverbasiert und unterstützt separate SiteScope-Installationen für beide Seiten einer Firewall. Über HTTP oder HTTPS kann von einer Workstation aus simultan auf zwei oder mehrere SiteScope-Installationen zugegriffen werden.

Überlegungen für Windows-Umgebungen

SiteScope muss über ein Konto mit Administratorberechtigungen installiert werden. Außerdem wird empfohlen, den SiteScope-Dienst über ein Benutzerkonto auszuführen, das über

Administratorberechtigungen verfügt. Ein lokales Systemkonto kann verwendet werden, wirkt sich jedoch auf die Konfiguration von Verbindungsprofilen für Windows-Remoteserver aus.

SiteScope verwendet außerdem die Windows-Leistungsindikatoren auf Remotecomputern zur Überwachung von Serverressourcen und -verfügbarkeit. Zum Aktivieren dieser Überwachungsfunktion muss der Remoteregistrierungsdienst für die Remote-Computer aktiviert werden.

Überlegungen für Linux-Umgebungen

SiteScope muss vom Root-Benutzer in einer Linux-Umgebung installiert werden. Nachdem SiteScope installiert wurde, können Sie ein Nicht-Root-Benutzerkonto mit den Berechtigungen zum Ausführen von SiteScope erstellen (sofern der SiteScope-Webserver nicht auf einem privilegierten Port ausgeführt wird; in diesem Fall sollte die Ausführung durch den Root-Benutzer erfolgen). Details zum Konfigurieren eines Nicht-Root-Benutzers mit Berechtigungen zum Ausführen von SiteScope finden Sie unter "Konfigurieren eines Nicht-Root-Benutzerkontos mit Berechtigungen zum Ausführen von SiteScope" auf der nächsten Seite.

Im Folgenden finden Sie zusätzliche Informationen zur Einrichtung einer agentlosen Überwachung von UNIX-Remoteservern mit SiteScope.

- **Remoteanmeldekonto-Shells.** SiteScope kann als Applikation unter den gängigsten UNIX-Shells erfolgreich ausgeführt werden. Wenn SiteScope mit einem UNIX-Server kommuniziert, wird die Kommunikation mit Bourne-Shell (sh) oder tsch-Shell bevorzugt. Das entsprechende Anmeldekonto auf den jeweiligen UNIX-Remoteservern sollte deshalb so eingerichtet sein, dass seine Shell eine dieser Shells verwendet.

  Hinweis: Legen Sie das Shell-Profil nur für die Anmeldekonten fest, die von SiteScope für die Kommunikation mit dem Remotecomputer verwendet werden. Andere Applikationen und Konten auf dem Remotecomputer können ihre aktuell definierten Shells verwenden.

- **Kontoberechtigungen.** Unter Umständen müssen Befehlsberechtigungseinstellungen für die Überwachung von UNIX-Remoteservern aufgelöst werden. Die meisten Befehle, die von SiteScope zum Abrufen von Serverinformationen von einem UNIX-Remoteserver ausgeführt werden, befinden sich im Verzeichnis **/usr/bin** auf dem Remoteserver. Einige Befehle, darunter der Befehl zum Abrufen von Arbeitsspeicherinformationen, befinden sich in **/usr/sbin**. Der Unterschied zwischen diesen beiden Speicherorten besteht darin, dass **/usr/sbin**-Befehle gewöhnlich für Stammbenutzer oder sehr privilegierte Benutzer reserviert sind.

> **Hinweis:** Obwohl SiteScope umfassende Kontoberechtigungen erfordert, wird aus Sicherheitsgründen davon abgeraten, SiteScope über das Stammkonto auszuführen oder für die Verwendung von Stammanmeldekonten auf Remoteservern zu konfigurieren.

Bei Problemen mit Berechtigungen müssen Sie entweder dafür sorgen, dass sich SiteScope als ein anderer Benutzer mit Berechtigungen zum Ausführen des Befehls anmeldet, oder die Berechtigungen für das von SiteScope verwendete Benutzerkonto ändern.

Konfigurieren eines Nicht-Root-Benutzerkontos mit Berechtigungen zum Ausführen von SiteScope

SiteScope muss von einem Root-Benutzerkonto in einer Linux-Umgebung installiert werden. Nachdem SiteScope installiert wurde, können Sie ein Nicht-Root-Benutzerkonto mit Berechtigungen zum Ausführen von SiteScope erstellen.

> **Hinweis:** Auch wenn SiteScope umfassende Kontoberechtigungen erfordert, um die gesamte Bandbreite der Serverüberwachung zu ermöglichen, wird davon abgeraten, SiteScope aus dem Stammkonto auszuführen oder SiteScope für die Verwendung des Stammkontos für den Zugriff auf Remoteserver zu konfigurieren.

So erstellen Sie ein Nicht-Root-Benutzerkonto mit Berechtigungen zum Verwenden von SiteScope:

1. Fügen Sie einen neuen Benutzer hinzu: `useradd newuser`
2. Ändern Sie die Berechtigungen für den SiteScope-Installationsordner: `chmod 755 /opt/HP/SiteScope/ -R`
3. Ändern Sie den Besitzer des SiteScope-Installationsordners: `chown newuser /opt/HP/SiteScope/ -R`
4. Melden Sie sich als der neue Benutzer an: `su newuser`
5. Navigieren Sie zum Installationsordner: `cd /opt/HP/SiteScope`
6. Führen Sie SiteScope aus: `./start`

> **Hinweis:** Um die Integration von HP Operations Manager-Ereignissen und -Metriken zu ermöglichen, muss der HP Operations Agent auf dem SiteScope-Computer unter demselben

Benutzer wie in SiteScope ausgeführt werden, d. h. als Nicht-Root-Benutzer. Details finden Sie im Abschnitt zum Konfigurieren eines Agenten für die Ausführung unter einem alternativen Benutzer unter UNIX im "HP Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide".

Kapitel 6: Anpassen von SiteScope

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über das Anpassen von SiteScope

Da die standardmäßige SiteScope-Konfiguration die Ausführung unzähliger Monitore ermöglicht, ist möglicherweise bei der SiteScope-Installation eine Dimensionierung des Servers erforderlich, um optimale Leistung zu erzielen. Da jede Konfiguration anders ist, sollten Sie den SiteScope-Kapazitätsrechner verwenden, um zu überprüfen, ob für Ihre Konfiguration eine Dimensionierung erforderlich ist.

Die angemessene Dimensionierung des Servers, auf dem SiteScope ausgeführt werden soll, bildet die Grundlage einer erfolgreichen Überwachungsbereitstellung. Zur Gewährleistung der optimalen Dimensionierung empfiehlt HP nachdrücklich die Verwendung der folgenden SiteScope-Serverumgebung:

- SiteScope wird als eigenständiger Server ausgeführt. Um beste Ergebnisse zu erzielen, sollte SiteScope das einzige Programm sein, das auf einem Server ausgeführt wird. BSM, BMC, HP LoadRunner, Datenbanken, Webserver usw. sollten sich nicht auf dem SiteScope-Server befinden.
- Es gibt nur eine Instanz von SiteScope, die auf einem Server ausgeführt wird. Das Ausführen mehrerer Instanzen von SiteScope auf einem Server kann zu ernsthaften Ressourcenproblemen führen. Die Empfehlung schließt auch für System Health verwendete SiteScope-Instanzen ein.
- SiteScope-Failover muss genau wie der primäre SiteScope-Server dimensioniert werden.

SiteScope-Kapazitätsrechner

SiteScope umfasst ein Werkzeug, mit dem Sie das Verhalten Ihres Systems vorhersagen und die Kapazitätsplanung für SiteScope durchführen können. Sie geben die CPU- und Speicherdetails des Systems ein, unter dem SiteScope ausgeführt wird, sowie die Anzahl der Monitore des jeweiligen Typs und die Häufigkeit, mit der sie ausgeführt werden sollen. Der Rechner zeigt dann die erwartete CPU- und Speichernutzung für jeden Monitortyp sowie die Systemanforderungen für die angegebene Arbeitslast an. Auf diese Weise können Sie feststellen, ob Sie Ihre Konfiguration noch optimieren sollten.

Hinweis: Der SiteScope-Kapazitätsrechner wird nur bei Ausführung von SiteScope auf Windows-Versionen und für die unter "Unterstützte Monitore und Lösungsvorlagen" auf Seite 56 aufgelisteten 64-Bit-Monitore und Lösungsvorlagen unterstützt.

So verwenden Sie den SiteScope-Kapazitätsrechner:

1. Schätzen Sie vor der Verwendung des Kapazitätsrechners die Auslastung des SiteScope-Servers ab und verwenden Sie die Empfehlungen zu Systemanforderungen in diesem Handbuch, um Ihren Hardwarebedarf zu ermitteln.

   Weitere Informationen finden Sie unter "Systemhardwareanforderungen" auf Seite 74.

2. Öffnen Sie den SiteScope-Kapazitätsrechner unter:

   - SiteScope-Installationsordner: **<SiteScope-Stammverzeichnis>\tools\SiteScopeCapacityCalculator.xls**
   - Die HP-Website zur Software-Unterstützung.

3. Wählen Sie abhängig vom verwendeten Betriebssystem, unter dem SiteScope installiert ist, die Registerkarte für die Monitornutzung aus. Beachten Sie, dass SiteScope 11.30 ausschließlich 64-Bit-Betriebssysteme unterstützt.

4. Geben Sie im Abschnitt für die Anforderungen die folgenden Informationen ein:

   - Durchschnittliche CPU-Nutzung in Prozent
   - CPU-Typ
   - Heap-Größe des Speichers (in MB)

- Wählen Sie für eine 64-Bit-Installation TRUE aus, wenn SiteScope mit BSMintegriert ist. Wählen Sie FALSE für eine eigenständige SiteScope-Installation.

5. Geben Sie im Abschnitt für Monitore die Anzahl der Monitore des jeweiligen Typs sowie die Aktualisierungsrate für jeden Monitor ein.

6. Die Ergebnisse und Empfehlungen werden im Abschnitt für Ergebnisse und Empfehlungen angezeigt. Eine Abweichung von 30 bis 40 Prozent der tatsächlichen Ergebnisse von den erwarteten Ergebnissen liegt im Toleranzbereich.

Unterstützte Monitore und Lösungsvorlagen

Die folgenden Monitore und Lösungsvorlagen werden vom SiteScope-Kapazitätsrechner unterstützt:

Monitore.

- CPU
- Datenbankindikator
- Datenbankabfrage (nur 64-Bit-Version)
- Verzeichnis-Monitor (nur 64-Bit-Version)
- Speicherplatz
- DNS-Monitor
- Datei-Monitor (nur 64-Bit-Version)
- JMX-Monitor (nur 64-Bit-Version)
- Protokolldatei-Monitor (nur 32-Bit-Version)
- Speicher-Monitor
- Microsoft IIS Server-Monitor
- Microsoft SQL Server-Monitor (nur 32-Bit-Version)
- Microsoft Windows-Ereignisprotokollmonitor (nur 32-Bit-Version)
- Microsoft Windows-Ressourcen-Monitor
- Ping-Monitor
- SAP CCMS-Monitor (nur 32-Bit-Version)
- Service-Monitor
- Siebel Applikationsserver-Monitor (nur 32-Bit-Version)
- SNMP by MIB Monitor
- UNIX-Ressourcen-Monitor (nur 64-Bit-Version)
- URL-Monitor
- URL Listen-Monitor (nur 64-Bit-Version)
- WebLogic-Applikationsserver-Monitor (nur 32-Bit-Version)
- Webservice-Monitor (nur 64-Bit-Version)
- WebSphere Applikationsserver-Monitor (nur 32-Bit-Version)

Lösungsvorlagen:

- Microsoft Exchange 2003 Lösungsvorlage (nur 32-Bit-Version)
- Siebel-Lösungsvorlagen (nur 32-Bit-Version)

Hinweis: Die anderen 32-Bit-Monitore von SiteScope werden nicht mehr unterstützt und funktionieren nach einer Aktualisierung auf SiteScope 11.30 nicht mehr. Weitere Informationen finden Sie unter "Migrieren von 32-Bit- auf 64-Bit-SiteScope" auf Seite 88.

Anpassen von SiteScope auf Windows-Plattformen

Wenn Sie eine SiteScope-Installation auf einer Windows-Plattform dimensionieren wollen, sollten Sie die folgenden Dimensionierungsschritte an SiteScope und am Windows-Betriebssystem durchführen:

1. **Dimensionieren Sie SiteScope.**

   Sie sollten zunächst SiteScope dimensionieren und dann für mindestens 24 Stunden laufen lassen, bevor Sie mit dem nächsten Schritt fortfahren. Details finden Sie im Verfahren "Anpassen von SiteScope" unten.

2. **Optimieren Sie das Windows-Betriebssystem.**

   Wenn Sie SiteScope dimensioniert und mindestens 24 Stunden gewartet haben, müssen Sie das Windows-Betriebssystem optimieren und den SiteScope-Server dann neu starten, damit die Parameteränderungen wirksam werden. Details finden Sie im Verfahren "Optimieren des Microsoft Windows-Betriebssystems" auf der nächsten Seite.

3. **Allgemeine Wartungsempfehlungen.**

   Zusätzliche sollten einige allgemeine Wartungsempfehlungen befolgt werden, um die bestmögliche Optimierung zu gewährleisten. Weitere Informationen finden Sie unter "Allgemeine Wartungsempfehlungen" auf Seite 59.

Hinweis:

- Sie sollten Sicherungen aller Dateien bzw. Parameter erstellen, die Sie ändern, damit Sie diese ggf. aus der Sicherung wiederherstellen können.
- Sollten die Einstellungen nicht effektiv sein, ist es nicht ratsam, diese willkürlich herauf- oder herabzusetzen. Weitere Informationen zu Analyse und Problembehebung erhalten Sie bei der HP Software-Unterstützung.

Anpassen von SiteScope

Die Dimensionierung von SiteScope beinhaltet das Überprüfen von Monitoren, die die Option **Fehler überprüfen** nur falls unbedingt erforderlich verwenden. Diese Option sollte nur für eine kleine Zahl von Monitoren verwendet werden sowie für Monitore, bei denen es bereits falsche **Keine Daten**-Warnungen

aufgrund von Netzwerkproblemen oder Serverlastproblemen auf dem überwachten Remotecomputer gab.

Ist dieses Feature aktiviert, wird ein ausgefallener Monitor direkt wieder ausgeführt. Damit wird der Scheduler umgangen, bevor die Warnungsbedingungen überprüft wurden. Eine große Zahl dieser zusätzlichen Ausführungen kann zu einer beträchtlichen Störung des Schedulers und damit zu einer Verschlechterung der Leistung von SiteScope führen. Bei Monitoren, die aufgrund von Verbindungsproblemen ausfallen, kann das Überprüfen auf Fehler solange dauern wie die Zeitüberschreitung bei der Verbindung, bevor der Monitor beendet wird. In diesem Zeitraum werden Monitorthread und Verbindung standardmäßig für zwei Minuten gesperrt. Diese Verzögerung kann dazu führen, dass andere Monitore warten müssen und der ausgefallene Monitor übersprungen wird.

So dimensionieren Sie SiteScope:

1. Wechseln Sie für jeden Monitor zur Registerkarte **Eigenschaften**, öffnen Sie den Ausschnitt **Einstellungen für Monitorausführung** und überprüfen Sie, ob **Fehler überprüfen** ausgewählt ist. Deaktivieren Sie das Kontrollkästchen für Monitore, die diese Option nicht erfordern.

   Tipp: Bei mehreren Monitoren empfiehlt sich die Verwendung von **Globales Suchen und Ersetzen** für diese Aufgabe.

2. Führen Sie SiteScope mindestens 24 Stunden lang aus, bevor Sie das Windows-Betriebssystem optimieren.

Optimieren des Microsoft Windows-Betriebssystems

Um das Microsoft Windows-Betriebsystem zu optimieren, muss mithilfe des Konfigurationswerkzeug eine Reihe von Parametern geändert werden. Zusätzliche sollten einige allgemeine Wartungsempfehlungen befolgt werden, um die bestmögliche Optimierung zu gewährleisten.

So optimieren Sie Microsoft Windows-Betriebssysteme:

1. Führen Sie das Konfigurationswerkzeug aus und wählen Sie die Option **Anpassen** aus.

   Mit diesem Werkzeug wird die JVM-Heap-Größe auf 4096 MB, die Desktop-Heap-Größe auf 8192 KB und die Anzahl der Dateihandles auf 18.000 erhöht. Außerdem werden Popupwarnungen für ausführbare SiteScope-Dateien deaktiviert. Weitere Informationen finden Sie unter "Ausführen des Konfigurationswerkzeugs auf Windows-Plattformen" auf Seite 151.

   Hinweis: Das Konfigurationswerkzeug bietet nur Unterstützung für den standardmäßigen

SiteScope-Dienstnamen. Wenn Sie den Dienstnamen geändert haben, setzen Sie sich mit dem HP Software-Support in Verbindung, anstatt das Konfigurationswerkzeug auszuführen.

2. Starten Sie den SiteScope-Server neu, damit die Parameteränderungen übernommen werden.
3. Konfigurieren Sie nach Bedarf die übrigen Parameter in Zusammenhang mit der Dimensionierung unter **Voreinstellungen > Infrastrukturvoreinstellungen**.

Tipp: Um eine optimale Leistung zu erreichen, wird empfohlen, die Standardwerte für diese Einstellungen zu verwenden.

Allgemeine Wartungsempfehlungen

Folgen Sie bei der Dimensionierung von SiteScope unter Windows den allgemeinen Wartungsempfehlungen.

- **Bestimmen Sie eine geeignete Monitorhäufigkeit.**

  Überprüfen Sie die Häufigkeit der Monitorausführung und stellen Sie sicher, dass die Monitore in einem geeigneten Intervall ausgeführt werden. So müssen beispielsweise die meisten Monitore zur Überwachung von Datenträgern nicht alle fünf Minuten ausgeführt werden. Im Allgemeinen sind Intervalle von 15, 30 oder sogar 60 Minuten für alle Volumes geeignet. Ausnahmen bilden u. U. die Volumes `/var`, `/tmp` und `swap`. Durch die Reduzierung der Monitorhäufigkeit wird die Anzahl von Monitorausführungen pro Minute herabgesetzt und damit die Leistung und Kapazität verbessert.

- **Optimieren Sie die Gruppenstruktur.**

  Bei der Gruppenstruktur sollte die einfache Verwendbarkeit mit SiteScope sowie die Leistungsoptimierung für SiteScope berücksichtigt werden. Idealerweise sollte die Anzahl übergeordneter Gruppen ebenso wie die Strukturtiefe möglichst klein gehalten werden.

  Die Leistung kann abnehmen, wenn eine Gruppenstruktur über mehr als 50 übergeordnete Gruppen und eine Tiefe von mehr als fünf Ebenen verfügt.

- **Lösen Sie SiteScope-Konfigurationsfehler auf.**

  Verwenden Sie die Monitore zur Überwachung des Zustands, um Monitorkonfigurationsfehler aufzulösen. Auch eine geringe Anzahl von Fehlern kann zu Leistungs- und

Stabilitätsverschlechterungen führen. Weitere Informationen zur Auflösung dieser Fehler erhalten Sie beim HP Software Support.

- **Planen Sie den physischen Standort der SiteScope-Server.**

  SiteScope-Server sollten physisch so nah wie möglich an den zu überwachenden Computern im lokalen Netzwerk positioniert werden. Es wird davon abgeraten, Überwachungen über eine WAN-Verbindung durchzuführen, auch wenn dies in einigen Fällen, in denen die Verbindung über genügend Kapazität und eine niedrige Latenz verfügt, akzeptabel sein kann.

Anpassen von SiteScope auf Linux-Plattformen

Die Dimensionierung von SiteScope Linux-Betriebssystemen beinhaltet die Änderung einer Reihe von Parametern. Zusätzliche sollten einige allgemeine Wartungsempfehlungen befolgt werden, um die bestmögliche Optimierung zu gewährleisten.

1. **Optimieren Sie das Betriebssystem.**

   Konfigurieren Sie die entsprechende Anzahl von Threads für die SiteScope-Instanz und konfigurieren Sie die Parameter für das Linux-Betriebssystem. Details finden Sie im Verfahren "Optimieren des Betriebssystems" unten.

2. **Optimieren Sie die Java Virtual Machine.**

   Konfigurieren Sie JVM-Heap-Größe und Threadstapelgröße und implementieren Sie die parallele automatische Speicherbereinigung. Details finden Sie im Verfahren "Optimieren der Java Virtual Machine" auf Seite 62.

3. **Allgemeine Wartungsempfehlungen.**

   Zusätzliche sollten einige allgemeine Wartungsempfehlungen befolgt werden, um die bestmögliche Optimierung zu gewährleisten. Weitere Informationen finden Sie unter "Allgemeine Wartungsempfehlungen" auf Seite 63.

Optimieren des Betriebssystems

Das Optimieren des Betriebssystems beinhaltet das Konfigurieren der entsprechenden Anzahl von Monitoren für die SiteScope-Instanz sowie das Konfigurieren der Parameter für das Linux-Betriebssystem.

Konfigurieren der maximalen Anzahl an ausgeführten Monitoren

Sie können die Einstellung **Max. Anzahl der Monitorausführungen** unter **Voreinstellungen > Infrastrukturvoreinstellungen > Server-Einstellungen** konfigurieren. Details finden Sie im Abschnitt zu den Voreinstellungen unter "Verwenden von SiteScope" in der SiteScope-Hilfe.

Tipp: Um eine optimale Leistung zu erreichen, wird empfohlen, den Standardwert für diese Einstellung zu verwenden.

Konfigurieren von Parametern für das Linux-Betriebssystem

Das Linux-Betriebssystem bietet Unterstützung für eine große Anzahl von Threads. Führen Sie zum Aktivieren dieses Features folgende Schritte auf dem SiteScope-Server aus.

So konfigurieren Sie die Parameter für das Linux-Betriebssystem:

1. **Ändern Sie die Dateideskriptorlimits des Kernels.**

   a. Bearbeiten Sie die Datei **/etc/system** und fügen Sie die folgende Zeile hinzu:

   ```
   set rlim_fd_max=8192
   ```

   Hinweis: Bei `1024` handelt es sich um den Standardwert (das Limit gilt nicht für Benutzer mit `Root`-Rechten). Der Wert `8192` ist auch für die größte SiteScope-Instanz ausreichend. Verwenden Sie diesen hohen Wert, anstatt mit niedrigeren Werten zu experimentieren. Dadurch vermeiden Sie, den Computer später neu starten zu müssen, falls der niedrige Werte nicht ausreichend ist.

   b. Starten Sie den Server neu.

2. **Ändern Sie die Laufzeitlimits für Benutzer.**

   a. Fügen Sie im Verzeichnis **<SiteScope-Stammverzeichnis>\bin** den SiteScope-Startskripts **start-monitor** und **start-service** folgende Zeile hinzu:

   ```
   ulimit -n 8192
   ```

   b. Überprüfen Sie, ob die folgenden Parameter die folgenden Mindestwerte haben. Wenden Sie sich an Ihren UNIX-Systemadministrator, um weitere Informationen zu erhalten.

Parameter	Mindestwert
core file size (blocks)	Unbegrenzt
data seg size (kbytes)	Unbegrenzt
file size (blocks)	Unbegrenzt
open files	8192
pipe size (512 bytes)	10
stack size (kbytes)	8192
cpu time (seconds)	Unbegrenzt
max user processes	8192
virtual memory (kbytes)	Unbegrenzt

Sie müssen die SiteScope-Applikation bzw. den Server nach dem Ändern der Laufzeitlimits nicht neu starten.

Optimieren der Java Virtual Machine

Für eine optimale Leistung sollten Sie die JVM wie folgt konfigurieren.

So konfigurieren Sie die JVM:

1. **Vergrößern Sie den Heap-Speicher.**

   Standardmäßig ist der Java-Heap-Speicher für SiteScope auf 512 MB festgelegt. Dies ist für den normalen Betrieb großer Instanzen nicht ausreichend.

   Der Heap-Speicher lässt sich auf bis zu 4.096 MB vergrößern (dies ist die empfohlene Heap-Größe für große Auslastungen), indem Sie die Skripts **start-service** und **start-monitor** im Verzeichnis **<SiteScope-Stammverzeichnis>\bin** ändern.

   Wir empfehlen, die minimale Heap-Größe auf den Maximalwert zu setzen, um einen optimalen Systemstart von SiteScope zu ermöglichen. Ändern Sie also beispielsweise `-Xmx4096m –Xms512m` in `-Xmx4096m –Xms4096m`.

2. **Verringern Sie die Threadstapelgröße (-Xss).**

Jeder von SiteScope erstellte Thread instanziiert einen Stapel mit der Menge -Xss an zugewiesenem Speicher. Der Standard für die maximale Threadstapelgröße von UNIX JRE, -Xss, beträgt 512 KB Speicher pro Thread.

Sofern in der Java-Befehlszeile in **<SiteScopeStammverzeichnis>\bin\start-monitor** nicht anders angegeben, wird der Standardwert für die maximale Threadstapelgröße verwendet. Die Standardgröße kann zu einer Beschränkung der Anzahl von Threads führen, wenn der verfügbare Speicher überschritten wird.

Instanzen mit 4000 oder mehr Monitoren können von einem -Xss-Wert von 128 KB profitieren.

Allgemeine Wartungsempfehlungen

Es gibt allgemeine Wartungsempfehlungen für die Dimensionierung von SiteScope auf Linux-Plattformen.

- **Verwenden Sie Zustandsmonitore.**

  Verwenden Sie nach Möglichkeit Zustandsmonitore mit der Option **Abhägig von**, vor allem für Monitore, die UNIX-Remoteverbindungen verwenden. Der Zustandsmonitor kann eine Verschlechterung der Serverleistung verhindern, indem er erkennt, ob mehrere Computer nicht mehr verfügbar sind und SSH-Verbindungsthreads sperren.

- **Minimieren Sie die Verwendung des Features Fehler überprüfen.**

  Ist dieses Feature im Ausschnitt **Einstellungen für Monitorausführung** aktiviert, wird ein ausgefallener Monitor direkt wieder ausgeführt. Damit wird der Scheduler umgangen, bevor die Warnungsbedingungen überprüft wurden. Eine große Zahl dieser zusätzlichen Ausführungen kann zu einer beträchtlichen Störung des Schedulers und damit zu einer Verschlechterung der Leistung von SiteScope führen. Bei Monitoren, die aufgrund von Verbindungsproblemen ausfallen, kann das Überprüfen auf Fehler solange dauern wie die Zeitüberschreitung bei der Verbindung, bevor der Monitor beendet wird. In diesem Zeitraum werden Monitorthread und Verbindung standardmäßig für zwei Minuten gesperrt. Diese Verzögerung kann dazu führen, dass andere Monitore warten müssen und der ausgefallene Monitor übersprungen wird.

- **Verwenden Sie SSH und interne Java-Bibliotheken.**

  Verwenden Sie nach Möglichkeit die Option für SSH und Internal Java Libraries, wenn Sie eine Remoteeinstellung mit einer SSH-Verbindungsmethode definieren. Bei Internal Java Libraries handelt es sich um den Java-basierten SSH-Client eines Drittanbieters. Der Client trägt zu einer

wesentlichen Verbesserung der Leistung und Skalierbarkeit über Telnet und den SSH-Client des Hostbetriebssystems bei. Der Client unterstützt SSH1, SSH2, Public Key Authentication etc.

Vergewissern Sie sich, dass das Verbindungscaching aktiviert ist (erweitern Sie im Dialogfeld "Neuer Microsoft Windows-Remoteserver/UNIX-Remoteserver bearbeiten" den Eintrag **Erweiterte Einstellungen** und deaktivieren Sie die Option **Verbindungscache deaktivieren**). Die Einstellung **Verbindungslimit** sollte so angepasst werden, dass alle Monitore, die für einen bestimmten Server ausgeführt werden, rechtzeitig ausgeführt werden können.

- **Bestimmen Sie eine geeignete Monitorhäufigkeit.**

  Überprüfen Sie die Häufigkeit der Monitorausführung und stellen Sie sicher, dass die Monitore in einem geeigneten Intervall ausgeführt werden. So müssen beispielsweise die meisten Monitore zur Überwachung von Datenträgern nicht alle fünf Minuten ausgeführt werden. Im Allgemeinen sind Intervalle von 15, 30 oder sogar 60 Minuten für alle Volumes geeignet. Ausnahmen bilden u. U. die Volumes "/var", "/tmp" und der Auslagerungsbereich. Durch die Reduzierung der Monitorhäufigkeit wird die Anzahl von Monitorausführungen pro Minute herabgesetzt und damit die Leistung und Kapazität verbessert.

- **Optimieren Sie die Gruppenstruktur.**

  Bei der Gruppenstruktur sollte die einfache Verwendbarkeit mit SiteScope sowie die Leistungsoptimierung für SiteScope berücksichtigt werden. Idealerweise sollte die Anzahl übergeordneter Gruppen ebenso wie die Strukturtiefe möglichst klein gehalten werden.

  Die Leistung kann abnehmen, wenn eine Gruppenstruktur über mehr als 50 übergeordnete Gruppen und eine Tiefe von mehr als fünf Ebenen verfügt.

- **Lösen Sie SiteScope-Konfigurationsfehler auf.**

  Verwenden Sie die Monitore zur Überwachung des Zustands, um Monitorkonfigurationsfehler aufzulösen. Auch eine geringe Anzahl von Fehlern kann zu Leistungs- und Stabilitätsverschlechterungen führen. Weitere Informationen zur Auflösung dieser Fehler erhalten Sie beim HP Software Support.

- **Planen Sie den physischen Standort der SiteScope-Server.**

  SiteScope-Server sollten physisch so nah wie möglich an den zu überwachenden Computern im lokalen Netzwerk positioniert werden. Bei der Überwachung über WAN oder langsame Netzwerkverbindungen wird das Netzwerk gewöhnlich zum Engpass. Dies kann einen zusätzlichen Zeitaufwand für die Ausführung der Monitore bedeuten. Es wird davon abgeraten, Überwachungen

über eine WAN-Verbindung durchzuführen, auch wenn dies in einigen Fällen, in denen die Verbindung über genügend Kapazität und eine niedrige Latenz verfügt, akzeptabel sein kann.

- **Verwenden Sie lokale Benutzerkonten.**

  Lokale Benutzerkonten werden bei der UNIX-Remoteauthentifizierung Verzeichnisdienstkonten vorgezogen. Lokale Benutzerkonten vermeiden die Abhängigkeit von einem Verzeichnisdienstserver für die Authentifizierung. Dadurch wird eine schnelle Authentifizierung gewährleistet und verhindert, dass es beim Ausfall des Verzeichnisdienstservers zu Verbindungsausfällen kommt.

  In einigen Fällen können sich sehr große Instanzen von SiteScope negative Auswirkungen auf die Leistung des Verzeichnisdienstservers haben. Dieser Server sollte sich in physischer Nähe zu den überwachten Servern befinden.

Fehlerbehebung und Einschränkungen

Problem: JVM stürzt ab, und es wird eine Fehlermeldung angezeigt, die besagt, dass der Auslagerungsbereich nicht ausreicht.

Sie können einen durch mangelnden Auslagerungsbereich verursachten Fehler folgendermaßen ermitteln:

1. Erstellen Sie einen Microsoft Windows-Ressourcen-Monitor, um den Zähler für virtuelle Byte auf dem SiteScope-Zielserver zu überwachen.
2. Konfigurieren Sie die folgenden Schwellenwerteinstellungen:

   Fehler, falls >= 7,9 GB

   Warnung, falls >= 7,8 GB

   (Erreicht der Wert 8 GB, stürzt der Prozess ab)

Lösung:

1. Reduzieren Sie die JVM-Heap-Größe. Details zur Änderung der JVM-Heap-Größe finden Sie unter "Ausführen des Konfigurationswerkzeugs auf Windows-Plattformen" auf Seite 151.
2. Reduzieren Sie die Anzahl der von SiteScope verwendeten Threads, indem Sie die Anzahl der parallel ausgeführten Monitore reduzieren (in **Voreinstellungen > Infrastrukturvoreinstellungen > Server-Einstellungen > Max. Monitorprozesse**).

Kapitel 7: Grundlegende Informationen zur agentlosen Überwachung

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über die Funktionen der SiteScope-Monitore

In diesem Abschnitt wird das Konzept der agentlosen Überwachung von SiteScope vorgestellt. Agentlose Überwachung bedeutet, dass die Überwachung ohne die Bereitstellung von Agentensoftware auf den zu überwachenden Servern erfolgen kann. Dies macht die Bereitstellung und Wartung von SiteScope im Vergleich zu anderen Leistungs- oder Betriebsüberwachungslösungen relativ einfach. Im Gegensatz zu agentbasierten Überwachungsansätzen führt SiteScope dank folgender Faktoren zu einer Reduzierung der Gesamtbetriebskosten:

- Sammlung detaillierter Leistungsdaten für Infrastrukturkomponenten.
- Es ist kein zusätzlicher Arbeitsspeicher und keine zusätzliche CPU-Leistung auf Produktionssystemen mehr erforderlich, um einen Überwachungsagenten auszuführen.
- Reduzierung von Zeit- und Kostenaufwand für Wartung durch die Konsolidierung aller Überwachungskomponenten auf einem zentralen Server.
- Produktionssysteme müssen nicht mehr offline geschaltet werden, um den entsprechenden Überwachungs-Agenten zu aktualisieren.
- Überwachungsagenten müssen nicht mehr angepasst werden, um mit anderen Agenten ausgeführt werden zu können.
- Reduzierung der Installationszeit, da Produktionsserver nicht mehr physisch aufgesucht werden müssen und kein Warten auf Softwareverteilungsoperationen erforderlich ist.
- Reduzierung der Wahrscheinlichkeit, dass ein instabiler Agent einen Systemausfall auf einem Produktionsserver verursacht.

SiteScope ist eine vielseitige Betriebsüberwachungslösung, die viele verschiedene Monitortypen für die Überwachung von Systemen und Diensten auf mehreren Ebenen bereitstellt. Viele der Monitortypen können für besondere Umgebungen weiter angepasst werden.

Unternehmen und Organisationen müssen häufig mehrere Lösungen bereitstellen und warten, um Operationen und Verfügbarkeit auf diesen verschiedenen Ebenen zu überwachen. Die Betriebsüberwachung lässt sich in verschiedene Ebenen bzw. Schichten unterteilen, wie in der folgenden Tabelle erläutert:

Monitortyp	Beschreibung
Serverzustand	Überwacht Servercomputerressourcen wie CPU-Auslastung, Arbeitsspeicher, Speicherplatz sowie den Status wichtiger Prozesse und Dienste.
Webprozess und -inhalt	Überwacht die Verfügbarkeit wichtiger URLs, die Funktion wichtiger webbasierter Prozesse und wichtige Textinhalte.
Applikationsleistung	Überwacht Leistungsstatistiken für unternehmenskritische Applikationen wie Webserver, Datenbanken und andere Applikationsserver.
Netzwerk	Überwacht Verbindungen und die Verfügbarkeit von Diensten.

Grundlegende Informationen zur agentenlosen Überwachungsumgebung

Ein Großteil der SiteScope-Überwachung erfolgt über die Emulation von Web- oder Netzwerkclients, die Anforderungen an Server und Applikationen der Netzwerkumgebung senden. Aus diesem Grund muss SiteScope auf Server, Systeme und Applikationen im gesamten Netzwerk zugreifen können.

Dieser Abschnitt umfasst die folgenden Themen:

- "SiteCcope-Überwachungsmethoden" unten
- "Firewalls und SiteScope-Bereitstellung" auf Seite 69

SiteCcope-Überwachungsmethoden

Die von SiteScope verwendeten Methoden zur Überwachung von Systemen, Servern und Applikationen lassen sich in zwei Kategorien unterteilen:

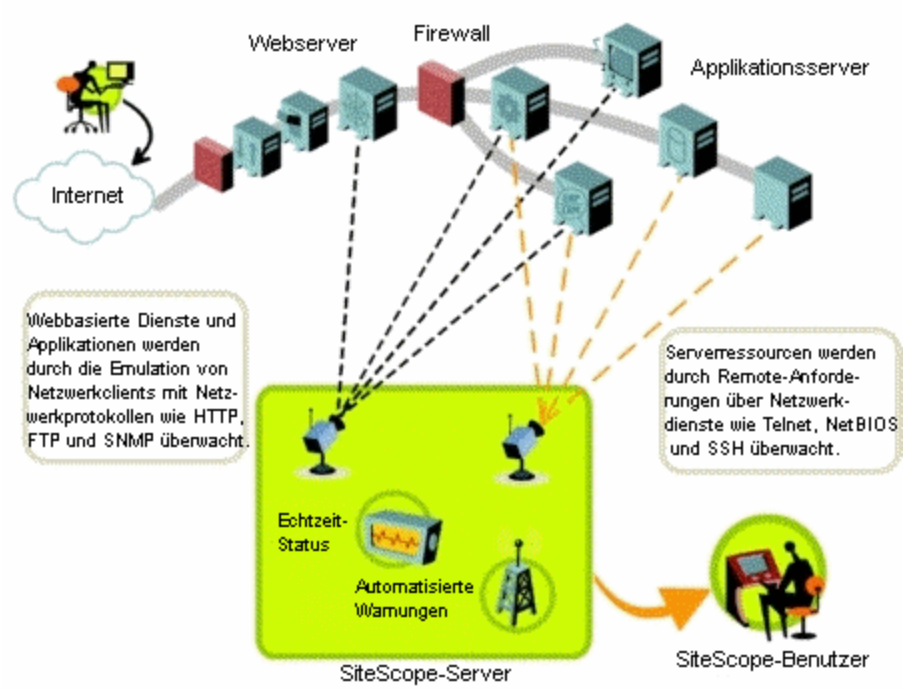
- **Standardbasierte Netzwerkprotokolle.**

  Diese Kategorie umfasst die Überwachung über HTTP, HTTPS, FTP, SMTP, SNMP und UDP. Diese Monitortypen sind im Allgemeinen unabhängig von der Plattform oder dem Betriebssystem, unter dem SiteScope ausgeführt wird. So kann beispielsweise eine SiteScope-Installation unter Linux Webseiten, Dateidownloads, E-Mail-Übertragungen und SNMP-Daten auf Servern unter Windows, HP-UX und Solaris überwachen.

- **Plattformspezifische Netzwerkdienste und -befehle.**

  Diese Kategorie umfasst Monitortypen, die sich als Client bei einem Remotecomputer anmelden und Informationen anfordern. So kann SiteScope beispielsweise Telnet oder SSH verwenden, um sich an einen Remote-Server anzumelden und Informationen zu Speicherplatz, Arbeitsspeicher oder Prozessen anzufordern. Auf der Microsoft Windows-Plattform verwendet SiteScope außerdem Windows-Leistungsindikatorenbibliotheken. Bei der betriebssystemübergreifenden Überwachung gibt es für Monitortypen, die auf plattformspezifische Dienste angewiesen sind, einige Einschränkungen.

  Die folgende Abbildung zeigt eine allgemeine Übersicht über die agentlose Überwachung mit SiteScope. SiteScope-Monitore senden Anforderungen an Dienste auf Remotecomputern, um Daten zu Leistung und Verfügbarkeit zu sammeln.



SiteScope-Server-Monitore (z. B. CPU, Disk Space, Memory, Service) können zur Überwachung von Serverressourcen auf den folgenden Plattformen verwendet werden: Windows, AIX, CentOS, FreeBSD, HP iLO, HP-UX, HP/UX, HP/UX64-bit, Linux, MacOSX, NonStopOS, OPENSERVER, Red Hat Enterprise Linux, SCO, SGI Irix, Solaris Zones, Sun Fire X64 ILOM, Sun Solaris, SunOS, Tru64 5.x,Tru64 Pre 4.x (Digital) und Ubuntu Linux.

Hinweis: Für die Überwachung von Serverressourcen (z. B. CPU-Auslastung, Arbeitsspeicher) auf Windows-Computern von einem SiteScope-Server unter UNIX ist eine SSH-Verbindung erforderlich. Auf allen Windows-Computern, die auf diese Weise überwacht werden sollen, muss ein Secure Shell-Server installiert sein. Weitere Informationen zum Aktivieren dieser Funktion finden Sie im Abschnitt zur SiteScope-Überwachung mit Secure Shell (SSH) im Kapitel "Verwenden von SiteScope" der SiteScope-Hilfe.

SiteScope beinhaltet eine Adapterkonfigurationsvorlage, mit deren Hilfe Sie SiteScope-Funktionen erweitern können, um andere Versionen des UNIX-Betriebssystems zu überwachen. Weitere Informationen finden Sie unter "Adapter für das Betriebssystem UNIX" in der SiteScope-Hilfe.

Sie müssen Anmeldekonten auf allen Servern aktivieren, auf deren Systemdaten SiteScope remote zugreifen soll. Das Anmeldekonto auf den überwachten Servern muss wie das Konto konfiguriert sein, unter dem SiteScope installiert wurde und ausgeführt wird. Wird SiteScope beispielsweise unter einem Konto mit dem Benutzernamen **sitescope** ausgeführt, müssen für Remoteanmeldekonten auf Servern, die von dieser SiteScope-Installation überwacht werden sollen, Benutzeranmeldekonten für den **sitescope**-Benutzer konfiguriert werden.

Firewalls und SiteScope-Bereitstellung

Aus Sicherheitsgründen ist davon abzuraten, SiteScope zur Überwachung von Servern über eine Firewall zu verwenden, da für die Überwachung der Server verschiedene Protokolle und Ports erforderlich sind. Die SiteScope-Lizenzierung unterstützt separate SiteScope-Installationen auf beiden Seiten einer Firewall. Über HTTP oder HTTPS kann von einer Workstation aus simultan auf zwei oder mehrere SiteScope-Installationen zugegriffen werden.

Die folgende Tabelle enthält eine Liste der Ports, die im Allgemeinen von SiteScope für die Überwachung und Warnungen in einer typischen Überwachungsumgebung verwendet werden:

SiteScope-Funktion	Verwendeter Standardport
SiteScope-Webserver	Port 8080
SiteScope-Reports	Port 8888
FTP-Monitor	Port 21

SiteScope-Funktion	Verwendeter Standardport
Mail-Monitor	Port 25 (SMTP), 110 (POP3), 143 (IMAP)
News-Monitor	Port 119
Ping-Monitor	ICMP-Pakete
SNMP-Monitor	Port 161 (UDP)
URL-Monitor	Port 80,443
Remote Windows Monitoring	Port 139
E-Mail-Warnung	Port 25
Post Alert	Port 80,443
SNMP Trap Alert	Port 162 (UDP)
Remote UNIX ssh	Port 22
Remote UNIX Telnet	Port 23
Remote UNIX rlogin	Port 513

Berechtigungen und Anmeldeinformationen für Monitore

Für den Zugriff auf die einzelnen Monitore sind Benutzerberechtigungen und Anmeldeinformationen erforderlich. Weitere Informationen zu den erforderlichen Anforderungen und Anmeldeinformationen sowie zu dem von den jeweiligen Monitoren verwendeten Protokoll finden Sie unter "Berechtigungen und Anmeldeinformationen für Monitore" in der SiteScope-Hilfe.

Teil 2: Vor dem Installieren von SiteScope

Kapitel 8: Übersicht über die Installation

SiteScope ist auf einem einzelnen Server installiert und wird als einzelne Applikation auf Windows-Plattformen oder als einzelne Applikation oder Mehrfachprozess auf Linux-Plattformen ausgeführt.

Vor der Installation von SiteScope sollten Sie einige Planungsschritte und Aktionen berücksichtigen, um die Bereitstellung und Verwaltung Ihrer Überwachungsumgebung zu vereinfachen.

Im Folgenden finden Sie eine Übersicht der zur Bereitstellung der SiteScope-Applikation erforderlichen Schritte.

1. **Bereiten Sie einen Server vor, auf dem die SiteScope-Applikation installiert und ausgeführt werden soll.**

   Hinweis:

   - Es wird empfohlen, nicht mehr als eine SiteScope-Installation auf einem einzigen Computer zu installieren.
   - Wenn Sie planen, SiteScope Failover für die Verfügbarkeit der Sicherungsüberwachung im Fall eines SiteScope-Serverfehlers zu verwenden, finden Sie weitere Informationen im HP SiteScope Failover Guide unter **<SiteScope-Stammverzeichnis>\sisdocs\pdfs\SiteScopeFailover.pdf**.

2. **Besorgen Sie sich die ausführbare SiteScope-Installationsdatei.**

   Weitere Informationen finden Sie unter "Installationsablauf" auf Seite 104.

3. **Erstellen Sie ein Verzeichnis, in dem die Applikation installiert wird, und legen Sie die erforderlichen Benutzerberechtigungen fest.**

   Hinweis: Sie müssen ein neues Verzeichnis für die Installation von SiteScope 11.30 erstellen. Installieren Sie Version 11.30 nicht in einem Verzeichnis, das für eine vorherige Version von SiteScope verwendet wurde.

4. **Führen Sie die ausführbare SiteScope-Installationsdatei bzw. das Installationsskript aus. Sorgen Sie dafür, dass das Skript die Applikation an dem von Ihnen vorbereiteten Speicherort installiert.**

Weitere Informationen finden Sie unter "Installationsablauf" auf Seite 104.

5. **Starten Sie den Server ggf. neu (nur Windows-Installationen).**

6. **Vergewissern Sie sich, dass SiteScope ausgeführt wird, indem Sie über einen kompatiblen Webbrowser eine Verbindung dazu herstellen.**

   Weitere Informationen finden Sie unter "Erste Schritte und Zugriff auf SiteScope" auf Seite 236.

7. **Führen Sie die Schritte nach der Installation durch, um SiteScope auf den Produktionsbetrieb vorzubereiten.**

   Weitere Informationen finden Sie unter "Verwaltung nach der Installation" auf Seite 237.

Kapitel 9: Installationsanforderungen

Dieses Kapitel umfasst die folgenden Themen:

- "Systemanforderungen" unten
- "SiteScope-Kapazitätsbeschränkungen" auf Seite 80
- "Tabellen zur SiteScope-Unterstützung" auf Seite 80

Systemanforderungen

In diesem Abschnitt werden die Mindestsystemanforderungen und Empfehlungen für die Ausführung von SiteScope auf den unterstützten Betriebssystemen beschrieben.

Hinweis:

- Die Installation von SiteScope auf einem 32-Bit-Windows oder Linux-Betriebssystem bzw. als 32-Bit-Applikation unter einem 64-Bit-Windows-Betriebssystem wird nicht mehr unterstützt. SiteScope kann nur noch als 64-Bit-Applikation installiert und ausgeführt werden.
- Das Ausführen von SiteScope auf einer Solaris-Plattform wird nicht mehr unterstützt und das Solaris-Installationsprogramm ist nicht mehr verfügbar.
- Informationen zur Fehlerbehebung und Einschränkungen für die Installation von SiteScope in verschiedenen Umgebungen finden Sie unter "Fehlerbehebung und Einschränkungen " auf Seite 114.

Dieser Abschnitt umfasst die folgenden Themen:

- "Systemhardwareanforderungen" unten
- "Serversystemanforderungen für Windows" auf Seite 76
- "Serversystemanforderungen für Linux" auf Seite 76
- "Clientsystemanforderungen" auf Seite 78

Systemhardwareanforderungen

Technische Details für Hardwareanforderungen:

Computer/Prozessor	1 Kern/2000 MHZ minimal
Arbeitsspeicher	Mindestens 2 GB 8 bis 16 GB bei Umgebungen mit hoher Auslastung
Freier Festplattenspeicher	Mindestens 10 GB
Netzwerkkarte	Mindestens 1 physische Gigabit-Netzwerkschnittstellen-Karte

Technische Details für Virtualisierungsanforderungen:

- Der Einsatz von VMware- und Hyper-V-VMs wird für alle unterstützten Betriebssysteme unterstützt (siehe "Serversystemanforderungen für Windows" auf der nächsten Seite, "Serversystemanforderungen für Linux" auf der nächsten Seite).
- Zur Optimierung von Leistung und Stabilität, insbesondere bei hochgradig ausgelasteten SiteScope-Umgebungen, wird die Verwendung von physischer Hardware empfohlen.
- Beim Einsatz von VMware müssen die VMware-Werkzeuge auf dem Gastbetriebssystem installiert werden.

Zertifizierte Konfigurationen

Die folgende Konfiguration wurde in einer Umgebung mit einer hohen Auslastung für eine Installation von SiteScope zertifiziert, die in BSM integriert wurde:

Betriebssystem	Microsoft Windows Server 2012 R2 (64-Bit)
Systemtyp	X64-basierter PC mit ACPI-Multiprozessor
CPU	4 physische Intel Xeon (R) x5650-Prozessoren mit jeweils 2,67 GHz
Physischer Arbeitsspeicher insgesamt	16 GB
Java-Heap-Speicher	8.192 MB
Gesamtanzahl Monitore	24.000
Gesamtanzahl Remoteserver	2.500
Monitorausführungen pro Minute	3.500

Hinweis:

- Monitorkapazität und -geschwindigkeit können durch zahlreiche Faktoren beträchtlich beeinträchtigt werden. Dazu gehören u. a.: SiteScope-Serverhardware, Betriebssystem, Patches, Software von Drittanbietern, Netzwerkkonfiguration und -architektur, der Standort des SiteScope-Servers im Verhältnis zu den überwachten Server, Protokolltypen für Remoteverbindungen, Monitortypen und Verteilung nach Typ, Monitorhäufigkeit, Monitorausführungszeit, Business Service Management-Integration und Datenbankprotokollierung.
- Bei hoher Last sollten Sie alle Monitore anhalten, bevor Sie erstmalig eine Verbindung zu BSM herstellen.

Serversystemanforderungen für Windows

Die folgenden Microsoft Windows-Betriebssystemversionen wurden zertifiziert:

- Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition (64-Bit)
- Microsoft Windows Server 2012 Standard/Datacenter Edition (64-Bit)
- Microsoft Windows Server 2012 R2 Standard Edition (64-Bit)

Serversystemanforderungen für Linux

Die folgenden Linux-Betriebssystemversionen wurden zertifiziert:

- Oracle Enterprise Linux (OEL) 6.0-6.5 (64-Bit)
- CentOS 6.2 (64 Bit)
- Red Hat ES/AS Linux 5.5-5.8, 6.0-6.5 (6.0, 6.2, 6.4, 6.5 sind zertifiziert) (64-Bit)

Hinweis:

- Die OEL- und CentOS-Umgebungen müssen vor der Installation von SiteScope manuell konfiguriert werden. Weitere Informationen finden Sie unter "Installieren von SiteScope in einer Oracle Enterprise Linux-Umgebung" auf Seite 110 und "Installieren von SiteScope in einer CentOS 6.2-Umgebung" auf Seite 110.
- Wenn Sie SiteScope mit HPOM oder BSM verknüpfen möchten, müssen Sie Abhängigkeiten für

die Red Hat ES Linux 6.0-Umgebung (64-Bit) konfigurieren, bevor Sie den HP Operations Agent installieren (der Agent ist erforderlich, um Ereignisse an HPOM oder BSM zu senden und Metrikdaten zu speichern). Details zum Konfigurieren der Abhängigkeiten und zum Installieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

- Wenn SiteScope unter Red Hat Linux installiert wird, benötigt der Monitor für den Zustand des SiteScope-Servers eine gültige Ausgabe der Befehl sar -W und sar -B für die Indikatoren SwapIns/sec, SwapOuts/sec, PageIns/sec und PageOuts/sec. Wenn diese Befehle nicht funktionieren, werden keine Fehler ausgegeben und die Indikatoren als **nicht verfügbar** angezeigt. Um ihre Ausführung zu aktivieren, bearbeiten Sie die Crontab durch Hinzufügen des Befehls "**/usr/local/lib/sa/sadc -**", der die Ausführung einmal am Tag anweist.
- Um die CPU- und Speicherauslastung auf dem SiteScope-Server oder einem Remoteserver zu überprüfen, der in einer Red Hat Linux-Umgebung ausgeführt wird, muss das **sysstat**-Paket auf dem SiteScope-Server und auf allen überwachten Remoteservern installiert werden (dieses Paket ist standardmäßig nicht enthalten).
- Red Hat Linux 9 mit Native POSIX Threading Library (NPTL) wird nicht unterstützt.
- Um bestimmte Report-Elemente für SiteScope für Linux anzuzeigen, ist es wichtig, dass ein X Window System auf dem Server installiert ist und ausgeführt wird, auf dem SiteScope läuft.

Clientsystemanforderungen

Der SiteScope-Client wird auf allen Microsoft Windows-Betriebssystemen wie folgt unterstützt:

Unterstützte Browser: SiteScope-Benutzeroberfläche	• Microsoft Internet Explorer 9, 10, 11 **Hinweis zu Internet Explorer 10:** ▪ Warnungs-, Monitor- und serverzentrierte Reports werden nur im Kompatibilitätsmodus mit dem **Dokumentmodus: Quirks** unterstützt; der Standardmodus **Dokumentmodus: IE5-Quirks** wird nicht unterstützt. Zum Aktivieren des Modus **Quirks** öffnen Sie den Warnungs-, Monitor- oder serverzentrierten Report und drücken auf F12. Wählen Sie in den Entwicklertools **Dokumentmodus > Quirks** aus. ▪ Add-Ons wie Java werden nicht unterstützt, wenn Internet Explorer 10 über den Startbildschirm verwendet wird. Um SiteScope in Internet Explorer 10 zu verwenden, müssen Sie in den Desktop-Modus von Internet Explorer wechseln und Java installieren. Details finden Sie unter http://windows.microsoft.com/en-us/internet-explorer/install-java#ie=ie-10. • Mozilla Firefox (aktuelle zertifizierte Version): 31.2.0 ESR • Safari 8.0 unter Mac OS (10.10 Yosemite) **Voraussetzungen:** • Der Browser muss so eingestellt sein, dass alle Cookies von Drittanbietern akzeptiert werden und Sitzungs-Cookies zulässig sind. • Der Browser muss so eingestellt sein, dass die JavaScript-Ausführung aktiviert ist. • Der Browser muss Popupfenster der SiteScope-Applikation akzeptieren. • (Nur für Safari) Das Java-Plugin muss unter **Preferences > Security > Manage Website Settings** auf **Run in Unsafe Mode** festgelegt werden, entweder für einzelne Websites (die SiteScope-Hosts) oder für alle Websites.

Unterstützte Browser: Übersichtskonsole (Multi-View, Ereigniskonsole)	• Google Chrome (aktuelle zertifizierte Version): 34.0.1847.137 m • Mozilla Firefox (aktuelle zertifizierte Version): 31.2.0 ESR • Safari (aktuelle zertifizierte Version): 8.0 für Mac • Internet Explorer 9, 10, 11 **Hinweis:** Internet Explorer 9 wird mit den folgenden Einschränkungen unterstützt: ■ Keine Unterstützung unter Microsoft Windows 7 N Edition. ■ Keine Unterstützung unter Microsoft Windows Server 2008. • iPad 3 mit Safari (iOS 7 mit den neuesten Updates) • Android-Tablet mit Chrome 34.0.1847 (Full HD-Display)
Unterstützte Browser: SiteScope Multi-View-Seite in MyBSM	• Internet Explorer 9, 10, 11 **Hinweis:** Internet Explorer 8 kann zwar für den Zugriff auf die Multi-View-Seite in MyBSM verwendet werden, wird aber nicht mehr offiziell unterstützt. Es wird daher empfohlen, zu einem der unterstützten Browser zu wechseln, da die Ereigniskonsole und die Registerkartenfunktionen in der Übersichtskonsole nicht in Internet Explorer 8 ausgeführt werden können.
Java Plug-In (erforderlich zum Öffnen der SiteScope-Benutzeroberfläche)	• **Unterstützt:** JRE-Version 6 oder 7 (das JRE 7-Update 67 ist die aktuelle zertifizierte Version) • **Empfohlen:** JRE 7 (Beachten Sie, dass es für das nächste Release von SiteScope geplant ist, die Unterstützung von JRE, Version 6, einzustellen.) **Tipp:** Java wird als Teil der SiteScope-Installation installiert und sollte nicht unabhängig als Patch oder Update aktualisiert werden. Sie können die Java-Version überprüfen, indem Sie unter **<SiteScope-Installationsverzeichnis>\java\bin** den folgenden Befehl über die Befehlszeile ausführen: `java -server -fullversion`

SiteScope-Kapazitätsbeschränkungen

- Ist SiteScope mit BSM integriert, können bei der Durchführung von Vorgängen mit hoher Auslastung Probleme in SiteScope auftreten. Wenden Sie die folgenden Richtlinien an:
  - Führen Sie den Assistenten zum Veröffentlichen von Vorlagenänderungen nicht für mehr als 3000 Monitore gleichzeitig aus.
  - Führen Sie den Assistenten für die Überwachungsbereitstellung nicht für mehr als 3000 Monitore gleichzeitig aus.
  - Kopieren Sie nicht mehr als 3000 Monitore im Rahmen einer Aktion bzw. fügen Sie sie nicht ein.
  - Führen Sie kein globales Suchen und Ersetzen durch, um die Eigenschaften der Business Service Management-Integration für mehr als 2500 Monitore gleichzeitig zu ändern.
- Es wird nicht empfohlen, mehr als 1000 Monitore zu erstellen, die eine SSH-Verbindung nutzen (vorausgesetzt, die Standardeinstellungen der Parameter, wie zum Beispiel Häufigkeit, Anzahl der Verbindungen usw., werden verwendet). Wenn Sie mehr als 1000 Monitore unter Verwendung von SSH überwachen müssen, sollten Sie einen weiteren SiteScope-Server hinzufügen.

Tipp: SiteScope umfasst ein Werkzeug, mit dem Sie das Verhalten Ihres Systems vorhersagen und die Kapazitätsplanung für SiteScope durchführen können. Weitere Informationen finden Sie unter "SiteScope-Kapazitätsrechner" auf Seite 54.

Tabellen zur SiteScope-Unterstützung

In diesem Abschnitt wird Folgendes behandelt:

Hinweis: Gleichzeitige Bereitstellungen von SiteScope 11.30 mit anderen Produkten wurden weder getestet noch zertifiziert. Derartige Bereitstellungen werden weder unterstützt noch empfohlen.

HP Business Service Management - Tabelle für die Integrationsunterstützung

HP SiteScope-Version	HP Business Service Management-Version				
	9.25	**9.2x**	**9.1x**	**9.0x**	**8.x**
SiteScope 11.3x	√ (Empfohlen)	√	√	√	√

Tabelle zur Unterstützung der HP Operations Manager (HPOM)-Integration

Die aktuelle Version der Unterstützungsmatrix, einschließlich der aktuellen zertifizierten Service Packs, finden Sie auf der Website der HP-Integrationen (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

HPOM-Version	Integration mit SiteScope 11.3x			
	Ereignisintegration	**Knoten-Discovery-Integration**	**Monitor-Discovery-Integration**	**Vorlagenintegration**
HPOM für Windows 8.1x (mit Patch OMW_00149)	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
HPOM für Windows 9.0	Unterstützt	Unterstützt mit Patch OMW_00097/98 oder höher (32-Bit/64-Bit)	Unterstützt	Unterstützung ab Patch 159
HPOM für Linux/Solaris 9.0	Unterstützt	Nicht unterstützt	Unterstützt	Unterstützt

HPOM für Linux/Solaris 9.10	Unterstützt	Unterstützt mit Patch 9.10.200 oder höher	Unterstützt	Unterstützt mit Patch 9.10.210 und Hotfix QCCR1A125751 oder mit allen Patches ab 9.10.210
HPOM für Linux/Solaris 9.20	Unterstützt	Unterstützt	Unterstützt	Unterstützt

Hinweis: Informationen zu den Hardware- und Softwarevoraussetzungen für HP Operations Manager finden Sie in der entsprechenden Version des Installationshandbuchs für Operations Manager für Windows/UNIX, das Sie über die HP-Website zur Software-Unterstützung herunterladen können.

Tabelle zur HP Operations Agent-Unterstützung

HP SiteScope-Version	HP Operations Agent-Version
11.0x	8.60.70
11.1x	8.60.501
11.20 - 11.22	11.02.011
11.23	11.02.011, 11.13*
11.24	11.02.011, 11.13**, 11.14**
11.30	11.14***
*Wird als Upgrade zur zertifizierten Version des installierten HP Operations Agent 11.02 unterstützt. **Der HP Operations-Agent sollte mithilfe des SiteScope-Konfigurationstools getrennt installiert und konfiguriert werden. ***Der HP Operations Agent ist nicht mehr Teil des SiteScope-Installationsprogramms oder des SiteScope-Konfigurationswerkzeugs. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Details finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.	

Hinweis:

- Zur Installation des HP Operations-Agent ist Microsoft Installer 4.5 oder höher erforderlich.
- Weitere Informationen zu den Anforderungen für die Installation des HP Operations-Agenten finden Sie im Installationshandbuch zu HP Operations Agent 11.14, das auf der HP-Website zur Software-Unterstützung zur Verfügung steht.

Tabelle zur Unterstützung von HP SiteScope für Lasttests

Die Liste der in dieser Version unterstützten LoadRunner- und Performance Center-Versionen finden Sie auf der HP-Website zu Integrationen:

- HP Performance Center: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=599
- HP LoadRunner: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=587

Hinweis: Für den Zugriff ist eine Anmeldung mit HP Passport erforderlich (registrieren Sie sich für HP Passport unter http://h20229.www2.hp.com/passport-registration.html).

Tabelle zur HP Network Node Manager i (NNMi)-Unterstützung

Die aktuelle Version der Unterstützungsmatrix, einschließlich der aktuellen zertifizierten Service Packs, finden Sie auf der Website der HP-Integrationen (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3).

Integration	**Unterstützte Versionen**
Ereignisintegration	SiteScope-Version 11.10 oder höher NNMi Version 9.10 oder höher (9.21 ist die aktuell zertifizierte NNMi-Version)
Metrikintegration	SiteScope-Version 11.10 oder höher NNMi-Version 9.10 oder höher NNM iSPI Performance for Metrics, Version 9.10 oder höher (9.22 ist die aktuell zertifizierte NNMi-Version)

Kapitel 10: Aktualisieren von SiteScope

Dieses Kapitel umfasst die folgenden Themen:

Vor Beginn der Aktualisierung

In diesem Abschnitt wird die Aktualisierung von SiteScope-Installationen auf SiteScope 11.30 mit möglichst wenigen Unterbrechungen des Systems und des Betriebs beschrieben.

SiteScope ist abwärtskompatibel. Das bedeutet, dass Sie neuere Versionen von SiteScope installieren und Monitorkonfigurationen aus einer vorhandenen SiteScope-Installation übertragen können.

Vor der Aktualisierung von SiteScope sollten Sie die folgenden Aufgaben durchführen:

- SiteScope muss in einer Windows- oder Linux-Umgebung installiert werden, wie unter "Systemanforderungen" auf Seite 74 aufgeführt.
- Wenn SiteScope für das Senden von Ereignissen und als Datenspeicher für Metrikdaten aktiviert werden soll und SiteScope mit HP Operations Manager oder BSM integriert ist, müssen Sie HP Operations Agent auf dem SiteScope-Server installieren. Details zum Installieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.
- Sie können ein Upgrade von Version 11.13 oder 11.24 auf SiteScope 11.30 durchführen, indem Sie

mit dem Konfigurationswerkzeug eine Sicherung der aktuellen SiteScope-Konfigurationsdaten erstellen, die aktuelle SiteScope-Version deinstallieren, SiteScope 11.30 installieren und dann die Konfigurationsdaten wieder in SiteScope importieren. Details zur Aktualisierung finden Sie unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.

- Sie können ein Upgrade von SiteScope 10.x durchführen, indem Sie zuerst ein Upgrade auf 11.13 oder 11.24 vornehmen und dann SiteScope 11.13 oder 11.24 auf 11.30 aktualisieren. Anweisungen zum Upgrade finden Sie unter "Aktualisieren von SiteScope 10.x auf SiteScope 11.13 oder 11.24" auf Seite 93.

Hinweise und Einschränkungen

- Eine plattformübergreifende Aktualisierung wird nicht unterstützt.
- Möglicherweise treten beim Importieren von SiteScope-Windows-Konfigurationen in Linux-Bereitstellungen Probleme auf (z. B. wenn Windows-Remotecomputer mit den NetBIOS- oder WMI-Verbindungstypen hinzugefügt werden). Überprüfen Sie, dass keine plattformspezifischen Monitoreinstellungen vorliegen, wie URL-Monitore mit WinInet-Optionen, Datei-Monitore auf Windows-Remotecomputern oder Skriptmonitore.
- Die folgenden Monitore werden nicht mehr unterstützt: Wenn diese Monitore in einer früheren Version von SiteScope konfiguriert wurden, werden sie in SiteScope weiterhin angezeigt, nachdem ein Upgrade durchgeführt wurde (32-Bit-Monitore sind jedoch nicht funktionsfähig). Diese Monitore werden in SiteScope 11.24 und früheren Versionen unterstützt.

Nur 32-Bit-Monitore (Keine Ausführung in 64-Bit-Umgebung)	**32-/64-Bit-Monitore**
■ Microsoft Exchange 2003-Postfach[1] ■ Öffentlicher Ordner von Microsoft Exchange 2003-Postfach[1] ■ Microsoft Windows Media Player [2] ■ Real Media Player[2] ■ Sybase ■ Tuxedo	■ Microsoft Exchange 5.5 Nachrichtenverkehr[1] ■ Microsoft Exchange 2000/2003 Nachrichtenverkehr[1] ■ Microsoft Windows-DFÜ[2]

Nur 32-Bit-Monitore (Keine Ausführung in 64-Bit-Umgebung)	**32-/64-Bit-Monitore**
Hinweise: [1] Wir empfehlen die Migration zu Microsoft Exchange 2007 oder höher. [2] Aktuell nicht für zukünftige Versionen geplant.	

Migrieren von 32-Bit- auf 64-Bit-SiteScope

SiteScope 11.30 unterstützt ausschließlich 64-Bit-Betriebssysteme und 64-Bit-Java-Versionen. Aus diesem Grund gibt es die 32-Bit- bzw. 32-Bit-auf-64-Bit-Installationsprogramme für SiteScope in SiteScope 11.30 nicht mehr.

Ab SiteScope 11.30 wird der Webskript-Monitor nur noch in der 64-Bit-Version unterstützt. Um den Monitor nutzen zu können, müssen Sie HP Load Generator 12.02 auf dem SiteScope-Server installieren und den Pfad zum Lastgenerator angeben. Details hierzu finden Sie im Abschnitt zum Webskript-Monitor im SiteScope-Referenzhandbuch.

Die anderen 32-Bit-Monitore werden nicht mehr unterstützt und sind nach einem Upgrade von SiteScope 11.13 oder 11.24 auf SiteScope 11.30 nicht mehr funktionsfähig. Eine Liste der betroffenen Monitore, Monitore, die alternativ verwendet werden können, sowie weitere Details finden Sie im Abschnitt "Hinweise und Einschränkungen" unter "Vor Beginn der Aktualisierung" auf Seite 85.

So führen Sie ein Upgrade von SiteScope 10.x (32-Bit-Version) auf SiteScope 11.30 (64-Bit-Version) aus

1. Führen Sie die im Abschnitt "Aktualisieren von SiteScope 10.x auf SiteScope 11.13 oder 11.24" auf Seite 93 beschriebenen Schritte aus.

2. Führen Sie die unter "Aktualisieren von SiteScope 11.13 oder 11.24 auf SiteScope 11.30" auf Seite 95 beschriebenen Schritte aus (achten Sie bei Schritt 5 darauf, SiteScope auf einem 64-Bit-System zu installieren).

Aktualisieren einer vorhandenen SiteScope-Installation

Hinweis: In diesem Thema finden Sie Informationen dazu, wie Sie Ihre aktuelle Version von SiteScope auf SiteScope 11.30 aktualisieren. Wenn Sie SiteScope installieren, ohne ein Upgrade auszuführen, finden Sie Informationen unter "Installationsworkflow" auf Seite 103.

Zur Aktualisierung Ihrer SiteScope-Version sollten Sie die folgenden Schritte ausführen:

1. **Vergewissern Sie sich, dass der SiteScope-Prozess/Dienst beendet wurde (das Installationsprogramm stoppt den Prozess normalerweise automatisch vor der Installation).**

   Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen" auf Seite 242 oder "Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen" auf Seite 243.

2. **Erstellen Sie mit dem Konfigurationswerkzeug in der aktuellen Version von SiteScope eine Sicherungskopie wichtiger Daten für die SiteScope-Monitorkonfiguration.**

   Erstellen Sie mit dem Konfigurationswerkzeug eine Sicherungskopie des aktuellen SiteScope-Installationsverzeichnisses, indem Sie die SiteScope-Daten aus der aktuellen SiteScope-Installation exportieren, um sie später in SiteScope zu importieren. Weitere Informationen finden Sie unter "Sichern von SiteScope-Konfigurationsdaten" auf Seite 92.

3. **Deinstallieren Sie die aktuelle SiteScope-Version und installieren Sie dann SiteScope 11.30.**

   Details zur Deinstallation von SiteScope finden Sie unter "Deinstallieren von SiteScope" auf Seite 175.

   Installieren Sie SiteScope 11.30 in einer sauberen Verzeichnisstruktur. Das neue, für die Installation von SiteScope erstellte Verzeichnis muss `SiteScope` heißen. Details zur Installation von SiteScope 11.30 finden Sie unter "Installationsablauf" auf Seite 104.

4. **Importieren Sie die neue SiteScope-Lizenz.**

   Um ein Upgrade einer früheren Version von SiteScope auf SiteScope 11.30 durchzuführen, müssen Sie sich zuerst mit Ihrem HP Support-Ansprechpartner für Vertragsverlängerungen in Verbindung setzen, um eine Migration des Produktvertrags zu beantragen. Navigieren Sie nach Abschluss der Vertragsmigration zum Portal für eigene Software-Updates

(https://h20575.www2.hp.com/usbportal/softwareupdate.do), und klicken Sie dort auf die Registerkarte **Get Licensing**, um den oder die neuen Lizenzschlüssel zu erhalten.

Öffnen Sie, nachdem Sie den Lizenzschlüssel erhalten haben, SiteScope, wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen** aus, und erweitern Sie den Bereich **Lizenzen**. Importieren Sie die neue Lizenzdatei. SiteScope sollte nun den Betrieb aufnehmen.

Hinweis: Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.

5. **Installieren und konfigurieren Sie den HP Operations Agent (erforderlich für die Integration von SiteScope mit HPOM oder BSM).**

   Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

6. **Installieren Sie Microsoft-Hotfixes.**

   Zum Verbessern der SiteScope-Skalierbarkeit und Leistung, wird empfohlen, Microsoft-Hotfixes zu installieren. Weitere Informationen finden Sie unter "Installieren von Microsoft-Hotfixes" auf Seite 240.

7. **Importieren Sie die Monitor-Konfigurationsdaten.**

   Importieren Sie nach der Installation die Monitorkonfigurationsdaten (aus Schritt 2) mithilfe des Konfigurationswerkzeugs. Weitere Informationen finden Sie unter "Importieren von Konfigurationsdaten" auf Seite 92.

8. **(Optional) Starten Sie SiteScope nach dem Importieren von Daten auf früheren Versionen von SiteScope, indem Sie die Batchdatei/das Skript "start command shell" ausführen.**

   Um zu verhindern, dass SiteScope automatisch einen Neustart durchführt, wenn das Starten der Monitore mehr als 15 Minuten in Anspruch nimmt, starten Sie SiteScope, indem Sie auf Windows-Plattformen die Datei **go.bat** aus dem **<SiteScope-Stammverzeichnis>\bin** ausführen. Auf Linux-Plattformen führen Sie das Skript **start command shell** mit der Syntax `<Installationspfad>/SiteScope/start` aus.

9. **Wenn Sie SiteScope-Failover verwenden, aktualisieren Sie den Failover-Server mit der entsprechenden SiteScope-Failover-Version.**

Nach der Aktualisierung des primären Servers aktualisieren Sie den Failover-Server mit der entsprechenden SiteScope-Failover-Version und stellen eine Verbindung zwischen dem Failover-Server und dem aktualisierten primären Server her. Details hierzu finden Sie unter "Aktualisieren von SiteScope-Failover" im SiteScope-Failover-Handbuch.

Sichern von SiteScope-Konfigurationsdaten

Der einfachste Weg, ein SiteScope-Upgrade vorzubereiten, besteht darin, mithilfe des Konfigurationswerkzeugs eine Sicherung des aktuellen SiteScope-Installationsverzeichnisses und der erforderlichen Unterverzeichnisse zu erstellen. Mithilfe des Konfigurationswerkzeugs können Sie SiteScope-Daten wie Vorlagen, Protokolle, Monitorkonfigurationsdateien, Serverzertifikate, Skripts usw. aus Ihrer aktuellen SiteScope-Installation exportieren und später in SiteScope importieren. Die Benutzerdaten werden in eine ZIP-Datei exportiert.

Sie können die SiteScope-Installation jedoch auch manuell sichern. Weitere Informationen finden Sie unter "Sichern und Wiederherstellen einer SiteScope-Installation, wenn SiteScope nicht gestartet werden kann" auf Seite 248.

Hinweis: Sie sollten eine Sicherungskopie des Verzeichnisses **<SiteScope>\htdocs** erstellen und nach einer Aktualisierung in das SiteScope 11.30-Verzeichnis kopieren, sodass Sie alte Reports anzeigen können, da dieses Verzeichnis beim Exportieren von SiteScope-Daten nicht kopiert wird.

Details zum Exportieren von SiteScope-Daten mithilfe des Konfigurationswerkzeugs finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151.

Alternativ können Sie SiteScope-Daten im Rahmen des Installationsprozesses exportieren. Weitere Informationen finden Sie unter "Installationsworkflow" auf Seite 103.

Importieren von Konfigurationsdaten

Nach der Aktualisierung von SiteScope können Sie Monitorkonfigurationsdaten aus früheren SiteScope-Versionen mithilfe des Konfigurationswerkzeugs kopieren. Weitere Informationen finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151.

Wenn Sie jedoch manuell eine Sicherung erstellt haben, müssen Sie im neuen Installationsverzeichnis alle Ordner und Dateien löschen, die Sie gesichert haben, und anschließend die gesicherten Ordner und Dateien in das Installationsverzeichnis kopieren. Weitere Informationen finden Sie unter "Sichern und Wiederherstellen einer SiteScope-Installation, wenn SiteScope nicht gestartet werden kann" auf Seite 248.

Aktualisieren von SiteScope 10.x auf SiteScope 11.13 oder 11.24

Da SiteScope kein direktes Upgrade von SiteScope 10.x auf 11.30 unterstützt, müssen Sie zuerst ein Upgrade auf SiteScope 11.13 oder 11.24 und danach ein Upgrade von 11.13 oder 11.24 auf SiteScope 11.30 durchführen.

Hinweis: Es empfiehlt sich, SiteScope 10.x-Versionen auf SiteScope 10.14 zu aktualisieren, bevor Sie ein Upgrade auf SiteScope 11.13 oder 11.24 durchführen.

So führen Sie die Aktualisierung durch:

1. Halten Sie den SiteScope-Dienst an.
2. Exportieren Sie die SiteScope-Konfiguration von SiteScope 10.x (vorzugweise nach einem Upgrade auf SiteScope 10.14).
    a. Sichern Sie den SiteScope 10.x-Ordner (kopieren Sie diesen in einen temporären Ordner auf Ihrem System).
    b. Exportieren Sie die SiteScope-Konfiguration:
        - Starten Sie das SiteScope-Konfigurationswerkzeug (**Start > Programme > HP SiteScope > Konfigurationswerkzeug**) und klicken Sie auf **Weiter**.
        - Wählen Sie **Benutzerdaten exportieren/importieren** aus und klicken Sie auf **Weiter**.
        - Wählen Sie **Benutzerdaten exportieren** aus und klicken Sie auf **Weiter**.
        - Wählen Sie den Pfad des SiteScope 10.x-Installationsverzeichnisses und ein Zielverzeichnis aus, in dem Sie die exportierten Daten speichern möchten. Geben Sie einen Namen für die Sicherungsdatei ein. Wenn Sie Reports für ältere Daten erstellen möchten, wählen Sie **Protokolldateien einschließen** aus.
        - Klicken Sie nach Beendigung des Exports auf **Weiter/Fertig stellen**.
        - Kopieren Sie die Bibliotheken von Drittanbietern und die für verschiedene Monitore (zum Beispiel SAP-Client, JDBC-Treiber) verwendeten JAR-Dateien von Drittanbietern in das temporäre Verzeichnis, da diese Dateien beim Export nicht berücksichtigt werden.

3. Deinstallieren Sie SiteScope 10.x.

   a. Wählen Sie **Start > Einstellungen > Systemsteuerung > Software** aus.

   b. Das Deinstallationsfenster wird geöffnet. Klicken Sie zwei Mal auf **Weiter**, um die Deinstallation zu starten.

   c. Klicken Sie nach Abschluss der Deinstallation auf **Fertig stellen**.

   d. Löschen Sie alle im SiteScope-Verzeichnis noch vorhandenen Dateien.

   e. Vergewissern Sie sich mit der Deinstallationsfunktion des Windows-Dienstes, dass der **SiteScope**-Dienst entfernt wurde. Wenn der SiteScope-Dienst noch immer angezeigt wird, können Sie diesen manuell entfernen, indem Sie über die Eingabeaufforderung den Befehl "`sc delete SiteScope`" ausführen.

   f. Starten Sie den Server neu.

4. Installieren Sie SiteScope 11.10 oder 11.20 und dann die aktuelle Minor-Minor-Version (11.13 oder 11.24) aus dem Bereich **Software Patches** der HP-Website zur Software-Unterstützung.

5. Importieren Sie die Daten nach SiteScope 11.13 oder 11.24:

   - Führen Sie das Konfigurationswerkzeug (**Start > Programme > HP SiteScope > Konfigurationswerkzeug**) aus und klicken Sie auf **Weiter**.
   - Wählen Sie **Konfiguration importieren** aus und klicken Sie auf **Weiter**.
   - Klicken Sie auf **Weiter**.
   - Wählen Sie die zuvor aus der 10.x-Installation exportierte ZIP-Datei aus, vergewissern Sie sich, dass das Zielverzeichnis korrekt ist, und klicken Sie auf **Weiter**.
   - Klicken Sie nach Abschluss des Imports auf **Fertig stellen** (das Konfigurationswerkzeug wird geschlossen).

     Hinweis: Führen Sie das Konfigurationswerkzeug aus und wählen Sie die Option **Anpassen** aus.

   - Wenn Sie zuvor generierte Reports verwenden möchten, ersetzen Sie den vorhandenen Ordner

<SiteScope>\htdoc durch den Ordner **\htdocs**, den Sie in Schritt 2a aus der Vorgängerversion von SiteScope gesichert haben.

6. Starten Sie SiteScope 11.13 oder 11.24 mit der SiteScope 10.x-Konfiguration. SiteScope aktualisiert die Konfiguration.

7. Fahren Sie mit den in Abschnitt "Aktualisieren von SiteScope 11.13 oder 11.24 auf SiteScope 11.30" unten beschriebenen Schritte fort.

Aktualisieren von SiteScope 11.13 oder 11.24 auf SiteScope 11.30

Vor der Aktualisierung von SiteScope 11.13 oder 11.24 auf SiteScope 11.30 sollten Sie die folgenden Schritte ausführen:

So führen Sie die Aktualisierung durch:

1. Halten Sie den SiteScope-Dienst an.

2. Sichern Sie den SiteScope 11.13- oder 11.24-Ordner (kopieren Sie ihn in einen temporären Ordner auf Ihrem System).

3. Exportieren Sie die SiteScope-Konfiguration aus SiteScope11.13 oder 11.24:

   - Starten Sie das SiteScope-Konfigurationswerkzeug (**Start > Programme > HP SiteScope > Konfigurationswerkzeug**) und klicken Sie auf **Weiter**.

   - Wählen Sie **Konfiguration exportieren** aus und klicken Sie auf **Weiter**.

   - Wählen Sie im Bildschirm **Konfiguration exportieren** den Pfad des SiteScope 11.13- oder 11.24-Installationsverzeichnisses und ein Zielverzeichnis aus, in dem Sie die exportierten Daten speichern möchten. Geben Sie einen Namen für die Sicherungsdatei ein. Wenn Sie Reports für ältere Daten erstellen möchten, wählen Sie **Protokolldateien einschließen** aus.

   - Klicken Sie nach Beendigung des Exports auf **Weiter/Fertig stellen**.

   - Kopieren Sie die Bibliotheken von Drittanbietern und die für verschiedene Monitore (zum Beispiel SAP-Client, JDBC-Treiber) verwendeten JAR-Dateien von Drittanbietern in das temporäre Verzeichnis, da diese Dateien beim Export nicht berücksichtigt werden.

4. Deinstallieren Sie SiteScope 11.13 oder 11.24 (**Start > Einstellungen > Systemsteuerung > Programme hinzufügen oder entfernen**):

   a. Das Deinstallationsfenster wird geöffnet. Klicken Sie zwei Mal auf **Weiter**, um die Deinstallation zu starten.

   b. Klicken Sie nach Abschluss der Deinstallation auf **Fertig stellen**.

   c. Löschen Sie alle im SiteScope-Verzeichnis noch vorhandenen Dateien.

   d. Vergewissern Sie sich mit der Deinstallationsfunktion des Windows-Dienstes, dass der **SiteScope**-Dienst entfernt wurde. Wenn der SiteScope-Dienst noch immer angezeigt wird, können Sie diesen manuell entfernen, indem Sie über die Eingabeaufforderung den Befehl "`sc delete SiteScope`" ausführen.

   e. Starten Sie den Server neu.

5. Installieren Sie SiteScope 11.30:

   a. Führen Sie das SiteScope 11.30-Installationsprogramm aus und klicken Sie auf **Weiter**.

   b. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

   c. Wählen Sie ein Verzeichnis für SiteScope 11.30 aus und klicken Sie auf **Weiter** .

   d. Wählen Sie den Installationstyp **HP SiteScope** aus und klicken Sie auf **Weiter**.

   e. Lassen Sie den Standard-Port unverändert und klicken Sie auf **Weiter**. Wenn der Standard-Port belegt ist, geben Sie stattdessen 8088 ein.

   f. Lassen Sie das Feld für den Lizenzschlüssel frei und klicken Sie auf **Weiter**.

   g. Klicken Sie im Übersichtsbildschirm auf **Weiter**.

   h. Klicken Sie nach Abschluss der Installation auf **Weiter** (das Installationsfenster wird geschlossen).

   i. Stellen Sie die Bibliotheken und JAR-Dateien von Drittanbietern wieder her, die Sie (in Schritt 3) in den temporären Ordner kopiert haben.

   j. Halten Sie den SiteScope-Dienst an.

6. Stellen Sie den SiteScope-Dienst so ein, dass er unter einem Überwachungskonto ausgeführt wird.

7. Importieren Sie Daten in SiteScope:

   - Führen Sie das Konfigurationswerkzeug (**Start > Programme > HP SiteScope > Konfigurationswerkzeug**) aus und klicken Sie auf **Weiter**.
   - Wählen Sie **Konfiguration importieren** aus und klicken Sie auf **Weiter**.
   - Wählen Sie im Bildschirm **Konfiguration importieren** die zuvor aus der 11.13- oder 11.24-Installation exportierte ZIP-Datei aus, vergewissern Sie sich, dass das Zielverzeichnis korrekt ist, und klicken Sie auf **Weiter**.
   - Klicken Sie nach Abschluss des Imports auf **Fertig stellen** (das Konfigurationswerkzeug wird geschlossen).

     Hinweis: Führen Sie das Konfigurationswerkzeug aus und wählen Sie die Option **Anpassen** aus.

   - Wenn Sie zuvor generierte Reports verwenden möchten, ersetzen Sie den vorhandenen Ordner **<SiteScope>\htdoc** durch den Ordner **\htdocs**, den Sie in Schritt 2 aus der Vorgängerversion von SiteScope gesichert haben.

8. Ändern Sie die Datenrückführung und andere Parameter in der Datei **master.config**:

   - Öffnen Sie die Datei **<SiteScope-Stammverzeichnis>\groups\master.config**.
   - Ändern Sie die Zeile **_topazEnforceUseDataReduction=** in **_topazEnforceUseDataReduction=false**.

     Hinweis: Wenn der Parameter nicht vorhanden ist, fügen Sie ihn hinzu, um ihn auf **false** festzulegen.

   - Ändern Sie die Zeile **_suspendMonitors=** in **_suspendMonitors=true**.
   - Fügen Sie den Parameter **_disableHostDNSResolution=true** hinzu.

     Hinweis: Alle Parameter sollten so hinzugefügt werden, dass sie sich in alphabetischer Reihenfolge befinden.

   - Speichern und schließen Sie die Datei **master.config**.

9. Starten Sie den SiteScope-Dienst. SiteScope aktualisiert die Konfiguration und startet sich selbst neu. Melden Sie sich bei der Benutzeroberfläche an und überprüfen Sie unter **Voreinstellungen > Integrationsvoreinstellungen**, ob die BSM-Integration korrekt durchgeführt wurde.

10. Setzen Sie sich mit Ihrem HP Support-Ansprechpartner für Vertragsverlängerungen in Verbindung, um die Migration das Produktvertrags zu beantragen. Navigieren Sie nach Abschluss der Vertragsmigration zum Portal für eigene Software-Updates (https://h20575.www2.hp.com/usbportal/softwareupdate.do), und klicken Sie dort auf die Registerkarte **Get Licensing**, um den oder die neuen Lizenzschlüssel zu erhalten.

    Öffnen Sie, nachdem Sie den Lizenzschlüssel erhalten haben, SiteScope, wählen Sie **Voreinstellungen > Allgemeine Voreinstellungen** aus, erweitern Sie den Bereich **Lizenzen**, und importieren Sie die neue Lizenzdatei.

    Hinweis: Bei Anfragen zum Erwerb von Lizenzen (oder wenn Sie zusätzliche Kapazität benötigen) wenden Sie sich an Ihren HP-Vertriebsmitarbeiter oder verwenden Sie den Link "Kontakt" auf der HP SiteScope-Produktseite.

11. Beenden Sie SiteScope.

12. Öffnen Sie die Datei **master.config** und führen Sie Folgendes aus:

    - Setzen Sie die Ausführung der Monitore fort, indem Sie die Zeile **_suspendMonitors=true** in **_suspendMonitors=** ändern.
    - Aktivieren Sie die Datenreduzierung, indem Sie die Zeile **_topazEnforceUseDataReduction=false** in **_topazEnforceUseDataReduction=** ändern.
    - Ändern Sie den Wert für den Parameter **_disableHostDNSResolution=true**.
    - Speichern und schließen Sie die Datei **master.config** und starten Sie SiteScope.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Fehlerbehebungen und Einschränkungen für SiteScope-Aktualisierungen.

- "Der erste Neustart von SiteScope nach der Aktualisierung kann lange dauern" auf der nächsten Seite

- "SiteScope kann die Kunden-ID nicht abrufen" unten
- "Standardwarnaktion wird nach Aktionstyp benannt" auf der nächsten Seite
- "Integration von BSM/ServiceCenter oder Service Manager" auf der nächsten Seite
- "SiteScope-Upgrade schlägt fehl" auf der nächsten Seite
- "Verschieben von SiteScope auf einen anderen Server bei einer BSM-Integration" auf Seite 101

Hinweis: Sie können in der Wissensdatenbank zum Lösen von Softwareproblemen auch selbst nach Informationen zum Aktualisieren von SiteScope suchen. Melden Sie sich für den Zugriff auf die Wissensdatenbank mit Ihrer HP-Passport-ID an.

Der erste Neustart von SiteScope nach der Aktualisierung kann lange dauern

Problem: Der erste SiteScope-Neustart nach einer Aktualisierung kann einige Zeit in Anspruch nehmen (mehr als 15 Minuten). Wenn die Monitore nach 15 Minuten nicht gestartet wurden, wird SiteScope automatisch neu gestartet.

Mögliche Lösung:

Um zu verhindern, dass SiteScope automatisch einen Neustart durchführt, wenn das Starten der Monitore mehr als 15 Minuten in Anspruch nimmt, starten Sie SiteScope, indem Sie auf Windows-Plattformen die Datei **go.bat** aus dem **<SiteScope-Stammverzeichnis>\bin** ausführen. Auf Linux-Plattformen führen Sie das Skript **start command shell** mit der Syntax **<Installationspfad>/SiteScope/start** aus.

Deaktivieren Sie Monitore, die auf nicht ausgeführte Umgebungen ausgerichtet sind. Auf diese Weise wird die Dauer beim Warten auf die Systemantwort verkürzt.

SiteScope kann die Kunden-ID nicht abrufen

Problem: Bei älteren Versionen als SiteScope 9.0 speichert SiteScope, wenn eine Verbindung zu BSM besteht, die Kunden-ID in einer Einstellungsdatei unter **<SiteScope-Stammverzeichnis>\cache\persistent\TopazConfiguration**.

Wird SiteScope zum ersten Mal nach der Aktualisierung auf 9.x gestartet, versucht SiteScope die Einstellungsdatei zu lesen und die Verbindungsdetails für BSM abzurufen. Wenn die Datei beschädigt ist (etwa durch nicht ordnungsgemäßes Durchführen der Exportkonfiguration), kann SiteScope die Kunden-

ID möglicherweise nicht abrufen und versucht, diese über BSM zu beziehen. Wenn BSM während des Neustarts nicht verfügbar ist, kann SiteScope die Kunden-ID nicht abrufen, und SiteScope wird automatisch neu gestartet.

Mögliche Lösung: Stellen Sie sicher, dass mit BSM verbundene SiteScope-Installationen ausgeführt werden, bevor Sie SiteScope nach einer Aktualisierung starten.

Standardwarnaktion wird nach Aktionstyp benannt

Problem: Unter SiteScope 9.0 wurden Warnaktionen hinzugefügt. Bei einer Aktualisierung auf eine Version von SiteScope 9.0 oder eine spätere Version wird eine Standardwarnaktion erstellt, die nach dem Aktionstyp benannt wird (beispielsweise **E-Mail**, **Pager** oder **SMS**). Dies kann ein Problem darstellen, wenn der Standardname mit der Warnung verkettet werden soll, die die Aktion enthält.

Mögliche Lösung: Öffnen Sie vor der Aktualisierung die Datei **master.config** unter **<SiteScope-Stammverzeichnis>\groups** und ändern Sie den Schlüssel **_AlertActionCompositeNameDelimiter**, sodass die Verkettung das gewünschte Trennzeichen enthält.

Integration von BSM/ServiceCenter oder Service Manager

Dieser Hinweis ist wichtig, wenn Sie eine Aktualisierung einer SiteScope-Version vor 10.00 durchführen und eine BSM-/ServiceCenter- oder ServiceManager-Integration verwenden. Beim Einrichten des ServiceCenter-Monitors in SiteScope wird eine Datei mit der Bezeichnung **peregrine.jar** erstellt und im Verzeichnis **WEB-INF\lib** auf dem Computer mit SiteScope abgelegt. Diese Datei muss von dem SiteScope-Upgrade gesichert werden. Andernfalls wird sie während des Upgrades gelöscht. Wenn das Upgrade abgeschlossen ist, kopieren Sie die gesicherte Datei **peregrine.jar** wieder in das Verzeichnis **WEB-INF\lib**.

SiteScope-Upgrade schlägt fehl

Wenn bei der Aktualisierung ein Fehler auftritt, überprüfen Sie die Datei **upgrade.log** im Verzeichnis <**SiteScope-Stammverzeichnis>\logs**, um den Grund für den Fehler zu ermitteln.

Wenn die Aktualisierung bei der Installation von SiteScope in einer Windows-Umgebung fehlschlägt, versucht SiteScope wiederholt einen Neustart durchzuführen.

Mögliche Lösung: Führen Sie die SiteScope-Installation erneut durch.

Verschieben von SiteScope auf einen anderen Server bei einer BSM-Integration

Dieses Verfahren ist relevant, wenn Sie Ihre SiteScope-Serverinstallation auf neue Hardware verschieben (mit neuem Hostnamen und IP-Adresse) und Sie eine BSM-Integration verwenden. Führen Sie die folgenden Schritte durch, um die Auswirkung auf die Integration zu minimieren:

1. Erstellen Sie eine Sicherung Ihrer aktuellen SiteScope-Installation. Weitere Informationen finden Sie unter "Sichern von SiteScope-Konfigurationsdaten" auf Seite 92.

2. Installieren Sie SiteScope auf der neuen Hardware und importieren Sie die SiteScope-Konfigurationsdaten in das SiteScope-Installationsverzeichnis. Weitere Informationen finden Sie unter "Importieren von Konfigurationsdaten" auf Seite 92.

3. Konfigurieren Sie den SiteScope-Server mit derselben Portnummer, die für die alte Hardware verwendet wurde.

4. Führen Sie in BSM folgende Aktionen aus:

   - Aktualisieren Sie die relevanten Felder für das SiteScope-Profil auf der Seite **Neuer SiteScope**.

   - Aktualisieren Sie die Informationen zum Computer mit SiteScope in der HOSTS-Tabelle.

Teil 3: Installieren von SiteScope

Kapitel 11: Installationsworkflow

Dieses Kapitel umfasst die folgenden Themen:

Installationsversionstypen

Beachten Sie, dass SiteScope als 64-Bit-Applikation installiert und ausgeführt wird. Es steht als selbstextrahierende ausführbare Datei und Paketordner zur Verfügung. In Haupt- und Nebenversionen ist diese Datei im SiteScope-Installationspaket (ZIP-Datei) verfügbar.

Bei Minor-Minor- und Patch-Versionen laden Sie die Datei aus dem Portlet **Software Patches** auf der Website für die HP Software-Unterstützung herunter.

> **Hinweis:** Minor-Minor- und Patch-Versionen von SiteScope sollten nur über Standardinstallationen von SiteScope installiert werden, nicht über nicht-standardmäßigen Installationen wie SiteScope Failover oder System Health.

Wenn Sie die aktuellste Version installieren möchten, müssen Sie SiteScope 11.30 und dann den aktuellsten kumulierten/zwischenzeitlichen Patch für die Minor-Minor-Version (angezeigt in der HP Support-Website im Patches-Abschnitt für 11.30) installieren.

Offizieller Name	Versionstyp	Beispiel	Installation
Haupt Neben	Komplette Installations-version	10.0, 11.0 10.10, 11.30 Beispieldateiname: `HPSiteScope_11.30_setup.exe`	Installation auf einem neuen System und Import von vorhergender Versionskonfiguration. Aktualisierung wird beim ersten Start ausgeführt.
Minor-Minor (Patch)	Zusammenstellung von Fehlerkorrekturen aus den entsprechenden Haupt- oder Nebenversionen	10.11 (über 10.10) 10.01 (über 11.10) 11.24 (über 11.20 oder 11.2x) Beispieldateiname: `HPSiS1122_11.24_setup.exe`	Der Minor-Minor-Patch wird über der enstprechenden Version installiert. Es ist keine Aktualisierung erforderlich.
Kumulierter/ zwischenzeit-licher/ öffentlicher Patch	Pakete, die offizielle Fehlerkorrekturen für dringende Fehler enthalten	SS1122130529 SS<Ver><Datum> Beispieldateiname: `SS1122130529-11.22.000-WinNT4.0.msi`	Gilt nur für die Installation über einer einzelnen dedizierten Haupt-, Neben- oder Minor-Minor-Version.

Installationsablauf

Dieses Thema enthält Anleitungen für die Installation von SiteScope 11.30.

Hinweis: Wenn Sie eine vorhandene Version von SiteScope aktualisieren möchten, befolgen Sie die Anleitungen unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.

1. **Voraussetzungen für die Installation (nur für Linux).**

   a. Wählen Sie einen geeigneten Installationsspeicherort aus und legen Sie die Kontoberechtigungen fest. Weitere Informationen finden Sie unter "Vorbereiten der Linux-Installation" auf Seite 109.

   b. Wenn Sie SiteScope auf einer der folgenden Plattformen installieren, müssen Sie die Umgebung manuell konfigurieren, bevor Sie SiteScope installieren:

Plattform	Voraussetzungen für die Installation
Oracle Enterprise Linux 6.0, 6.1	Informationen hierzu finden Sie unter "Installieren von SiteScope in einer Oracle Enterprise Linux-Umgebung" auf Seite 110.
CentOS 6.2	Informationen hierzu finden Sie unter "Installieren von SiteScope in einer CentOS 6.2-Umgebung" auf Seite 110.
Eine HP Cloud Services-Instanz (HPCS), die unter einem CentOS 6.2-Betriebssystem ausgeführt wird	Informationen hierzu finden Sie unter "Installieren von SiteScope auf einer HP Cloud Services-Instanz, die unter CentOS 6.2 ausgeführt wird" auf Seite 111.
Red Hat ES/AS Linux 6.0	Wenn Sie SiteScope mit HPOM oder BSM verknüpfen möchten, müssen Sie Abhängigkeiten für die Red Hat ES Linux 6.0-Umgebung (64-Bit) konfigurieren, bevor Sie den HP Operations Agent installieren (der Agent ist erforderlich, um Ereignisse an HPOM oder BSM zu senden und Metrikdaten zu speichern). Details zum Konfigurieren der Abhängigkeiten und zum Installieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

2. **Laden Sie SiteScope 11.30 herunter.**

   a. Laden Sie das plattformspezifische Installationspaket (**SiteScope_11.30_Windows.zip** oder **SiteScope_11.30_Linux.zip**) auf dem Computer herunter, auf dem Sie SiteScope installieren möchten. SiteScope steht wie folgt über HP Systems zur Verfügung:

Kunde	Download-Optionen
Für Evaluierungskunden	Link für elektronische Download-Evaluierung HP Software Partner Central für HP-autorisierte Softwarepartner (Für die oben genannten Links sind HP Passport-Konten erforderlich. Registrieren Sie sich für einen HP Passport unter http://h20229.www2.hp.com/passport-registration.html.)
Für neue Kunden	Elektronischer Software-Download. Der Kunde erhält einen Link per E-Mail, über den die Software heruntergeladen werden kann. Dieser Link ist auf die Bestellung abgestimmt.

Kunde	Download-Optionen
Aktualisierungen für bestehende Kunden	https://h20575.www2.hp.com/usbportal/softwareupdate.do **Voraussetzungen:** i. Sie müssen über ein HP Passport-Konto verfügen, um auf den obigen Link zugreifen zu können. Ferner ist eine Support Agreement-ID (SAID) erforderlich, um Aktualisierungen über das SSO-Portal zu erhalten. Informationen zum Registrieren für einen HP Passport finden Sie unter http://h20229.www2.hp.com/passport-registration.html. Details zum Aktivieren der SAID finden Sie unter **FAQ** auf der Website Software Support Online. ii. Für das Software-Upgrade ist ein neuer Lizenzschlüssel erforderlich. Setzen Sie sich mit Ihrem HP Support-Ansprechpartner für Vertragsverlängerungen in Verbindung, um zuerst die Migration das Produktvertrags zu beantragen. Navigieren Sie nach Abschluss der Vertragsmigration zum Portal für eigene Software-Updates (https://h20575.www2.hp.com/usbportal/softwareupdate.do), und klicken Sie dort auf die Registerkarte **Get Licensing**, um den oder die neuen Lizenzschlüssel zu erhalten. **So laden Sie Software-Updates herunter:** i. Wählen Sie die Option **My software updates** aus. ii. Erweitern Sie **Application Performance Management**, wählen Sie die benötigten HP SiteScope 11.30 Software-E-Medien aus und klicken Sie dann auf **Get software updates**. iii. Klicken Sie auf der Registerkarte **Selected Products** auf **Get Software** für die gewünschten Produktaktualisierungen und folgen Sie den Anweisungen auf der Seite, um die Software herunterzuladen.

b. Extrahieren Sie die komprimierte Datei in ein geeignetes Verzeichnis.

3. **Installieren Sie SiteScope 11.30.**

   Installieren Sie SiteScope mithilfe einer der folgenden Installationsoptionen:

Betriebssystem	Installationsoptionen
Windows	■ Über die Benutzeroberfläche ausführbare Datei (Installations-Assistent). Weitere Informationen finden Sie unter "Installation mithilfe des Installationsassistenten" auf Seite 116. ■ Unbeaufsichtigte Installation. Weitere Informationen finden Sie unter "Installieren von SiteScope im unbeaufsichtigten Modus" auf Seite 148.
Linux	■ Über die Benutzeroberfläche ausführbare Datei (Installations-Assistent). Weitere Informationen finden Sie unter "Installation mithilfe des Installationsassistenten" auf Seite 116. ■ Konsolenmodus-Installationsskript unter Verwendung einer Befehlszeileneingabe. Weitere Informationen finden Sie unter "Installieren auf Linux-Plattformen unter Verwendung des Konsolenmodus" auf Seite 139. ■ Unbeaufsichtigte Installation. Weitere Informationen finden Sie unter "Installieren von SiteScope im unbeaufsichtigten Modus" auf Seite 148.

Hinweis:

- Die Installation im Konsolenmodus wird nicht für Windows-Installationen unterstützt.
- Wenn bereits eine Installation von SiteScope vorhanden ist, müssen Sie diese deinstallieren, bevor Sie SiteScope 11.30 installieren.
- Haben Sie vorher SiteScope-Daten mithilfe des Konfigurationswerkzeugs exportiert (Details finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151), können Sie die **.zip**-Datei der Benutzerdaten importieren.
- Wenn Sie über Middleware und Treiber von Drittanbietern verfügen, müssen Sie diese manuell kopieren oder installieren.

4. **Installieren und konfigurieren Sie den HP Operations Agent (erforderlich für die Integration von SiteScope mit HPOM oder BSM).**

   Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

5. **Installieren Sie Microsoft-Hotfixes.**

   Zum Verbessern der SiteScope-Skalierbarkeit und Leistung, wird empfohlen, Microsoft-Hotfixes zu installieren. Weitere Informationen finden Sie unter "Installieren von Microsoft-Hotfixes" auf Seite 240.

6. **Stellen Sie eine Verbindung zu SiteScope her.**

   Weitere Informationen finden Sie unter "Verbinden mit SiteScope" auf Seite 244.

Vorbereiten der Linux-Installation

Je nach Umgebung beinhaltet die Vorbereitung der Installation von SiteScope unter Linux das Auswählen eines geeigneten Speicherorts für die Installation und das Einrichten von Kontoberechtigungen.

So bereiten Sie die Installation von SiteScope unter Linux vor:

1. Stellen Sie sicher, dass der Installationsspeicherort für die SiteScope-Applikation (`/opt/HP/SiteScope`) über genügend Festplattenspeicher für die Installation und den Betrieb von SiteScope verfügt.

2. Erstellen Sie ein Nicht-Root-Benutzerkonto, das die SiteScope-Applikation ausführt, und legen Sie für diesen Benutzer Kontoberechtigungen für `/opt/HP/SiteScope` fest. Legen Sie die Standardshell für das Konto fest. Weitere Informationen finden Sie unter "Konfigurieren eines Nicht-Root-Benutzerkontos mit Berechtigungen zum Ausführen von SiteScope" auf Seite 51.

Hinweis:

- Das Installationsverzeichnis für Linux kann während der Installation nicht geändert werden und es wird nicht empfohlen, es nach der Installation zu ändern.
- Auch wenn SiteScope umfassende Kontoberechtigungen erfordert, um die gesamte Bandbreite der Serverüberwachung zu ermöglichen, wird davon abgeraten, SiteScope mit dem Root-Konto auszuführen oder SiteScope für die Verwendung des Root-Kontos für den Zugriff auf Remoteserver zu konfigurieren.
- Sie können für SiteScope auch eine unbeaufsichtigte Installation durchführen. Weitere Informationen finden Sie unter "Installieren von SiteScope im unbeaufsichtigten Modus" auf Seite 148.

Installieren von SiteScope in einer Oracle Enterprise Linux-Umgebung

Bevor SiteScope unter Oracle Enterprise Linux installiert werden kann, müssen in der Umgebung die folgenden Abhängigkeiten installiert werden:

- glibc-2.12-1.25.el6.i686.rpm
- glibc-common-2.12-1.25.el6.i686.rpm
- nss-softokn-freebl-3.12.9-3.el6.i686.rpm
- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm

Sie können die Abhängigkeiten mit dem `yum` Package Manager von Oracle Enterprise Linux installieren, indem Sie folgenden Befehl ausführen:

```
yum install -y glibc glibc-common nss-softokn-freebl libXau libxcb libX11 libXext
```

Diese Abhängigkeiten finden Sie in den Standard-Repositorys (**/etc/yum.repos.d**) für alle Red Hat-basierten Systeme.

Installieren von SiteScope in einer CentOS 6.2-Umgebung

Bevor Sie SiteScope auf CentOS 6.2 (64-Bit) installieren, vergewissern Sie sich, dass in der Linux-Umgebung eine der folgenden zusätzlichen Bibliotheken installiert ist (es wird empfohlen, die erste Option zu verwenden):

- Installieren Sie die **glibc.i686**- und die **libXp.i686**-Bibliothek, indem Sie folgenden Befehl ausführen:

  ```
  [root@centos ~]# yum install glibc.i686 libXp.i686
  ```

- Vergewissern Sie sich, dass eine beliebige JRE installiert ist und die Pfade zu ihr korrekt geschrieben sind:

  ```
  [root@centos ~]# java -version
  java version "1.6.0_22"
  ```

```
OpenJDK Runtime Environment (IcedTea6 1.10.6) (rhel-1.43.1.10.6.el6_2-x86_64)
OpenJDK 64-Bit Server VM (build 20.0-b11, mixed mode)
```

Wenn ein Fehler mit dem Hinweis angezeigt wird, dass der Befehl nicht gefunden wurde, müssen Sie eine JRE installieren. Verwenden Sie hierzu den folgenden Befehl:

```
root@centos ~]# yum install java-1.6.0-openjdk
```

Hinweis: Normalerweise sind in der CentOS-Installation die Bibliotheken bereits installiert. In diesem Fall verwendet das Installationsprogramm **glibc.i686** sobald JRE von glibc und libXp abhängt. Da SiteScope über ein eigenes Java verfügt, ist JRE nur für das Ausführen des Installationsprogramms erforderlich.

Tipps für das Installieren von SiteScope auf einem CentOS 6-Server:

Überprüfen Sie den Hostnamen des CentOS 6.2-Servers und vergewissern Sie sich, dass der Host aufgelöst wird:

1. Fragen Sie Ihren Hostnamen ab, indem Sie den Hostnamen-Befehl ausführen.
2. Führen Sie `ping <Ihr_Hostname>` aus. Wenn die Ping-Anforderung erfolgreich verläuft, kann der Host bereits aufgelöst werden.
3. Schlägt die Anforderung fehl, bestimmen Sie Ihre IP mit `ifconfig`.
4. Führen Sie `echo "<Ihre_IP> <Ihr_Hostname>" >> /etc/hosts` aus, um eine Zeichenfolge mit einer IP, die Ihrem Hostnamen entspricht, zur Host-Datei hinzuzufügen.
5. Führen Sie `ping <Ihr_Hostname>` erneut aus, um sich zu vergewissern, dass der Host aufgelöst wurde.

   Wird der Hostname nicht aufgelöst, kann dies dazu führen, dass SiteScope nicht startet.

Installieren von SiteScope auf einer HP Cloud Services-Instanz, die unter CentOS 6.2 ausgeführt wird

SiteScope wird in einer HP Cloud Services-Instanz (HPCS) unterstützt, die unter einem CentOS 6.2-Betriebssystem ausgeführt wird.

Tipps für die SiteScope-Installation auf HPCS:

1. **Überprüfen Sie den Hostnamen des HP Cloud Services-Servers und vergewissern Sie sich, dass der Host aufgelöst wird.**

   a. Fragen Sie Ihren Hostnamen ab, indem Sie den Hostnamen-Befehl ausführen.

   b. Führen Sie `ping <Ihr_Hostname>` aus. Wenn die Ping-Anforderung erfolgreich verläuft, kann der Host bereits aufgelöst werden.

   c. Schlägt die Anforderung fehl, bestimmen Sie Ihre IP mit `ifconfig`.

   d. Führen Sie `echo "<Ihre_IP> <Ihr_Hostname>" >> /etc/hosts` aus, um eine Zeichenfolge mit einer IP, die Ihrem Hostnamen entspricht, zur Host-Datei hinzuzufügen.

   e. Führen Sie `ping <Ihr_Hostname>` erneut aus, um sich zu vergewissern, dass der Host aufgelöst wurde.

2. **Überprüfen Sie den Auslagerungsbereich.**

   a. Führen Sie den free-Befehl aus, um zu überprüfen, ob der Auslagerungsbereich erstellt wurde.

   b. Wenn Sie feststellen, dass der Auslagerungsbereich nicht vorhanden ist:

   ```
   [root@centos ~]# free | grep Swap
   Swap: 0 0 0
   ```

   führen Sie die folgenden Befehle aus:

   Erstellen Sie eine 2-GB-Datei:

   ```
   [root@centos ~]# dd if=/dev/zero of=/swapfile bs=1M count=2048
   ```

   Initialisieren Sie diese als Auslagerungsbereich:

   ```
   [root@centos ~]# mkswap /swapfile
   ```

   Führen Sie die Aktivierung durch:

   ```
   [root@centos ~]# swapon /swapfile
   ```

   c. Überprüfen Sie den Auslagerungsbereich erneut:

```
root@centos ~]# free | grep Swap
Swap: 2097144 0 2097144
```

3. **Installieren Sie zusätzliche Bibliotheken.**

   Weitere Informationen finden Sie unter "Installieren von SiteScope in einer CentOS 6.2-Umgebung" auf Seite 110.

Konfiguration der Sicherheitsgruppe

IP-Protokoll	Von Port	Zu Port	Typ	CIDR IPS
tcp	8080	8080	IPs	0.0.0.0/0
tcp	22	22	IPs	0.0.0.0/0
tcp	8888	8888	IPs	0.0.0.0/0
icmp	-1	-1	IPs	0.0.0.0/0

Installieren von SiteScope auf HPCS

So installieren Sie SiteScope auf HPCS:

1. Ändern Sie das aktuelle Verzeichnis in den Speicherort, an dem sich das SiteScope-Installationsprogramm befindet, und führen Sie das SiteScope-Installationsprogramm aus:

   ```
   [root@centos ~]# sh ./HPSiteScope_11.30_setup.bin -i console
   ```

2. Installieren Sie SiteScope unter Verwendung des Konsolenmodus. Weitere Informationen finden Sie unter "Installieren auf Linux-Plattformen unter Verwendung des Konsolenmodus" auf Seite 139.

3. Führen Sie nach Abschluss der Installation SiteScope aus:

   ```
   [root@centos ~]# /opt/HP/SiteScope/start
   ```

4. Warten Sie einige Minuten, bis der SiteScope-Dienst gestartet wurde, und vergewissern Sie sich anschließend, dass die erforderlichen Prozesse ausgeführt werden:

   ```
   [root@centos ~]# ps -ef | grep SiteScope | grep -v grep |awk '{print $3}
   '84758477
   ```

Der letzte Befehl zeigt die Prozess-IDs der SiteScope-Prozesse. Wenn zwei Prozesse vorhanden sind, wurde der SiteScope-Server erfolgreich gestartet.

Hinweise und Einschränkungen

Die Operations Manager-Integration wird zurzeit in SiteScope 11.30 auf einem CentOS 6.2-Server nicht unterstützt.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält die folgenden Fehlerbehebungen und Einschränkungen für die SiteScope-Installation.

- "SiteScope kann möglicherweise nicht unter Verwendung des Konsolenmodus installiert werden" unten
- "Fehler bei der Installation von HP Operations Agent – Prüfen Sie die Protokolldateien" unten
- "Nach der Deinstallation von SiteScope schlägt eine nachfolgende SiteScope-Installation fehl" auf der nächsten Seite

SiteScope kann möglicherweise nicht unter Verwendung des Konsolenmodus installiert werden

Das Installieren von SiteScope in Linux Red Hat-Umgebungen unter Verwendung des Konsolenmodus kann fehlschlagen, wenn zu viele X-Sitzungen geöffnet sind.

Problemumgehung: Schließen Sie einige der X-Sitzungen oder löschen Sie die DISPLAY-Variable.

Fehler bei der Installation von HP Operations Agent – Prüfen Sie die Protokolldateien

Wenn bei der Installation des HP Operations Agent ein Fehler auftritt oder Sie den Installationsstatus anzeigen möchten, können Sie die Protokolldateien prüfen.

- SiteScope-Protokoll. Dieses Protokoll zeigt nur an, ob die Installation erfolgreich durchgeführt wurde.

Name der Protokolldatei: **HPSiteScope_config_tool.log**

Speicherort der Protokolldatei:

- **win- %temp%** auf Windows-Plattformen
- **/temp** oder **/var/temp** auf UNIX/Linux-Plattformen

(Suchen Sie nach Ergebnissen für "installOATask")

- Protokolldateien des HP Operations Agents.

Name der Protokolldatei: **oainstall.log**, **oapatch.log**

Speicherort der Protokolldatei:

- **%ovdatadir%\log** auf Windows-Plattformen
- **/var/opt/OV/log/** auf UNIX-/Linux-Plattformen

Nach der Deinstallation von SiteScope schlägt eine nachfolgende SiteScope-Installation fehl

Nach der Deinstallation von SiteScope kann eine nachfolgende Installation nicht vollständig ausgeführt werden und die folgende Meldung wird angezeigt: "Please enable windows scripting host." (Aktivieren Sie den Windows-Scripting-Host.) Der Grund dafür ist, dass Windows die Variable `%SystemRoot%` in der Umgebungsvariable PATH nicht auflösen kann (obwohl `%SystemRoot%` im Pfad vorliegt).

Problemumgehung: Ersetzen Sie die Variable `%SystemRoot%` in der Umgebungsvariable PATH durch den aktuellen Pfad für **C:\Windows\system32**.

Kapitel 12: Installation mithilfe des Installationsassistenten

Führen Sie die folgenden Schritte aus, um SiteScope mithilfe des Installationsassistenten in unterstützten Windows- oder Linux-Umgebungen zu installieren. Eine Liste der unterstützten Umgebungen finden Sie unter "Systemanforderungen" auf Seite 74.

Der Installationsassistent wird automatisch ausgeführt, wenn bereits X11-Bibliotheken auf dem Server installiert wurden. Sind diese Bibliotheken nicht installiert, haben Sie folgende Möglichkeiten:

- Installieren Sie SiteScope im Grafikmodus auf einem Computer ohne X11-Server. Weitere Informationen finden Sie unter "Installieren von SiteScope mithilfe des Installationsassistenten auf einem Computer ohne X11 Server" auf Seite 137.
- Installieren Sie SiteScope unter Linux-Plattformen im Konsolenmodus. Weitere Informationen finden Sie unter "Installieren auf Linux-Plattformen unter Verwendung des Konsolenmodus" auf Seite 139.

Hinweis:

- Sie können für SiteScope auch eine unbeaufsichtigte Installation durchführen. Weitere Informationen finden Sie unter "Installieren von SiteScope im unbeaufsichtigten Modus" auf Seite 148.
- Wenn Sie eine vorhandene Version von SiteScope aktualisieren möchten, befolgen Sie die Prozeduren unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.
- Die Option zum Installieren und Deinstallieren von HP Operations Agent direkt aus SiteScope wurde aus dem Konfigurationsassistenten und dem Konfigurationswerkzeug entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

So installieren Sie SiteScope:

1. Besorgen Sie sich das SiteScope-Installationspaket.

   a. Laden Sie das plattformspezifische Installationspaket (**SiteScope_11.30_Windows.zip** oder **SiteScope_11.30_Linux.zip**) auf dem Computer herunter, auf dem Sie SiteScope installieren möchten. SiteScope steht wie folgt über HP Systems zur Verfügung:

Kunde	Download-Optionen
Für Evaluierungskunden	Link für elektronische Download-Evaluierung HP Software Partner Central für HP-autorisierte Softwarepartner **Hinweis:** Für die oben genannten Links sind HP Passport-Konten erforderlich. Registrieren Sie sich für einen HP Passport unter http://h20229.www2.hp.com/passport-registration.html.
Für neue Kunden	Elektronischer Software-Download. Der Kunde erhält einen Link per E-Mail, über den die Software heruntergeladen werden kann. Dieser Link ist auf die Bestellung abgestimmt.

Kunde	Download-Optionen
Aktualisierungen für bestehende Kunden	https://h20575.www2.hp.com/usbportal/softwareupdate.do **Voraussetzungen:** i. Sie müssen über ein HP Passport-Konto verfügen, um auf den obigen Link zugreifen zu können. Ferner ist eine Support Agreement-ID (SAID) erforderlich, um Aktualisierungen über das SSO-Portal zu erhalten. Informationen zum Registrieren für einen HP Passport finden Sie unter http://h20229.www2.hp.com/passport-registration.html. Details zum Aktivieren der SAID finden Sie unter **FAQ** auf der Website Software Support Online. ii. Für das Software-Upgrade ist ein neuer Lizenzschlüssel erforderlich. Setzen Sie sich mit Ihrem HP Support-Ansprechpartner für Vertragsverlängerungen in Verbindung, um zuerst die Migration das Produktvertrags zu beantragen. Navigieren Sie nach Abschluss der Vertragsmigration zum Portal für eigene Software-Updates (https://h20575.www2.hp.com/usbportal/softwareupdate.do), und klicken Sie dort auf die Registerkarte **Get Licensing**, um den oder die neuen Lizenzschlüssel zu erhalten. **So laden Sie Software-Updates herunter:** i. Wählen Sie die Option **My software updates** aus. ii. Erweitern Sie **Application Performance Management**, wählen Sie die benötigten HP SiteScope 11.30 Software-E-Medien aus und klicken Sie dann auf **Get software updates**. iii. Klicken Sie auf der Registerkarte **Selected Products** auf **Get Software** für die gewünschten Produktaktualisierungen und folgen Sie den Anweisungen auf der Seite, um die Software herunterzuladen.

b. Extrahieren Sie die komprimierte Datei in ein geeignetes Verzeichnis.

2. Führen Sie die SiteScope-Installation gemäß Ihrem Betriebssystem aus. Beachten Sie, dass SiteScope nur als 64-Bit-Applikation installiert und ausgeführt werden kann.

   Für Windows:

   a. Führen Sie die Datei **HPSiteScope_11.30_setup.exe** aus.

   b. Geben Sie die Ihrem Betriebssystem und Ihrer Architektur entsprechende Netzwerkadresse ein, von der Sie die SiteScope-Installation ausführen, gefolgt vom Namen der ausführbaren Datei.

      Beispiel:

      ```
      <SiteScope_Installation>\HPSiteScope_11.30_setup.exe
      ```

   Für Linux:

   a. Melden Sie sich am Server als Benutzer **root** an.

   b. Führen Sie das Installationsprogramm aus, indem Sie Folgendes eingeben: **./HPSiteScope_11.30_setup.bin**.

      Hinweis: Wenn auf dem Server der Microsoft-Terminalserverdienst ausgeführt wird, muss sich der Dienst beim Installieren von SiteScope im Installationsmodus befinden. Befindet sich der Dienst nicht im richtigen Modus, gibt der Assistent eine Fehlermeldung aus und beendet dann die Installation. Wechseln Sie mithilfe des Befehls **change user** in den Installationsmodus. Weitere Informationen finden Sie auf der Microsoft-Supportseite (http://support.microsoft.com/kb/320185).

3. Der Bildschirm für die Auswahl des Gebietsschemas wird angezeigt.

Wählen Sie aus der Liste der Sprachen eine Sprache für die SiteScope-Installation. Abhängig von dem Gebietsschema des Betriebssystems zeigt das Installationsprogramm verschiedene Sprachgruppen an. Eine Liste der für die SiteScope-Benutzeroberfläche verfügbaren Sprachen finden Sie unter "Internationalisierung in SiteScope" im Handbuch Verwenden von SiteScope.

Klicken Sie auf **OK**, um mit der Installation fortzufahren. Die Seite für die Initialisierung wird angezeigt.

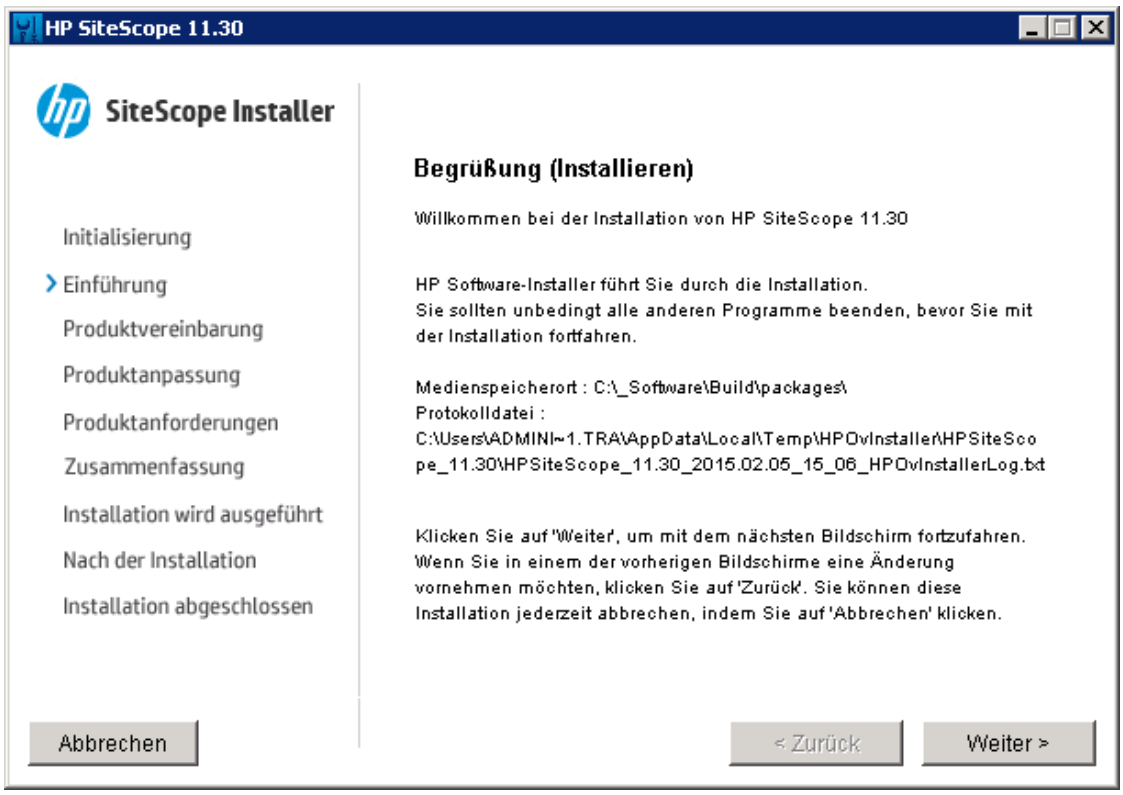
Wenn das Installationsprogramm auf dem System ein Antivirenprogramm erkennt, werden Sie aufgefordert, die Warnungen zu beachten, bevor Sie mit der Installation fortfahren.

4. Lesen Sie die Warnungen, die ggf. auf der Seite mit den Anwendungsanforderungen zum Überprüfen der Warnungen angezeigt werden, und befolgen Sie die dort angezeigten Anweisungen.

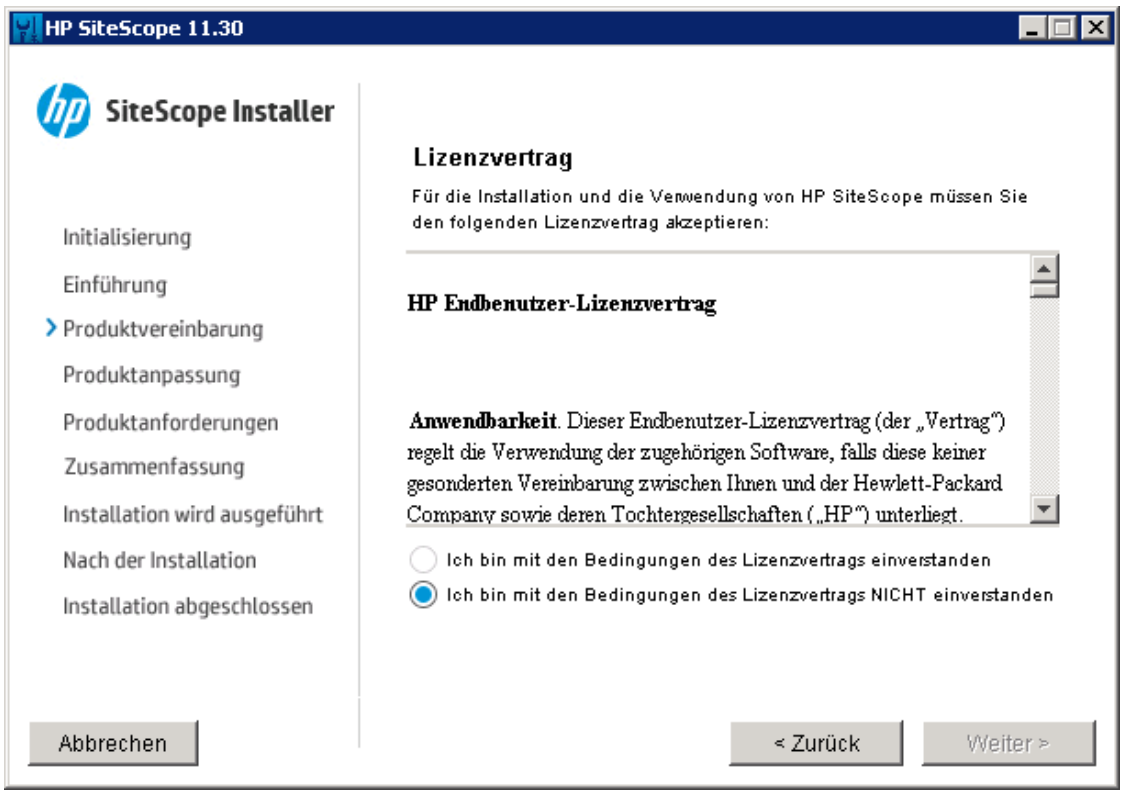
Wenn das Installationsprogramm ein Antivirenprogramm feststellt, können Sie versuchen, SiteScope zu installieren, ohne das Antivirenprogramm zu deaktivieren.

Klicken Sie auf **Fortfahren**, um mit der Installation fortzufahren.

5. Klicken Sie auf der angezeigten Seite **Begrüßung (Installieren)** auf **Weiter**.



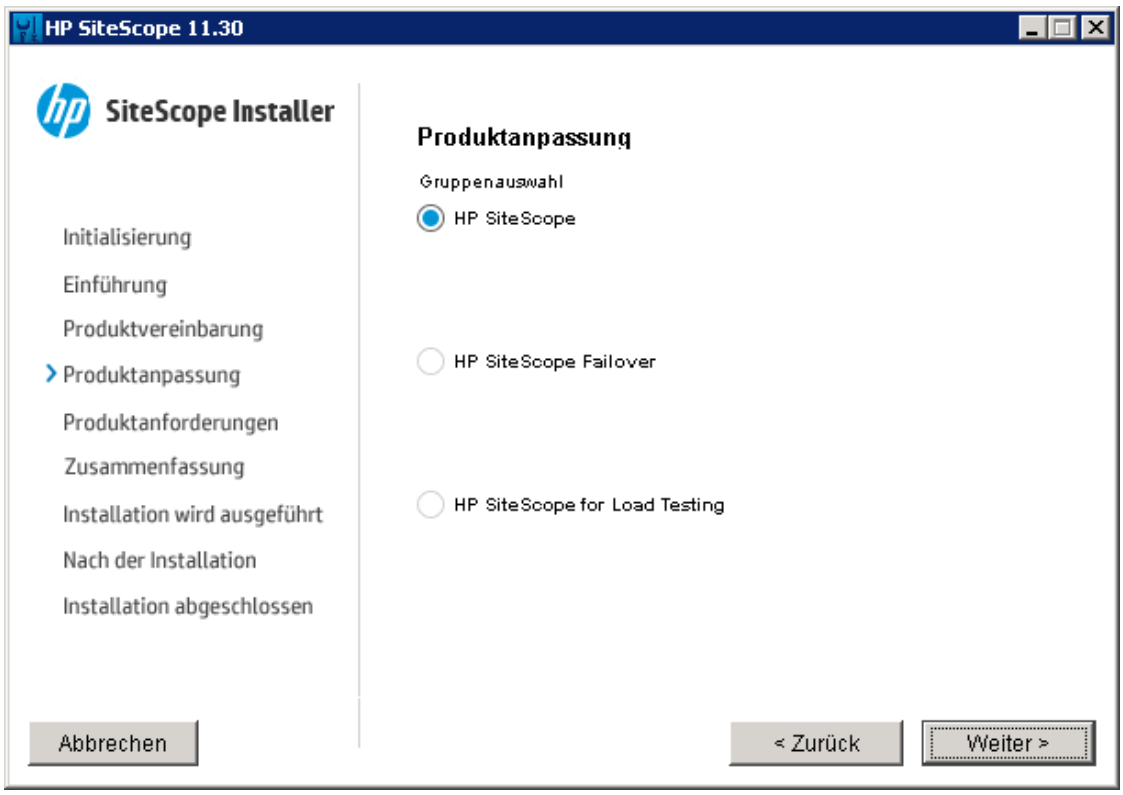
6. Die Seite **Lizenzvertrag** wird angezeigt.



Lesen Sie den SiteScope-Lizenzvertrag.

Wählen Sie **Ich bin mit den Bedingungen des Lizenzvertrags einverstanden** zum Installieren von SiteScope aus und klicken Sie dann auf **Weiter**.

7. Wählen Sie auf der Seite zur Produktanpassung den Installationstyp für SiteScope.

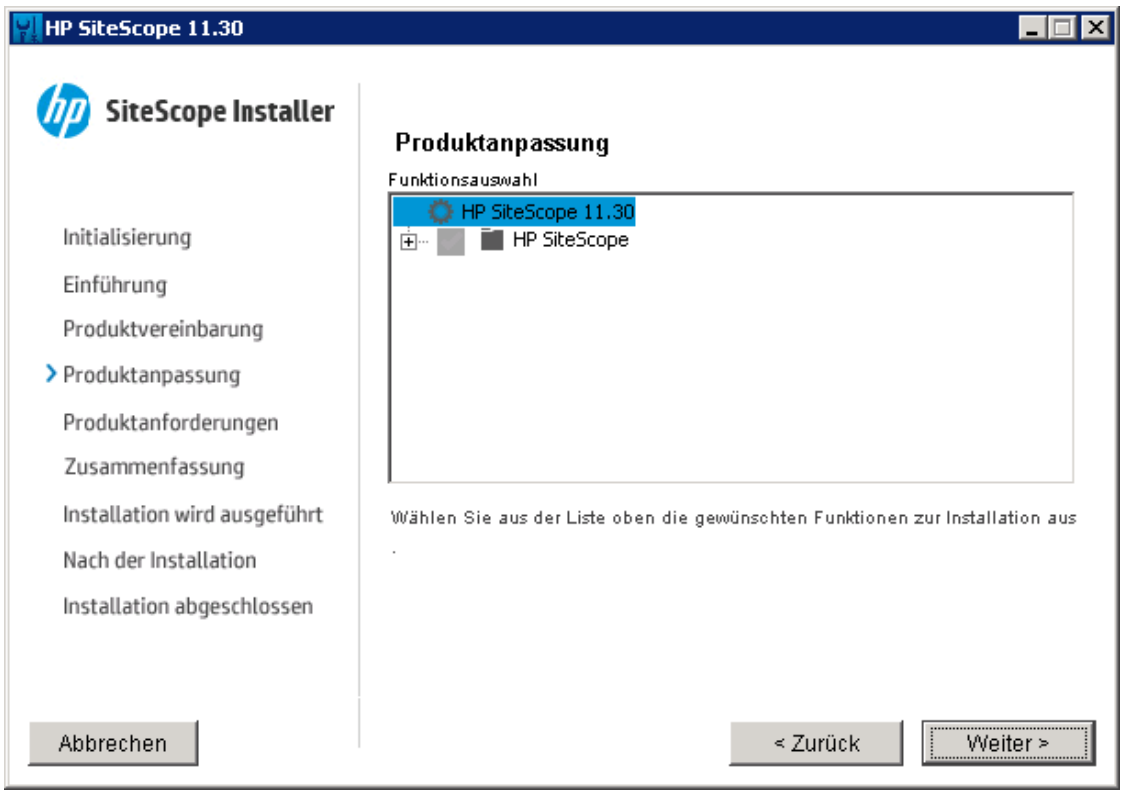


- **HP SiteScope.** Hierbei handelt es sich um die SiteScope-Standardinstallation.
- **HP SiteScope Failover.** Diese Installation bietet eine Sicherung, damit die Überwachungsinfrastruktur zur Verfügung steht, wenn ein primärer SiteScope-Server ausfällt.
- **HP SiteScope for Load Testing.** Dieser Installationstyp wird nur mit der Installation von HP LoadRunner oder HP Performance Center verwendet. Er ermöglicht den Benutzern das Definieren und Verwenden von SiteScope-Monitoren in einer LoadRunner- oder Performance Center-Applikation. SiteScope bietet zusätzliche Überwachungsmöglichkeiten, die die nativen LoadRunner- und Performance Center-Monitore ergänzen. Weitere Informationen hierzu finden Sie in den jeweiligen Dokumentationen zu LoadRunner oder Performance Center.

  Hinweis: Diese Installationsoption steht nicht zur Verfügung, wenn Sie die Installation auf Linux-Plattformen durchführen.

Klicken Sie auf **Weiter**, um fortzufahren.

8. Wählen Sie im Bildschirm für die Auswahl der Funktionen die Installationsoption.

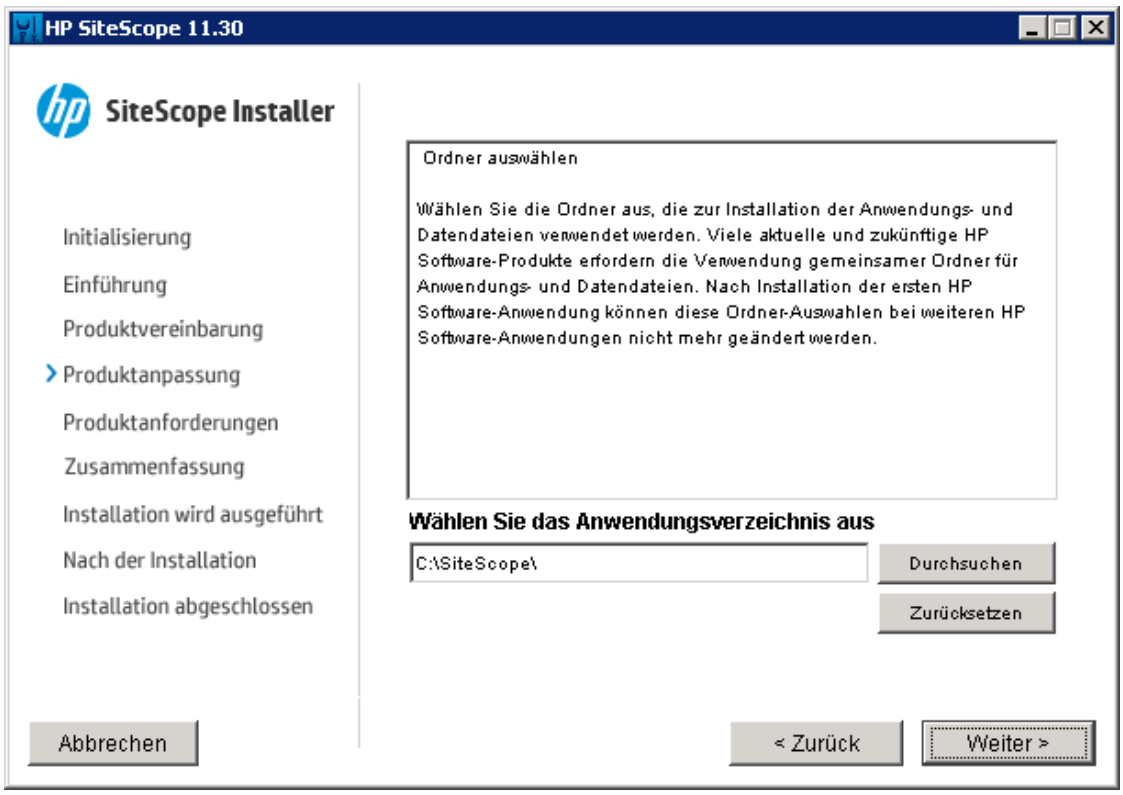


- **HP SiteScope.** Installiert SiteScope als 64-Bit-Applikation auf einem 64-Bit-Betriebssystem.

Klicken Sie auf **Weiter**, um fortzufahren.

9. Wenn Sie die Installation auf Linux-Plattformen durchführen, wird SiteScope automatisch im Verzeichnis **/opt/HP/SiteScope/** installiert. Fahren Sie mit Schritt 10 fort.

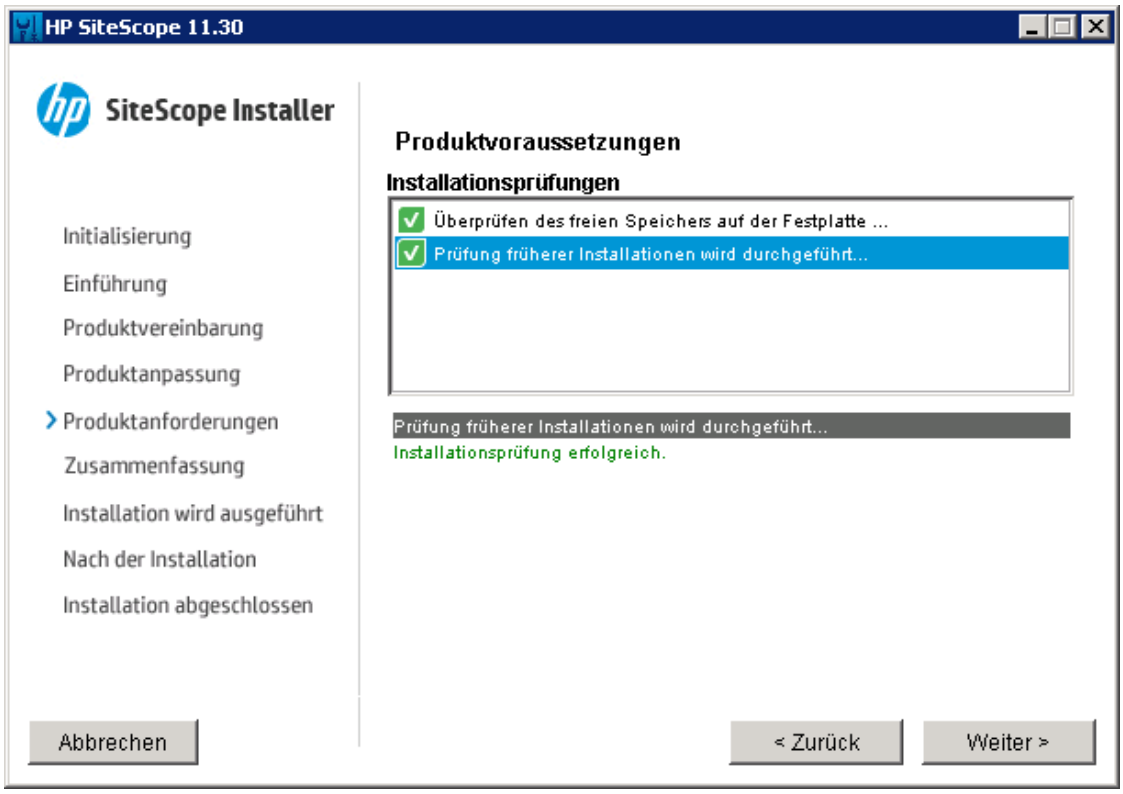
   Die Seite für das Auswählen der Ordner wird angezeigt.



   Akzeptieren Sie den Standardverzeichnis-Speicherort oder klicken Sie auf **Durchsuchen**, um ein anderes Verzeichnis auszuwählen. Wenn Sie ein anderes Verzeichnis auswählen, darf der Name des Installationspfads keine Leerzeichen oder nichtlateinischen Buchstaben enthalten und muss mit einem Ordner namens **SiteScope** enden (bitte beachten Sie beim Ordnernamen die Groß- oder Kleinschreibung). Zum Wiederherstellen des Standardinstallationspfads klicken Sie auf **Zurücksetzen**.

   Klicken Sie auf **Weiter**, um fortzufahren.

10. Die Seite für Installallationsprüfungen wird angezeigt und die Überprüfungsverfahren werden durchgeführt.

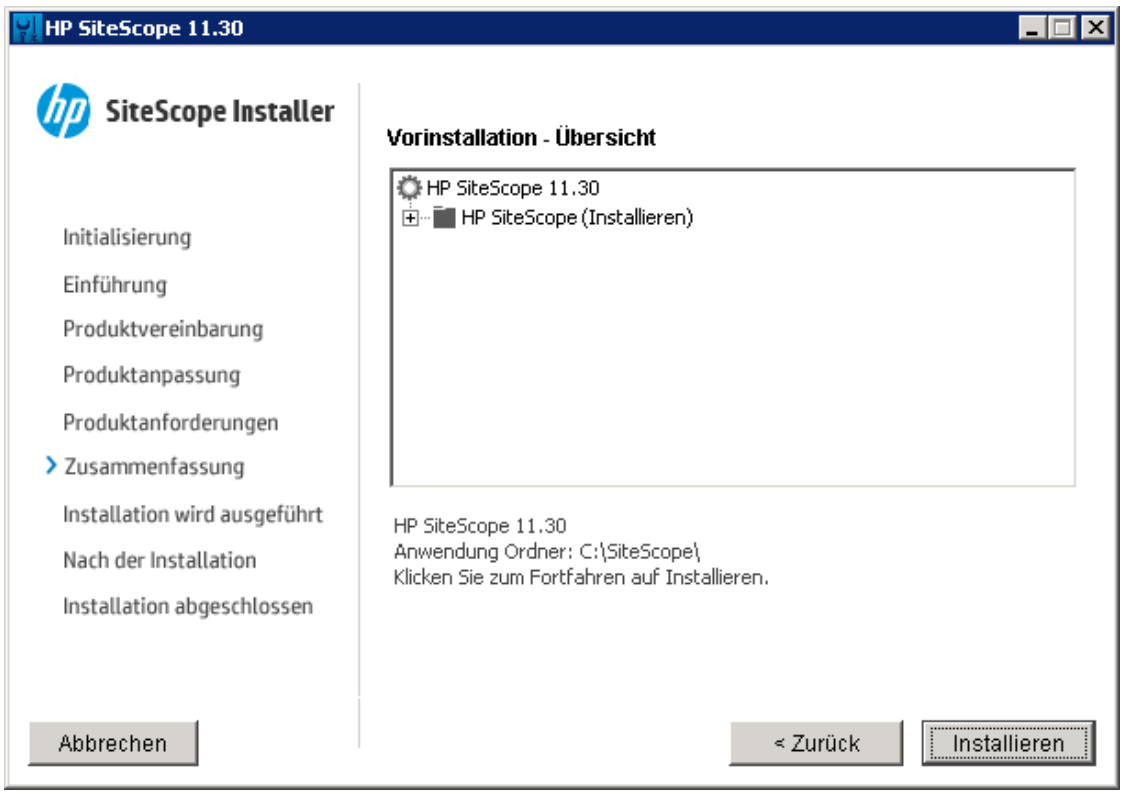


Klicken Sie auf **Weiter**, nachdem die Überprüfung des freien Speicherplatzes erfolgreich abgeschlossen wurde.

War die Überprüfung des freien Speicherplatzes nicht erfolgreich, gehen Sie folgendermaßen vor:

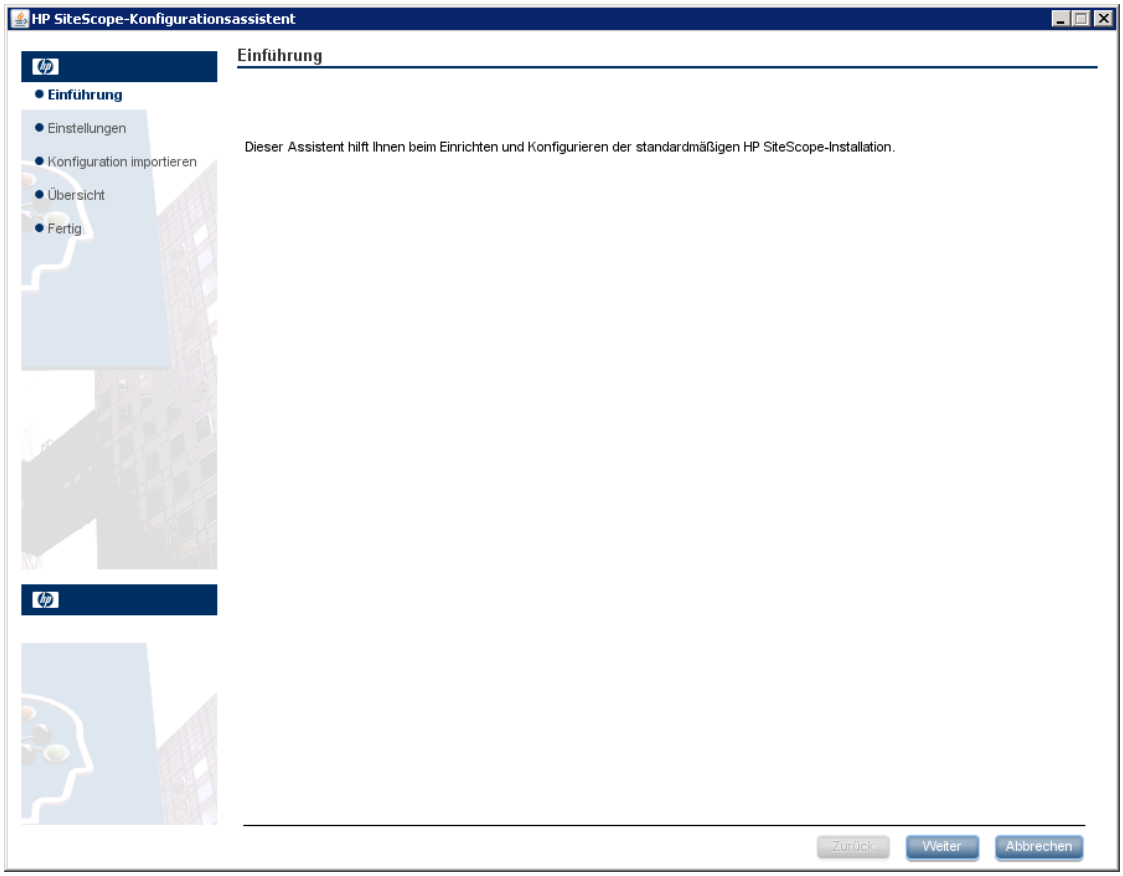
- Schaffen Sie freien Speicherplatz, z. B. durch die Verwendung des Windows-Dienstprogramms zur Datenträgerbereinigung.
- Wiederholen Sie die Schritte 9 und 10.

11. Klicken Sie im Bildschirm mit der Übersicht über die Vorinstallation auf **Installieren**.



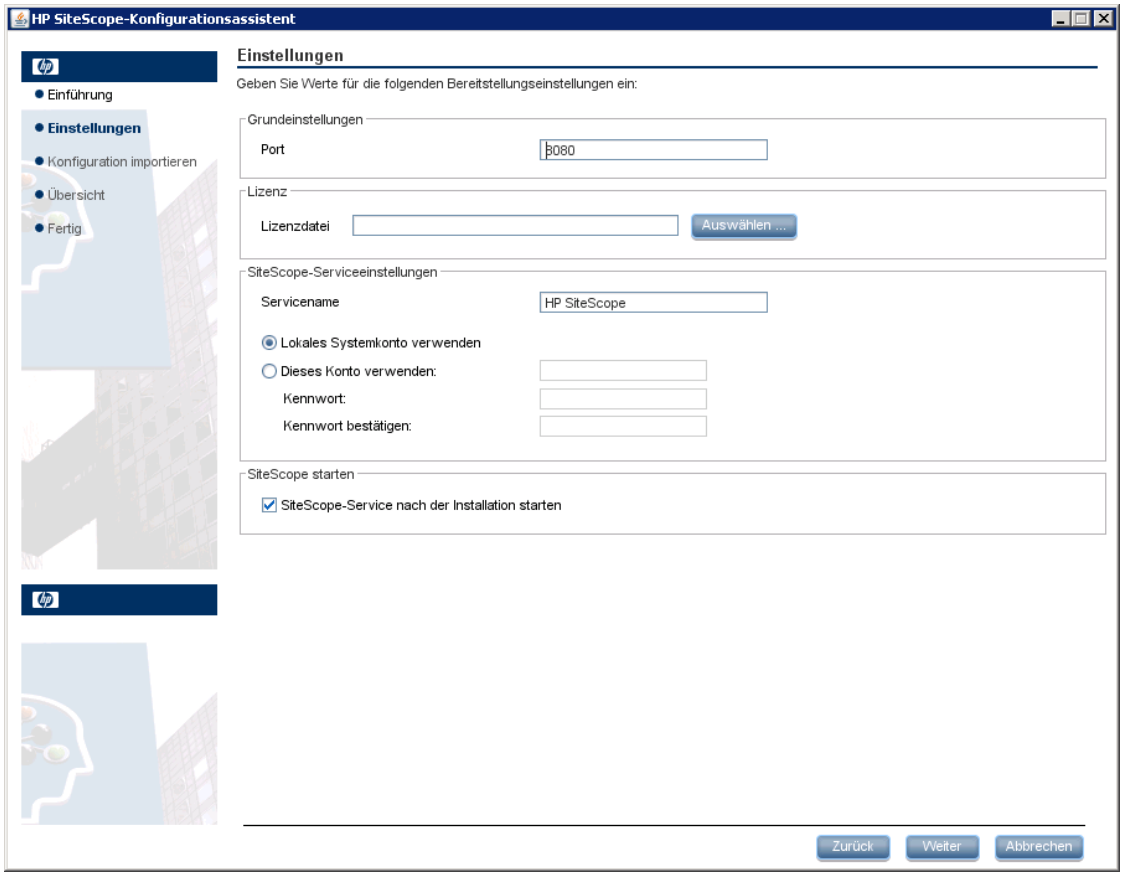
12. Der Installationsbildschirm wird angezeigt und das Installationsprogramm wählt die erforderlichen SiteScope-Softwarekomponenten aus und installiert sie. Alle Softwarekomponenten und deren Installationsverlauf werden auf der Seite während der Installation angezeigt.

13. Nach der Installation der SiteScope-Komponenten wird die Seite des SiteScope-Konfigurationsassistenten angezeigt.



Klicken Sie auf **Weiter**.

14. Die Seite **Einstellungen** des SiteScope-Konfigurationsassistenten wird angezeigt.



Geben Sie die erforderlichen Konfigurationsinformationen ein und klicken Sie auf **Weiter**:

- **Port.** Die SiteScope-Portnummer. Wird die Portnummer bereits verwendet (eine Fehlermeldung wird angezeigt), geben Sie einen anderen Port ein. Falls erforderlich, können Sie den Port später mithilfe des Konfigurationswerkzeugs ändern. Der Standardport ist `8080`.

- **Lizenzdatei.** Geben Sie den Pfad für die Lizenzdatei ein oder klicken Sie auf **Auswählen** und wählen Sie dann die SiteScope-Lizenzschlüsseldatei aus. Zu diesem Zeitpunkt müssen Sie die Lizenzinformationen noch nicht eingeben, da nach einer normalen SiteScope-Installation automatisch die Lizenz der SiteScope Community-Edition aktiviert wird. Um die SiteScope-Funktionalität über die in der Community-Edition verfügbaren Funktionen hinaus zu erweitern, müssen Sie die Lizenz einer kommerziellen Edition erwerben (siehe "Aktualisieren der SiteScope-Versionslizenz" auf Seite 36).

- **Lokales Systemkonto verwenden** (gilt nicht für Linux-Installationen). Standardmäßig wird SiteScope für die Ausführung als **lokales Systemkonto** installiert. Dieses Konto verfügt über weitreichende Privilegien auf dem lokalen Computer und über Zugriff auf meisten Systemobjekte. Wird SiteScope unter einem lokalen Systemkonto ausgeführt, versucht es, eine Verbindung zu Remoteservern unter Verwendung der in SiteScope konfigurierten Anmeldeinformationen des Servers herzustellen.

  Hinweis: Es empfiehlt sich jedoch, den SiteScope-Dienst so zu konfigurieren, dass die Anmeldung als Benutzer mit Domänenadministratorberechtigungen erfolgt, da das lokale Systemkonto möglicherweise nicht über ausreichende Berechtigungen verfügt (das lokale Systemkonto verfügt über Domänenadministrator-Benutzerberechtigungen in einer Domänenumgebung und über integrierte Administrator-Benutzerberechtigungen in einer Nicht-Domänenumgebung).

- **Dieses Konto verwenden** (gilt nicht für Linux-Installationen). Wählen Sie diese Option, um das Benutzerkonto des SiteScope-Diensts zu ändern. Sie können den SiteScope-Dienst so ändern, dass eine Anmeldung als Benutzer mit Domänenadministratorberechtigungen durchgeführt wird. So erhält SiteScope Zugriffsberechtigungen für das Überwachen von Serverdaten innerhalb der Domäne. Geben Sie ein Konto und ein Kennwort (bestätigen Sie das Kennwort) für den Zugriff auf die Remoteserver ein.

  Hinweis: Wurde SiteScope für die Ausführung als benutzerdefiniertes Benutzerkonto installiert, muss das verwendete Konto über die Berechtigung **Anmelden als Dienst** verfügen. So weisen Sie einem Benutzer Zugriff auf die Anmeldung als Dienst zu:

  i. Doppelklicken Sie in der Windows-Systemsteuerung auf **Verwaltung**.

  ii. Doppelklicken Sie auf **Lokale Sicherheitsrichtlinie** und wählen Sie **Lokale Richtlinie > Zuweisen von Benutzerrechten > Anmelden als Dienst**.

  iii. Klicken Sie auf die Schaltfläche **Benutzer oder Gruppe hinzufügen**, wählen Sie den Benutzer aus, dem Sie Zugriff auf die Anmeldung als Dienst zuweisen möchten, und klicken Sie dann auf **OK**.

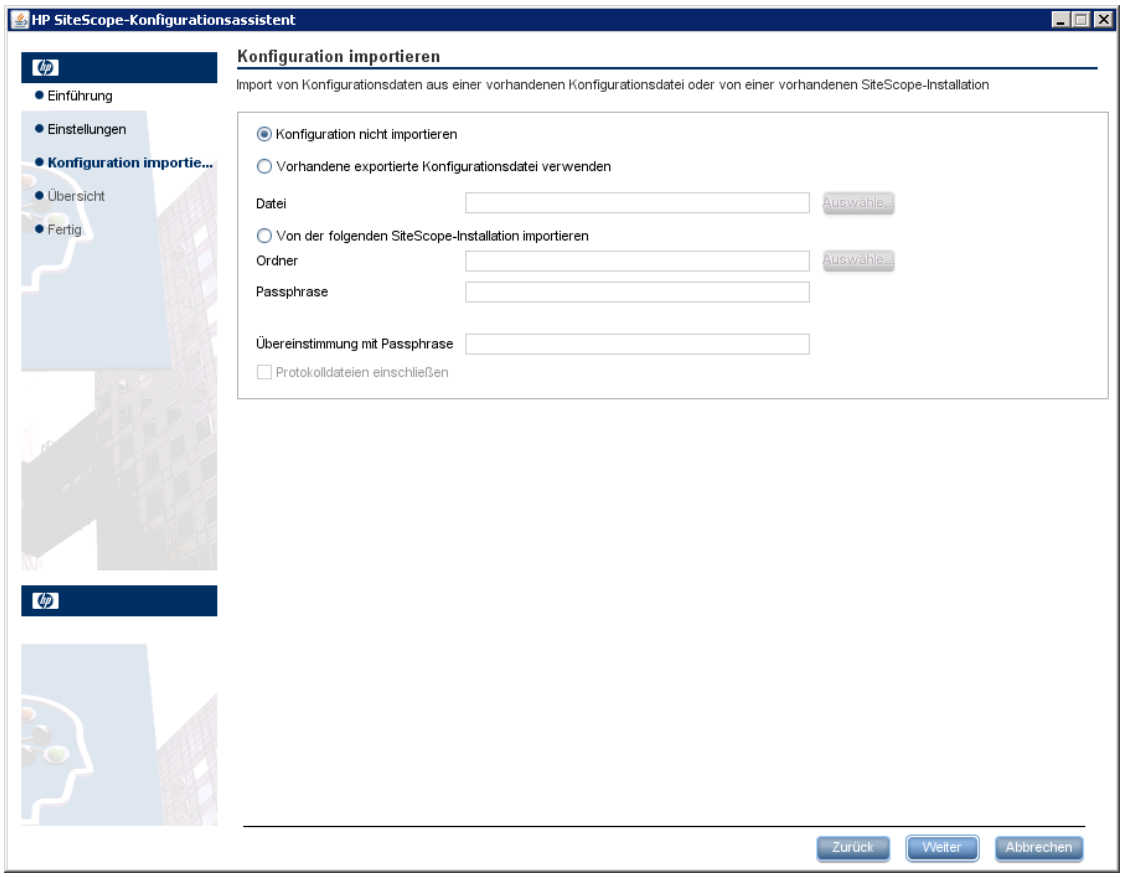
  iv. Klicken Sie auf **OK**, um die aktualisierte Richtlinie zu speichern.

- **Servicename** (gilt nicht für Linux-Installationen). Der Name des SiteScope-Diensts. Ist auf dem Computer eine Vorgängerversion von SiteScope installiert, geben Sie einen anderen Namen für

den SiteScope-Dienst ein. Der Standarddienstname ist `SiteScope`.

- **Starten Sie den SiteScope-Dienst nach der Installation** (gilt nicht für Linux-Installationen). Startet den SiteScope-Dienst automatisch nach Abschluss der Installation.

15. Die Seite **Konfiguration importieren** wird angezeigt, über die Sie vorhandene SiteScope-Konfigurationsdaten in die neue SiteScope-Installation importieren können.



Wählen Sie eine der folgenden Optionen aus und klicken Sie auf **Weiter**:

- **Konfiguration nicht importieren.**

- **Vorhandene exportierte Konfigurationsdatei verwenden.** Diese Option ermöglicht Ihnen das Verwenden von SiteScope-Daten wie beispielsweise Vorlagen, Protokollen, Monitorkonfigurationsdateien usw. aus einer vorhandenen exportierten Konfigurationsdatei. Die SiteScope-Daten werden mithilfe des Konfigurationswerkzeugs exportiert und im ZIP-Format gespeichert. Klicken Sie auf die Schaltfläche **Auswählen** und navigieren Sie zu der

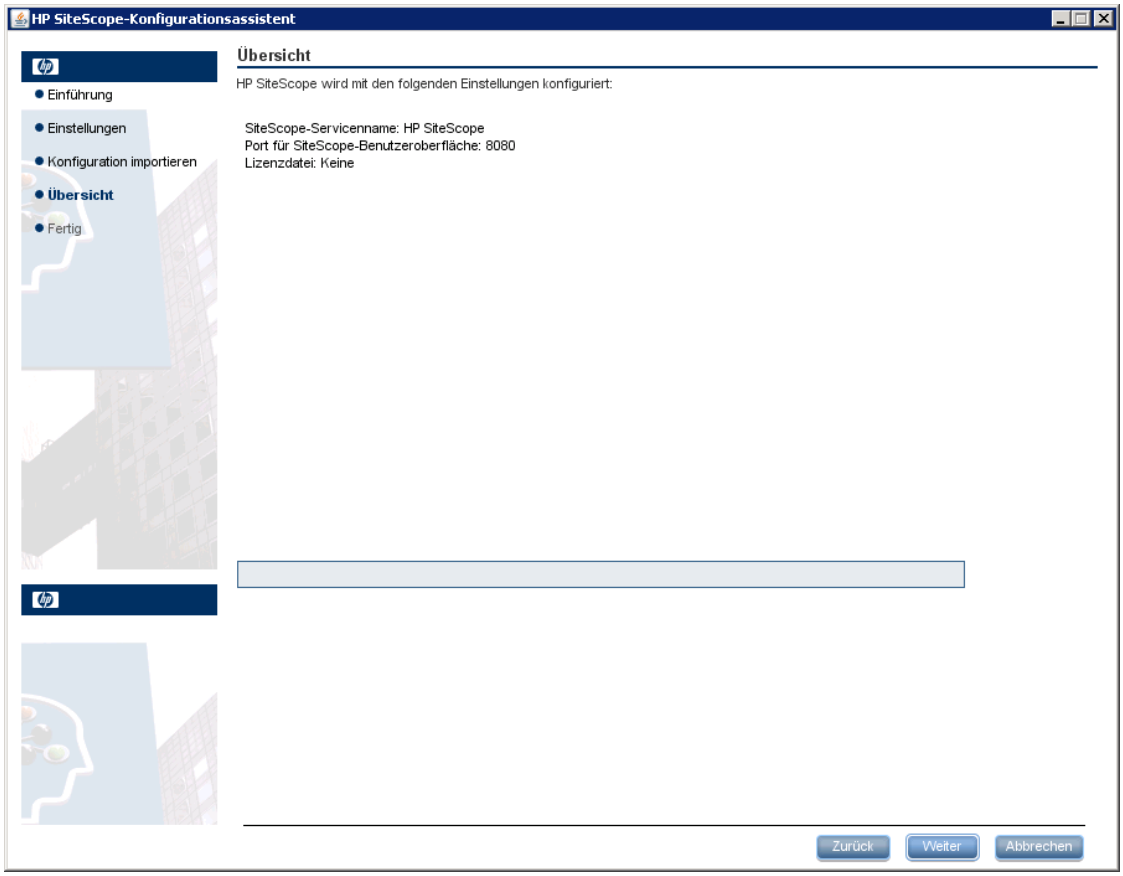
Benutzerdatendatei, die Sie importieren möchten.

- **Von der folgenden SiteScope-Installation importieren.** Klicken Sie auf die Schaltfläche **Auswählen** und navigieren Sie zu dem SiteScope-Installationsordner, aus dem Sie die Konfigurationsdaten importieren möchten.
  - **Protokolldateien einschließen.** Diese Option ermöglicht Ihnen das Importieren von Protokolldateien aus dem ausgewählten SiteScope-Installationsordner.
- Wenn SiteScope für das Ausführen der mit einer schlüsselverwalteten Verschlüsselung konfiguriert wurde, geben Sie die Passphrase für den KeyStore des SiteScope-Servers im Feld **Passphrase** ein. Bestätigen Sie die Passphrase im Feld **Übereinstimmung mit Passphrase**. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208. Diese Felder sind deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

Hinweis:

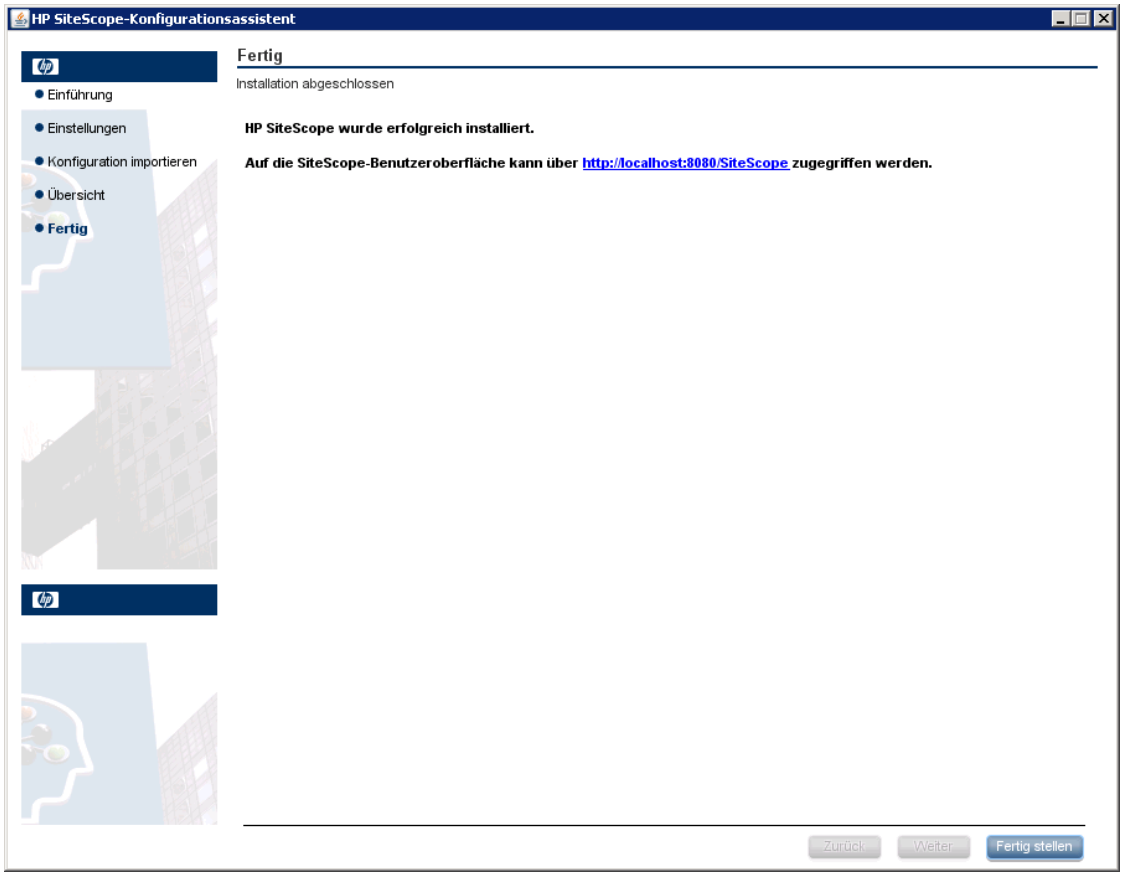
- Wenn Sie Konfigurationsdaten von einer SiteScope-Installation auf eine andere verschieben, müssen Sie darauf achten, dass sich der SiteScope-Server, von dem Sie die Konfigurationsdaten übernehmen, in derselben Zeitzone befindet wie der SiteScope-Server, auf den die Daten importiert werden sollen.
- Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.

16. Die Seite **Übersicht** wird angezeigt.



Stellen Sie sicher, dass die Informationen richtig sind, und klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren, oder auf die Schaltfläche **Zurück**, um zur vorherigen Seite zurückzukehren und Ihre Auswahl zu ändern.

17. Die Seite **Fertig** wird angezeigt.

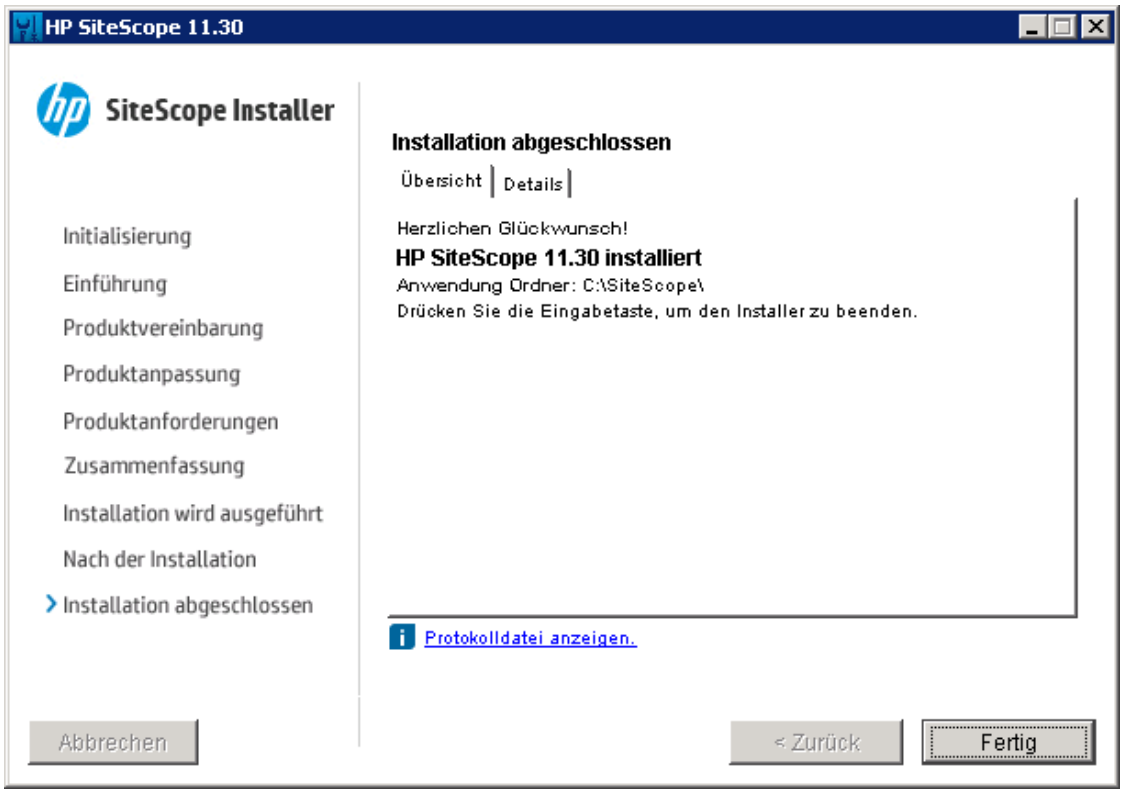


Um auf die SiteScope-Benutzeroberfläche zuzugreifen, klicken Sie auf die Verbindungsadresse für diese Installation von SiteScope.

Hinweis: Wenn Sie die Option **SiteScope-Service nach der Installation starten** auf der Seite **Konfigurationseinstellungen** nicht ausgewählt haben, müssen Sie den SiteScope-Dienst starten, bevor Sie eine Verbindung zu SiteScope herstellen können. Weitere Informationen finden Sie unter "Erste Schritte mit SiteScope" auf Seite 242.

Klicken Sie auf **Fertig stellen**, um den SiteScope-Konfigurationsassistenten zu schließen.

18. Nach Abschluss der Installation wird das Fenster **Installation abgeschlossen** geöffnet, in dem eine Zusammenfassung der verwendeten Installationspfade und der Installationsstatus angezeigt werden.



Wurde die Installation nicht erfolgreich durchgeführt, überprüfen Sie die Installationsprotokolldatei auf Fehler, indem Sie auf den Link **Protokolldatei anzeigen** im Fenster **Installation abgeschlossen** klicken, um die Protokolldatei in einem Webbrowser anzuzeigen.

Weitere Informationen zu den installierten Paketen erhalten Sie, wenn Sie auf die Registerkarte **Details** klicken.

Klicken Sie auf **Fertig**, um das Installationsprogramm zu schließen.

Wenn das Installationsprogramm festlegt, dass ein Neustart des Servers erforderlich ist, werden Sie aufgefordert, den Server neu zu starten.

19. Die neusten verfügbaren Funktionen erhalten Sie, indem Sie den neusten SiteScope-Patch (sofern verfügbar) von demselben Speicherort wie beim Installieren von SiteScope herunterladen und installieren. Informationen über den Zugriff auf die SiteScope-Schnittstelle finden Sie unter "Verbinden mit SiteScope" auf Seite 244.

20. Nach der Installation von SiteScope in einer Linux-Umgebung legen Sie die Berechtigungen für das SiteScope-Installationsverzeichnis fest und erteilen Sie Lese-, Schreib- und Ausführungsberechtigungen für das Benutzerkonto, das zum Ausführen der SiteScope-Applikation verwendet wird. Die Berechtigungen müssen auch für alle Unterverzeichnisse des SiteScope-Installationsverzeichnisses festgelegt werden.

Installieren von SiteScope mithilfe des Installationsassistenten auf einem Computer ohne X11 Server

Wenn Sie SiteScope mithilfe des Installationsassistenten auf einem Computer ohne X11 Server installieren möchten, haben Sie folgende Möglichkeiten:

- Verwenden eines VNC-Servers (auf vielen Linux-Systems ist ein VNC-Server standardmäßig installiert).
- Bearbeiten der DISPLAY-Umgebungsvariable, sodass die Programme X-Server auf einem anderen Computer verwenden können.

So installieren Sie SiteScope auf einem Computer ohne X11 mithilfe eines VNC-Servers:

1. Führen Sie in der Befehlszeile **vncserver** aus. Nach der Ausführung wählen Sie ein Kennwort aus und notieren die Anzeige, die der VNC-Server verwendet (standardmäßig `:1`)
2. Stellen Sie eine Verbindung zu Ihrem SiteScope-Computer über einen VNC-Client her. Verwenden Sie dabei folgendes Format: hostname:display. Beispielsweise `sitescope.company.name:1`
3. Navigieren Sie in der Konsole, die geöffnet wird, in das SiteScope-Installationsverzeichnis und führen Sie die Installation wie gewohnt aus.

So installieren Sie SiteScope auf einem Computer ohne X11 durch Umgehung von X:

1. Führen Sie ein beliebiges Linux-System mit einem X-Server aus oder installieren Sie einen X-Server unter Windows (beispielsweise `xming`).
2. Stellen Sie sicher, dass die X-Zugriffssteuerung dem SiteScope-Computer das Herstellen einer Verbindung ermöglicht. Auf Linux-Plattformen verwenden Sie `man xhost`. Für Windows-

Plattformen finden Sie weitere Informationen in der Dokumentation zur X-Server-Implementierung.

3. Führen Sie **export DISPLAY=x-server.machine.name:display** auf Ihrem SiteScope-Computer aus (der Wert für DISPLAY ist standardmäßig `0`).

4. Navigieren Sie in das SiteScope-Installationsverzeichnis in derselben Shell und führen Sie die Installation wie gewohnt durch.

Kapitel 13: Installieren auf Linux-Plattformen unter Verwendung des Konsolenmodus

Sie können SiteScope unter Linux über eine Befehlszeile oder den Konsolenmodus installieren. Verwenden Sie diese Option, wenn Sie SiteScope auf einem Remoteserver installieren oder andere Gründe vorliegen, die gegen die Verwendung der Installationsoption über die Benutzeroberfläche sprechen.

Hinweis: Die Option zum Installieren von HP Operations Agent direkt aus dem SiteScope-Konsolenmodus wurde entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

So installieren Sie SiteScope unter Linux unter Verwendung des Konsolenmodus:

1. Laden Sie die Installationsdatei (**SiteScope_11.30_Linux.zip**) auf den Computer herunter, auf dem Sie SiteScope installieren wollen. Sie können die SiteScope-Installationsdatei auch auf einen Datenträger oder an einen Netzwerkstandort kopieren, wo sie für das Benutzerkonto, das für die Installation von SiteScope verwendet wird, zugänglich ist.

   SiteScope ist wie folgt über HP Systems verfügbar:

Kunde	Download-Optionen
Für Evaluierungskunden	Link für elektronische Download-Evaluierung HP Software Partner Central für HP-autorisierte Softwarepartner (Für die oben genannten Links sind HP Passport-Konten erforderlich. Registrieren Sie sich für einen HP Passport unter http://h20229.www2.hp.com/passport-registration.html.)

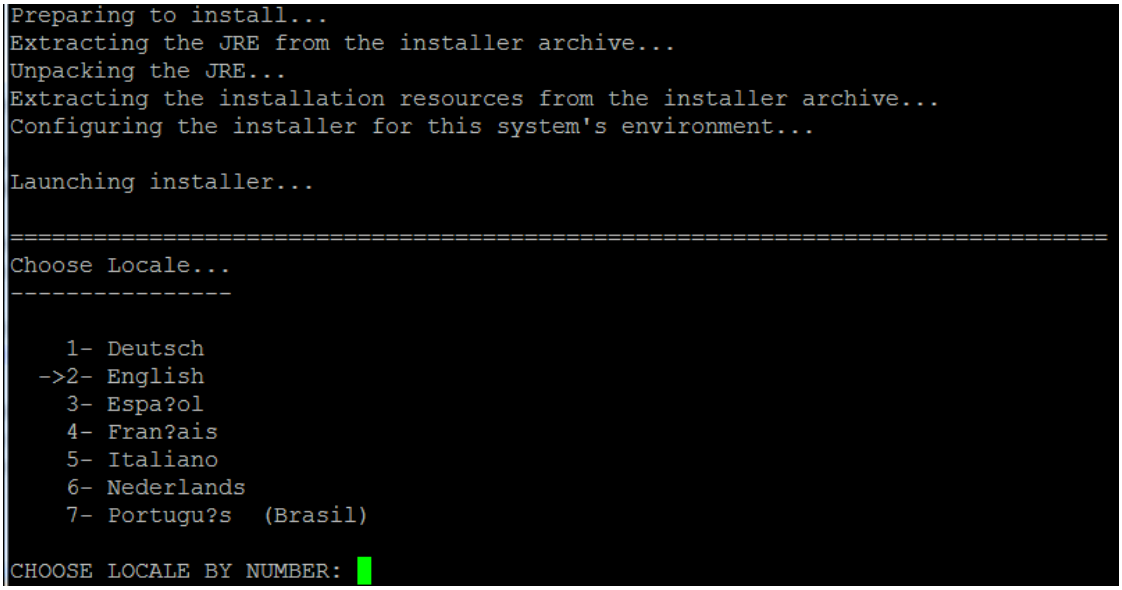
Kunde	Download-Optionen
Für neue Kunden	Elektronischer Software-Download. Der Kunde erhält einen Link per E-Mail, über den die Software heruntergeladen werden kann. Dieser Link ist auf die Bestellung abgestimmt.
Aktualisierungen für bestehende Kunden	https://h20575.www2.hp.com/usbportal/softwareupdate.do **Voraussetzungen:** a. Sie müssen über ein HP Passport-Konto verfügen, um auf den obigen Link zugreifen zu können. Ferner ist eine Support Agreement-ID (SAID) erforderlich, um Aktualisierungen über das SSO-Portal zu erhalten. Informationen zum Registrieren für einen HP Passport finden Sie unter http://h20229.www2.hp.com/passport-registration.html. Details zum Aktivieren der SAID finden Sie unter **FAQ** auf der Website Software Support Online. b. Für das Software-Upgrade ist ein neuer Lizenzschlüssel erforderlich. Setzen Sie sich mit Ihrem HP Support-Ansprechpartner für Vertragsverlängerungen in Verbindung, um zuerst die Migration das Produktvertrags zu beantragen. Navigieren Sie nach Abschluss der Vertragsmigration zum Portal für eigene Software-Updates (https://h20575.www2.hp.com/usbportal/softwareupdate.do), und klicken Sie dort auf die Registerkarte **Get Licensing**, um den oder die neuen Lizenzschlüssel zu erhalten. **So laden Sie Software-Updates herunter:** a. Wählen Sie die Option **My software updates** aus. b. Erweitern Sie **Application Performance Management**, wählen Sie die benötigten HP SiteScope 11.30 Software-E-Medien aus und klicken Sie dann auf **Get software updates**. c. Klicken Sie auf der Registerkarte **Selected Products** auf **Get Software** für die gewünschten Produktaktualisierungen und folgen Sie den Anweisungen auf der Seite, um die Software herunterzuladen.

2. Führen Sie den folgenden Befehl aus:

```
HPSiteScope_11.30_setup.bin -i console
```

Das Installationsskript veranlasst die Java Virtual Machine, mit der Installation zu beginnen.

3. Der Bildschirm für die Auswahl des Gebietsschemas wird angezeigt.

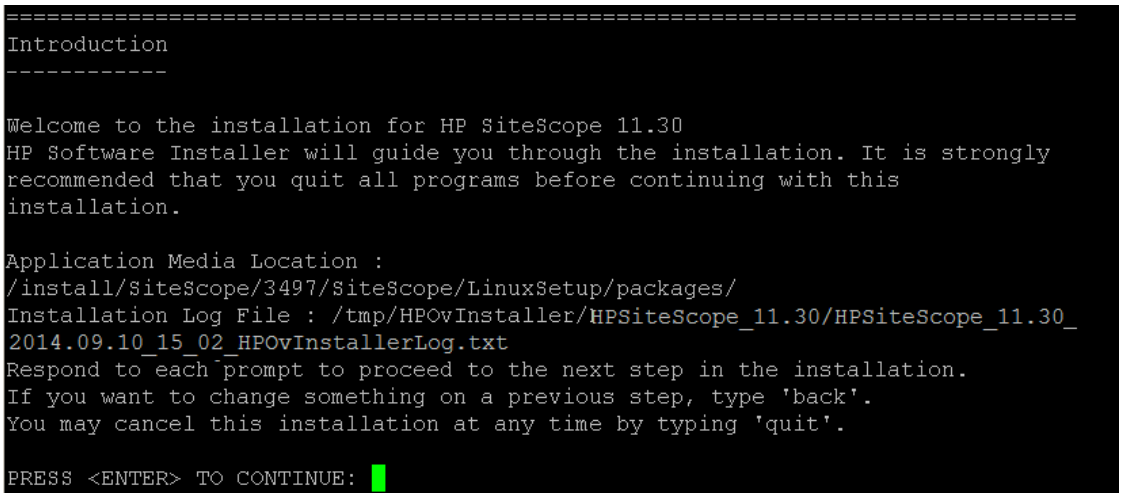


Geben Sie die Zahl für das gewünschte Gebietsschema ein und drücken Sie die EINGABETASTE, um fortzufahren.

4. Es wird ein Bestätigungsbildschirm angezeigt.

Drücken Sie die EINGABETASTE, um fortzufahren.

5. Der Bildschirm **Introduction** wird angezeigt.



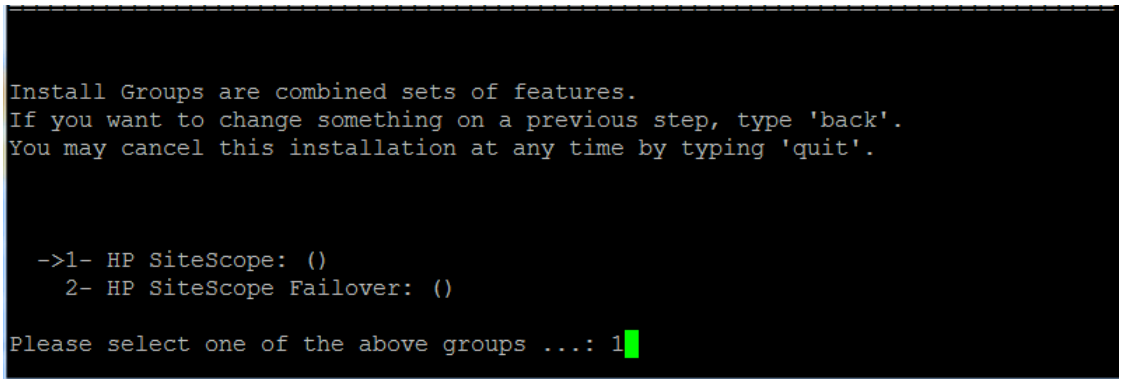
Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

6. Der Text der Lizenzvereinbarung wird angezeigt. Die SiteScope-Lizenzvereinbarung umfasst mehrere Seiten. Lesen Sie die angezeigte Seite. Drücken Sie die EINGABETASTE, um mit der jeweils nächsten Seite fortzufahren. Wenn Sie alle Seiten der Lizenzvereinbarung angezeigt haben, haben Sie die Möglichkeit, die Lizenzvereinbarung zu akzeptieren oder abzulehnen.

Um SiteScope installieren zu können, müssen Sie die Bedingungen der Lizenzvereinbarung akzeptieren. Die Standardauswahl besteht in der Ablehnung der Vereinbarung. Um die Lizenzvereinbarung zu akzeptieren und mit der Installation fortzufahren, wählen Sie Ja.

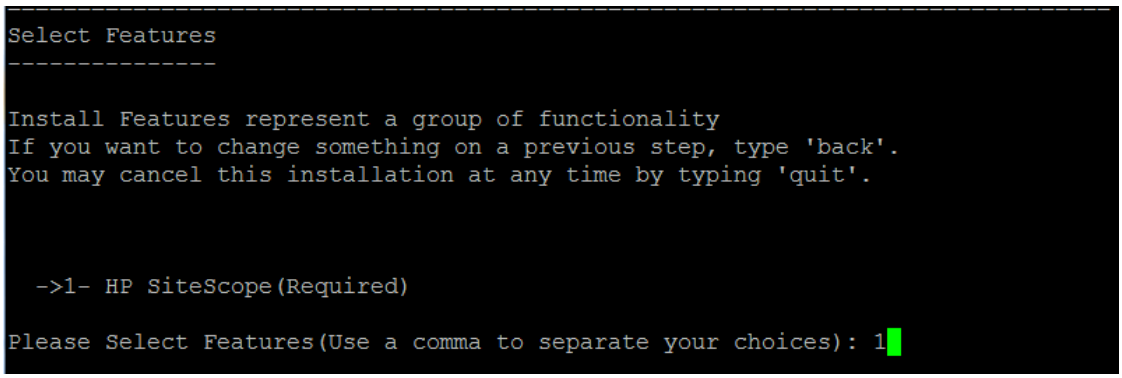
Hinweis: Um die Installation nach Ansicht der SiteScope-Lizenzvereinbarung abzubrechen, geben Sie N ein.

7. Der Bildschirm für den SiteScope-Installationstyp wird angezeigt.



Wählen Sie den geeigneten Typ für Ihren Standort aus. Geben Sie die Zahl für den Installationstyp ein und drücken Sie die EINGABETASTE, um fortzufahren.

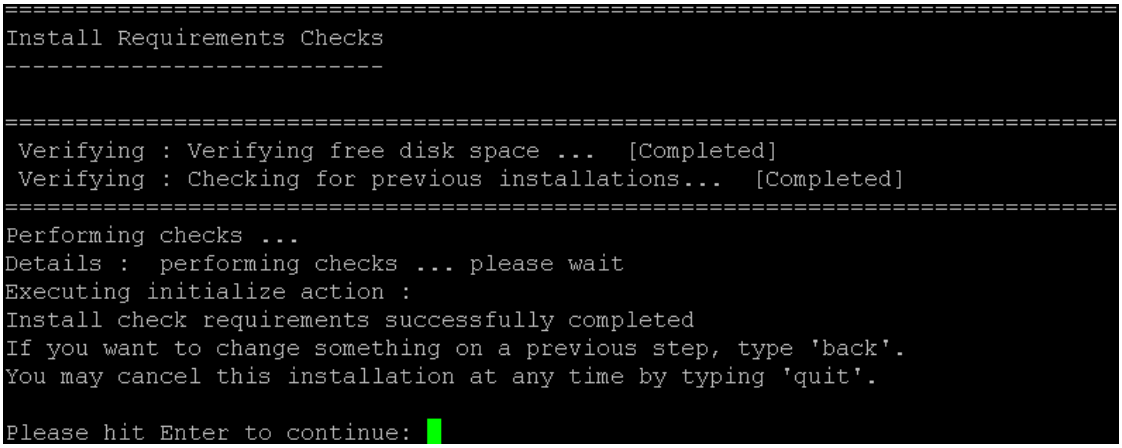
8. Der Bildschirm **Select Features** wird angezeigt.



Geben Sie die Zahl `1` ein, um SiteScope (erforderlich) zu installieren.

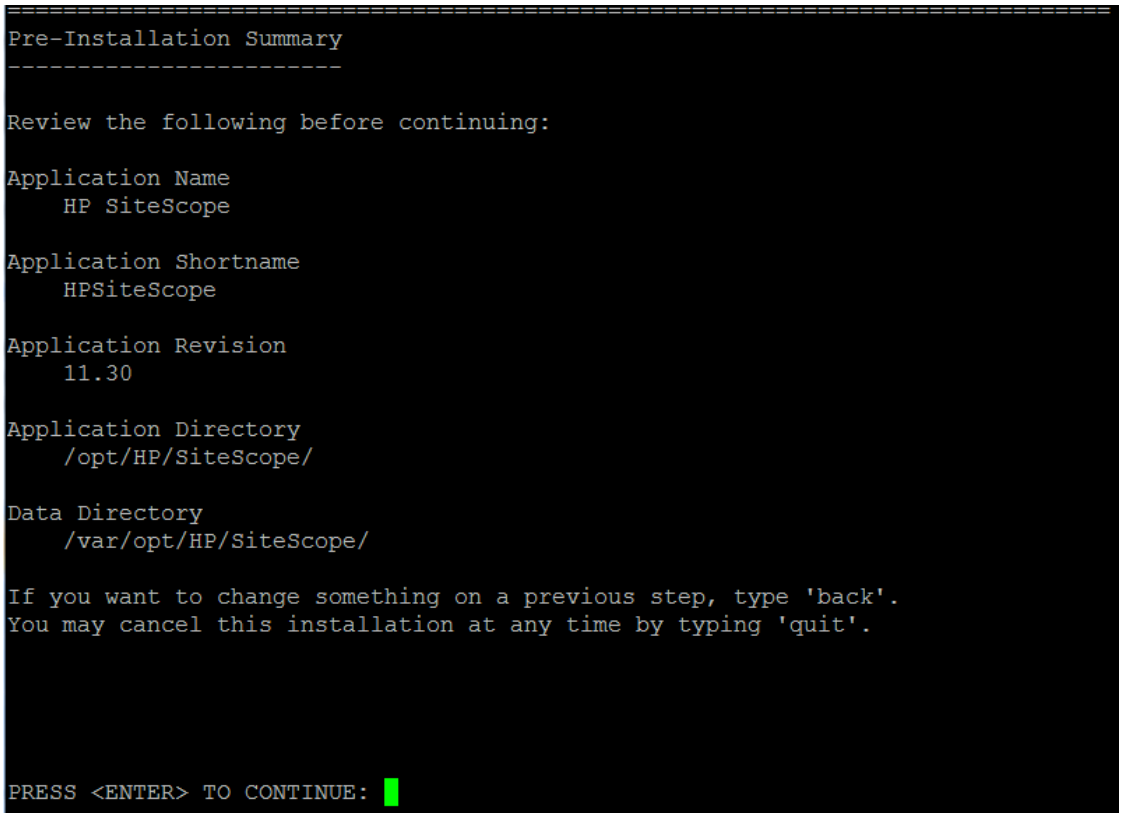
Drücken Sie die `EINGABETASTE`, um mit der Installation fortzufahren.

9. Der Bildschirm **Install Requirements Checks** wird angezeigt.



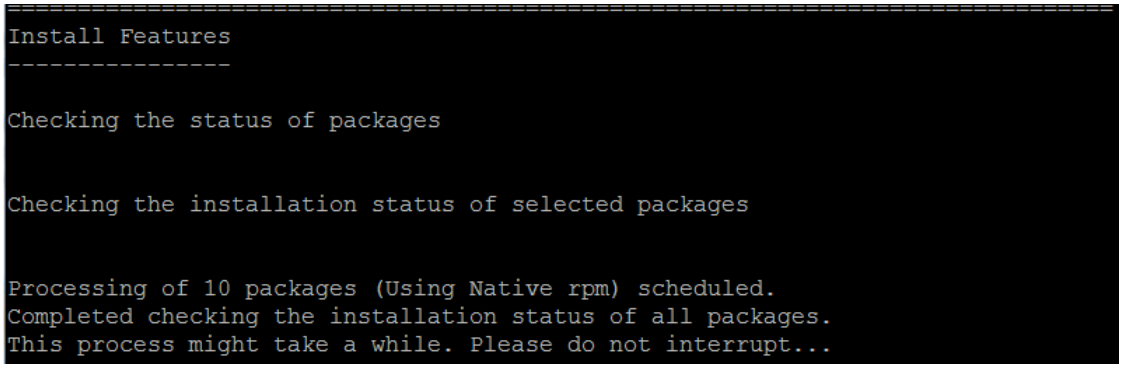
Drücken Sie die `EINGABETASTE`, um mit der Installation fortzufahren.

10. Der Bildschirm mit einer Zusammenfassung der ausgewählten Installationsoptionen wird angezeigt.



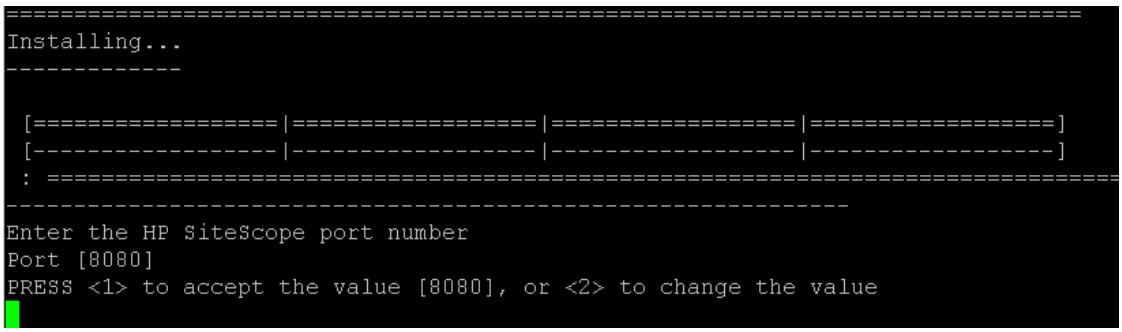
Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

11. Der Bildschirm **Install Features** wird angezeigt und die Installation beginnt.



Ist der Installationsprozess abgeschlossen, wird der Bildschirm für die Konfiguration nach der Installation geöffnet.

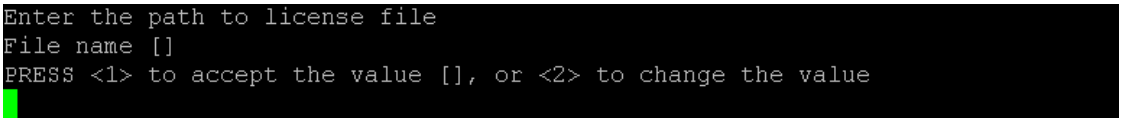
12. Der Bildschirm für die Porteingabe wird angezeigt:



Geben Sie die Zahl 1 ein, um die Standardportnummer 8080 zu akzeptieren, oder geben Sie 2 ein, um den Port zu ändern. Geben Sie anschließend eine andere Zahl ein, um die Portnummer zu ändern.

Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

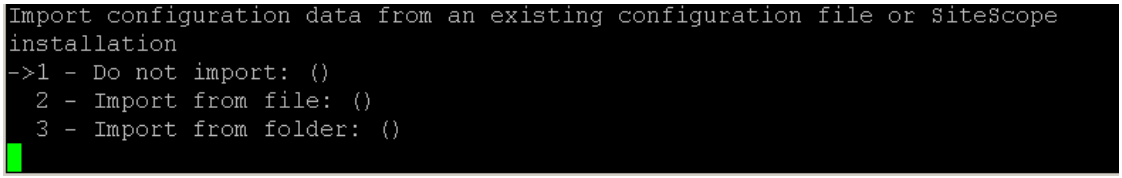
13. Die Eingabeaufforderung für den Lizenzdateipfad wird angezeigt.



Geben Sie die Zahl 1 ein, um keinen Eintrag für den Lizenzdateipfad vorzunehmen (es ist nicht erforderlich, an dieser Stelle Lizenzinformationen für die Verwendung von SiteScope, da die SiteScope Community-Editionslizenz automatisch nach einer regulären SiteScope-Installation aktiviert wird), oder geben Sie 2 und anschließend den Lizenzdateipfad im nächsten Textfeld ein.

Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

14. Der Bildschirm für den Import von Konfigurationsdaten wird angezeigt.



Geben Sie die Zahl 1 ein, wenn Sie keine Daten importieren möchten.

Geben Sie die Zahl 2 ein, wenn Sie SiteScope-Daten wie beispielsweise Vorlagen, Protokolle, Monitorkonfigurationsdateien usw. von einer vorhandenen exportierten Konfigurationsdatei übernehmen möchten. Wenn Sie diese Option auswählen, geben Sie den Pfad für die Konfigurationsdatei in das nächste Textfeld ein.

Geben Sie die Zahl 3 ein, um Konfigurationsdaten aus einem SiteScope-Installationsverzeichnis zu importieren. Wenn Sie diese Option auswählen, geben Sie den Pfad für den SiteScope-Installationsordner ein, aus dem Sie Konfigurationsdaten importieren möchten.

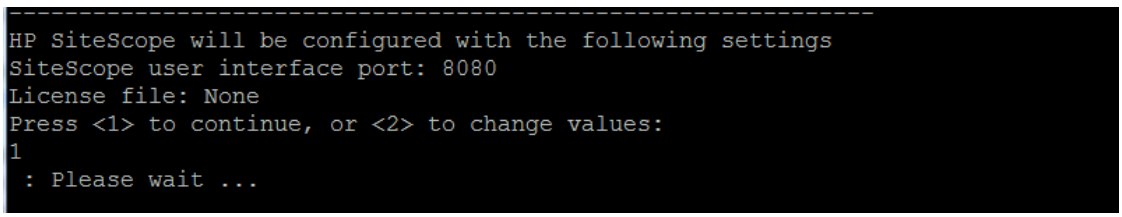
Wenn SiteScope für das Ausführen der Datenverschlüsselung der Schlüsselverwaltung konfiguriert wurde, geben Sie nach Aufforderung die Passphrase für den KeyStore des SiteScope-Servers ein und bestätigen Sie die Passphrase durch erneute Eingabe. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208.

Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

Hinweis:

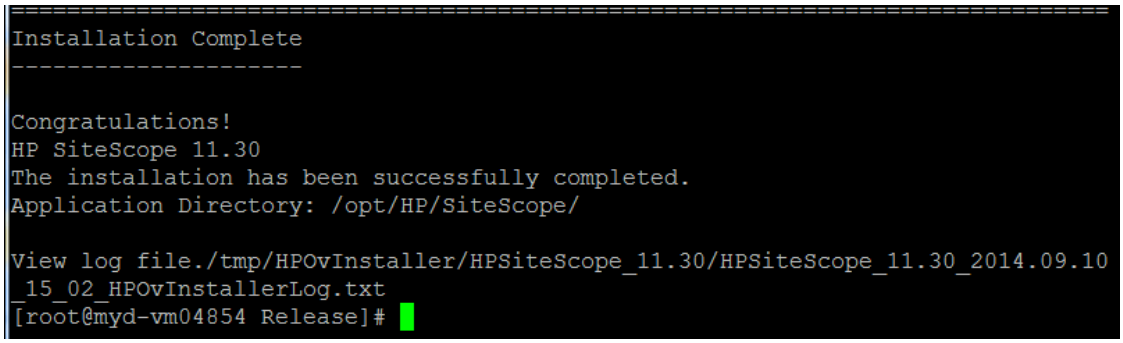
- Wenn Sie Konfigurationsdaten von einer SiteScope-Installation auf eine andere verschieben, müssen Sie darauf achten, dass sich der SiteScope-Server, von dem Sie die Konfigurationsdaten übernehmen, in derselben Zeitzone befindet wie der SiteScope-Server, auf den die Daten importiert werden sollen.
- Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.

15. Die Konsole zeigt die Installationsparameter zur Bestätigung an.



Geben Sie 1 ein, um mit der Installation unter Verwendung der angezeigten Parameter fortzufahren, oder geben Sie 2 ein, um die Werte zu ändern. Drücken Sie anschließend die EINGABETASTE.

Der Installationsprozess wird abgeschlossen. Es wird eine Installationsstatusmeldung angezeigt.



16. Legen Sie nach der Installation von SiteScope die Berechtigungen für das SiteScope-Installationsverzeichnis fest und erteilen Sie Lese-, Schreib- und Ausführungsberechtigungen für das Benutzerkonto, das zum Ausführen der SiteScope-Applikation verwendet wird. Die Berechtigungen müssen auch für alle Unterverzeichnisse des SiteScope-Installationsverzeichnisses festgelegt werden.

    Details zum Erstellen eines Nicht-Root-Benutzers zum Ausführen der SiteScope-Applikation und Informationen zum Festlegen von Kontoberechtigungen finden Sie unter "Konfigurieren eines Nicht-Root-Benutzerkontos mit Berechtigungen zum Ausführen von SiteScope" auf Seite 51.

17. Um eine Verbindung mit SiteScope herzustellen, führen Sie die Schritte in Abschnitt "Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen" auf Seite 243 aus.

Kapitel 14: Installieren von SiteScope im unbeaufsichtigten Modus

Dieses Kapitel umfasst die folgenden Themen:

Informationen zum Installieren von SiteScope im unbeaufsichtigten Modus

Sie können für SiteScope eine unbeaufsichtigte Installation durchführen. Bei einer Installation im unbeaufsichtigten Modus wird das gesamte Setup im Hintergrund ausgeführt, ohne dass Sie durch die Setupbildschirme navigieren und Ihre Auswahl angeben müssen. Stattdessen werden allen Konfigurationsparametern Werte zugewiesen, die Sie in einer Antwortdatei festlegen. Um Installationen im unbeaufsichtigten Modus für unterschiedliche Konfigurationen durchzuführen, können Sie mehrere Antwortdateien erstellen.

Hinweise und Einschränkungen

Vor der dem Durchführen der unbeaufsichtigten Installation sollten Sie die folgenden Punkte berücksichtigen:

- Beim Durchführen der Installation im unbeaufsichtigten Modus werden keine Meldungen angezeigt. Stattdessen können Sie in den Protokolldateien Installationsinformationen anzeigen, einschließlich der Information, ob die Installation erfolgreich war. Die Installationsprotokolldateien befindet sich unter:
  - **%tmp%\HPOvInstaller\HPSiteScope_11.30** auf Windows-Plattformen
  - **/tmp/HPOvInstaller/HPSiteScope_11.30** auf Linux-Plattformen
- Der Name des SiteScope-Installationspfads (`prodInstallDir=<Installationspfad>`) darf keine Leerzeichen oder nichtlateinischen Buchstaben enthalten und muss mit einem Ordner namens **SiteScope** enden (beachten Sie beim Ordnernamen die Groß- oder Kleinschreibung).

- Die Option zum Installieren von HP Operations Agent direkt aus SiteScope wurde entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

Durchführen einer unbeaufsichtigten Installation

Sie führen eine unbeaufsichtigte Installation mithilfe der Datei **ovinstallparams.ini** durch. Da diese Datei ein besonderes Format aufweist, sollten Sie die Datei für die unbeaufsichtigte Installation mithilfe der Beispieldatei **ovinstallparams.ini** erstellen.

Hinweis: Die Beispieldatei **ovinstallparams.ini** steht nur zur Verfügung, wenn SiteScope aus dem Verzeichnis **<SiteScope-Installationsverzeichnis>\examples\silent_installation** installiert wird.

So führen Sie eine unbeaufsichtigte Installation für SiteScope 11.30 durch:

1. Navigieren Sie zur Datei **ovinstallparams.ini** im Ordner **<SiteScope-Installationsverzeichnis>\examples\silent_installation**.
2. Erstellen Sie eine Kopie der Datei und bearbeiten Sie sie anschließend entsprechend Ihren Installationsanforderungen.
3. Kopieren Sie die Datei in den Setupordner, in dem sich die SiteScope-Installationsdatei (**HPSiteScope_11.30_setup.exe** oder **HPSiteScope_11.30_setup.bin**) befindet.
4. Führen Sie das Installationsprogramm an der Befehlszeile mit dem Kennzeichen **-i silent** aus. Geben Sie unter Windows den Wartemodus an. Beispiel:

   `start /wait HPSiteScope_11.30_setup.exe -i silent` (Windows)

   `HPSiteScope_11.30_setup.bin -i silent` (Linux)

So installieren Sie SiteScope im unbeaufsichtigten Modus:

Führen Sie unter Linux die folgende Befehlszeile aus:

```
/opt/HP/SiteScope/installation/bin/uninstall.sh -i silent
```

Führen Sie unter Windows Folgendes aus:

```
%SITESCOPE_HOME%\installation\bin\uninstall.bat -i silent
```

Kapitel 15: Verwenden des SiteScope-Konfigurationswerkzeugs

Dieses Kapitel umfasst die folgenden Themen:

Ausführen des Konfigurationswerkzeugs auf Windows-Plattformen

Das Konfigurationswerkzeug ist ein praktisches Dienstprogramm für das Verschieben von Konfigurationsdaten von einer SiteScope-Installation in eine andere. Sie können SiteScope-Daten wie Vorlagen, Protokolle, Monitorkonfigurationsdateien, Skripts, Serverzertifikate usw. aus Ihrer aktuellen SiteScope-Installation exportieren und später in SiteScope importieren. Mit dem Assistenten können Sie außerdem die Leistung von SiteScope optimieren, indem Sie die Größe der Windows-Registrierungsschlüssel anpassen, die Ports ändern, die SiteScope zugewiesenen sind, und die Installation des HP Operations Agent abschließen.

Wenn Sie während des Installationsvorgangs SiteScope-Daten exportiert haben, können Sie die Daten mithilfe des Konfigurationswerkzeugs importieren. Alternativ können Sie Daten mithilfe des Konfigurationswerkzeugs unabhängig aus Ihrer aktuellen SiteScope-Installation exportieren. Wenn Sie in vorherigen SiteScope-Versionen Konfigurationsdateien erstellt oder geändert haben, müssen Sie diese u. U. in das aktuelle SiteScope-Verzeichnis importieren.

Hinweis:

- Sie können das Konfigurationswerkzeug auf Windows-Plattformen auch im Konsolenmodus ausführen. Weitere Informationen finden Sie unter "Ausführen des Konfigurationswerkzeugs im Konsolenmodus" auf Seite 165.
- Die Option zum Installieren und Deinstallieren von HP Operations Agent direkt aus SiteScope

wurde aus dem Konfigurationswerkzeug entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

- Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten exportieren oder importieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen" auf Seite 242.
- Beim Importieren von Konfigurationen in dieselbe SiteScope-Version müssen Sie alle Vorlagenbeispielbehälter umbenennen oder löschen, damit die neuen Vorlagenbeispiele importiert werden können.
- Wenn Sie Konfigurationsdaten von einer SiteScope-Installation auf eine andere verschieben, müssen Sie darauf achten, dass sich der SiteScope-Server, von dem Sie die Konfigurationsdaten übernehmen, in derselben Zeitzone befindet wie der SiteScope-Server, auf den die Daten importiert werden sollen.
- Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.
- Dateien aus den folgenden Ordnern können nicht überschrieben werden, wenn Konfigurationsdaten importiert werden: **templates.os**, **templates.post**, **templates.health**, **templates.applications** und **conf\ems**.
- Das Konfigurationswerkzeug unterstützt beim Exportieren von Daten das Einbeziehen von Serverzertifikaten und Skripts. Informationen über die Einbeziehung von Serverzertifikaten und Skripts beim Exportieren von Daten aus früheren SiteScope-Versionen finden Sie unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.

So führen Sie das SiteScope-Konfigurationswerkzeug aus:

1. Wählen Sie auf dem SiteScope-Server **Start > Alle Programme > HP SiteScope > Konfigurationswerkzeug** aus. Der SiteScope-Konfigurationsassistent wird angezeigt.

2. Wählen Sie die Aktionen aus, die Sie durchführen möchten, und klicken Sie dann auf **Weiter**.

- **Anpassen.** Ermöglicht das Optimieren der SiteScope-Leistung durch Erhöhen der JVM-Heap-Größe, der Desktop-Heap-Größe und der Anzahl der Dateihandles in den Windows-Registrierungsschlüsseln. Details finden Sie unter Schritt 3.

  Hinweis: Wenn Sie SiteScope durch Ausführen der Datei **go.bat** im Verzeichnis **<SiteScope-Installation>\bin** starten, öffnen Sie **go.bat** und erhöhen Sie den Wert für den Parameter **–Xmx1024m** nach Bedarf, jedoch höchstens auf **–Xmx8192m** (für 8 GB).

- **Ports ändern.** Ermöglicht das Ändern aller Ports, die vom SiteScope-Server verwendet werden. Details finden Sie unter Schritt 4.

- **Konfiguration importieren.** Ermöglicht das Importieren von Konfigurationsdaten aus einer exportierten Konfigurationsdatendatei (.zip) oder aus einer bestehenden SiteScope-Installation. Details finden Sie unter Schritt 5.

- **Konfiguration exportieren.** Ermöglicht das Exportieren von SiteScope-Daten wie Vorlagen, Protokolle, Monitorkonfigurationsdateien aus Ihrer aktuellen SiteScope-Installation und den späteren Import in SiteScope. Details finden Sie unter Schritt 6.

- **Separat installierten HP Operations Agent konfigurieren.** Erforderlich, um die Installation des HP Operations Agent abzuschließen. Mithilfe des Agenten kann SiteScope oder SiteScope-Failover Ereignisse versenden und als Datenspeicher für Metriken fungieren, wenn SiteScope mit einem HP Operations Manager- oder BSM Gateway-Server integriert wird. Details finden Sie unter Schritt 7.

> **Hinweis:** Diese Option ist deaktiviert, wenn HP Operations Agent 11.14 nicht auf dem SiteScope-Server installiert wurde. Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

3. Wenn Sie die Option **Anpassen** ausgewählt haben, wird der Bildschirm **Anpassen** mit den Parametern aus der Windows-Registrierung geöffnet.

Sie können die Leistung von SiteScope optimieren, indem Sie Änderungen an den folgenden Windows-Registrierungsschlüsseln vornehmen:

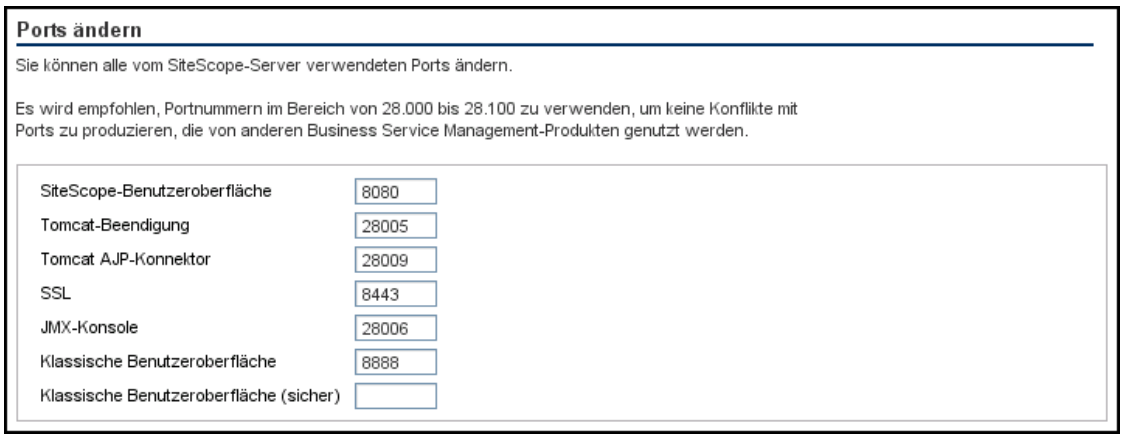
- **JVM-Heap-Größe.** Der Wert wurde von 512 MB auf 4096 MB geändert. Weitere Informationen zur JVM-Heap-Größe finden Sie unter http://java.sun.com/j2se/1.5.0/docs/guide/vm/gc-ergonomics.html.
- **Desktop-Heap-Größe.** Der Wert wurde von 512 KB auf 8.192 KB geändert. Weitere Informationen zur Desktop-Heap-Größe finden Sie unter http://support.microsoft.com/kb/126962.

  > **Hinweis:** Die Dimensionierung kann nur geändert werden, wenn der physische Speicher des SiteScope-Servers größer ist als die maximale JVM-Heap-Größe (Xmx), die vom Konfigurationswerkzeug konfiguriert wurde (4 GB bei einer 64-Bit-Installation).

  Klicken Sie auf **Weiter**, um die Anpassung abzuschließen.

- **Dateihandles.**Dieser Wert wird von 10.000 auf 18.000 Dateihandles erhöht. Weitere Informationen zum Ändern der Dateihandle-Anzahl finden Sie unter http://support.microsoft.com/kb/326591.

4. Wenn Sie die Option **Ports ändern** auswählen, wird die Seite **Ports ändern** angezeigt.



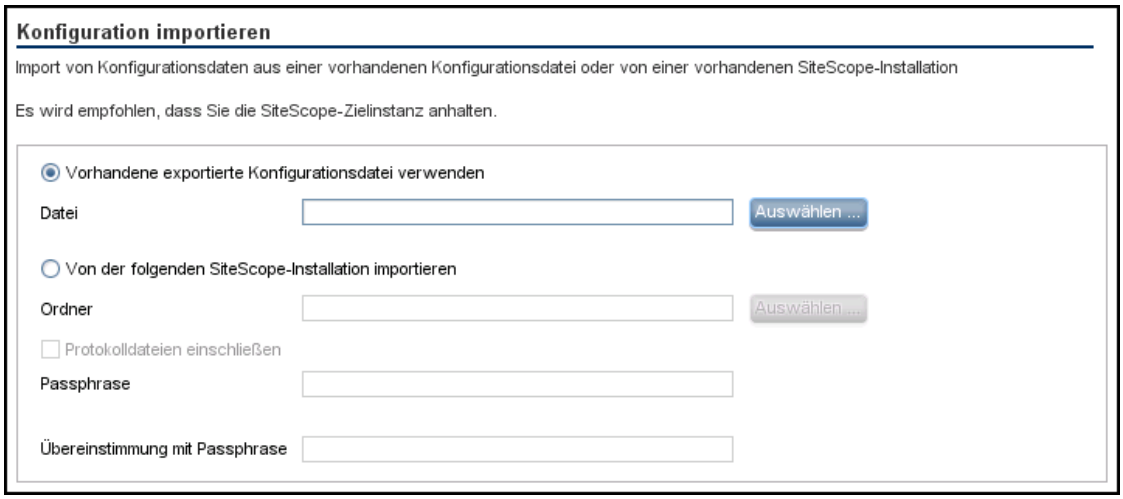
Ändern Sie die Ports, die von dem SiteScope-Server verwendet werden, wie gewünscht. Für die Portnummern muss ein numerischer Wert im Bereich 1-65534 eingegeben werden. Ein Port ist für alle Komponenten obligatorisch, mit Ausnahme der klassischen Benutzeroberfläche.

Hinweis: Es wird empfohlen, Ports aus dem Bereich 28000-28100 zu verwenden, damit keine Konflikte mit Ports auftreten, die von anderen Business Service Management-Instanzen verwendet werden.

Klicken Sie auf **Weiter**, um die Portänderung abzuschließen.

Hinweis: Nachdem Sie die Portänderung abgeschlossen haben, wird der Port in dem Link **Start > Alle Programme > HP SiteScope > HP SiteScope öffnen** aktualisiert.

5. Wenn Sie die Option **Konfiguration importieren** ausgewählt haben, wird die Seite für den Import der Konfiguration angezeigt.

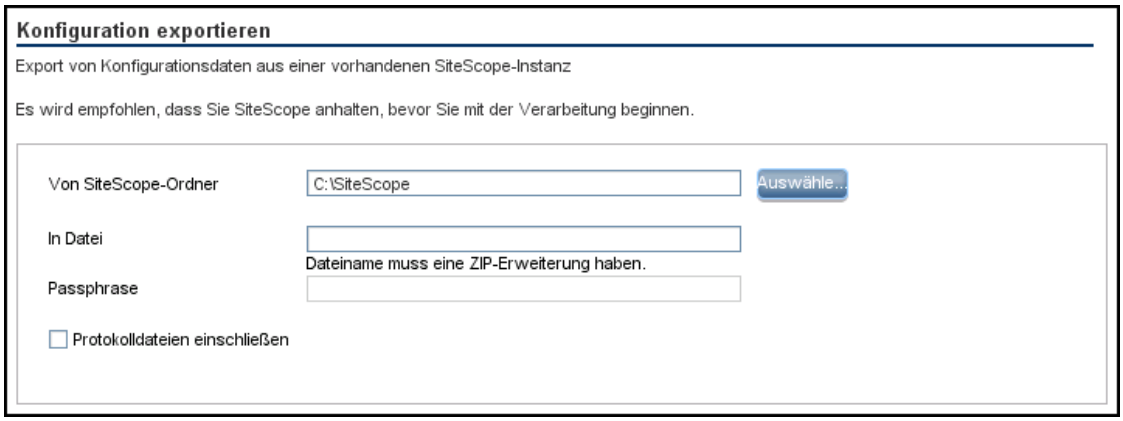


Hinweis: Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten importieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen" auf Seite 242.

- Wenn Sie **Vorhandene exportierte Konfigurationsdatei verwenden** auswählen, geben Sie den Namen der zu importierenden Benutzerdatendatei ein.
- Wenn Sie **Von der folgenden SiteScope-Installation importieren** auswählen, geben Sie das SiteScope-Installationsverzeichnis an, aus dem die Benutzerdatendatei importiert werden soll. Wenn Sie auch Protokolldateien importieren möchten, wählen Sie die Option **Protokolldateien einschließen** aus.
- Wenn SiteScope für das Ausführen der Datenverschlüsselung der Schlüsselverwaltung konfiguriert wurde, geben Sie die Passphrase für den KeyStore des SiteScope-Servers im Feld **Passphrase** ein. Bestätigen Sie die Passphrase, indem Sie dieselbe Passphrase in das Feld **Übereinstimmung mit Passphrase** eingeben. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208. Diese Felder sind deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

Klicken Sie auf **Weiter**, um den Import abzuschließen.

6. Wenn Sie die Option **Konfiguration exportieren** ausgewählt haben, wird die Seite für den Export der Konfiguration angezeigt.



- Akzeptieren Sie in **Von SiteScope-Ordner** das im Textfeld angegebene Standardverzeichnis oder geben Sie den vollständigen Pfad des SiteScope-Installationsverzeichnisses ein. Wenn Sie beispielsweise den aufgeführten Verzeichnispfad nicht akzeptieren möchten und der Installationsverzeichnispfad `D:\SiteScope11_0\SiteScope` lautet, geben Sie `D:\SiteScope11_0\SiteScope` ein.

- Geben Sie unter **In Datei** das Verzeichnis, in das die Benutzerdatendatei exportiert werden soll (das Verzeichnis muss vorhanden sein), und den Namen für die exportierte Benutzerdatendatei ein. Der Name muss auf **.zip** enden. Wenn Sie auch Protokolldateien exportieren wollen, wählen Sie die Option **Protokolldateien einschließen** aus.

- Wenn SiteScope für das Ausführen der mit einer schlüsselverwalteten Verschlüsselung konfiguriert wurde, geben Sie die Passphrase für den KeyStore des SiteScope-Servers im Feld **Passphrase** ein. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208. Dieses Feld ist deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

Hinweis:

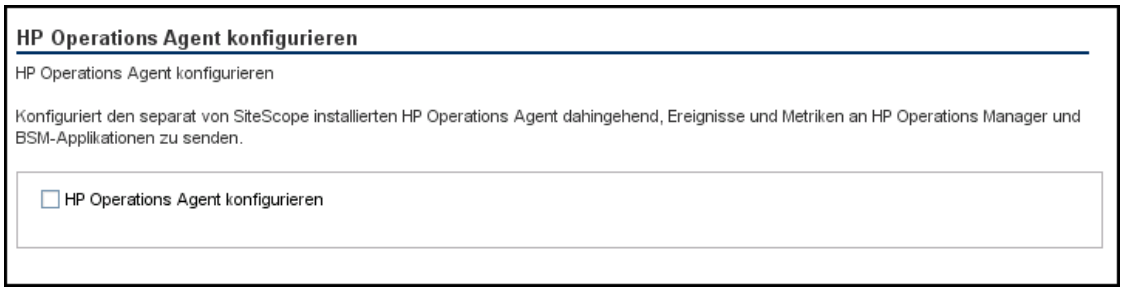
- Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten exportieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen" auf Seite 242.

- Sie sollten eine Sicherungskopie des Verzeichnisses erstellen und nach einer Aktualisierung

in das SiteScope 11.30-Verzeichnis kopieren, sodass Ihnen alte Reports angezeigt werden können, da das Verzeichnis **\htdocs** beim Exportieren von SiteScope-Daten nicht kopiert wird.

Klicken Sie auf **Weiter**, um den Export abzuschließen.

7. Wenn Sie die Option **Separat installierten HP Operations Agent konfigurieren** ausgewählt haben, wird die Seite **HP Operations Agent konfigurieren** angezeigt.



Wählen Sie **HP Operations Agent konfigurieren** aus. Dies ist erforderlich, um die Installation des HP Operations Agent abzuschließen. Mithilfe des Agenten kann SiteScope Ereignisse versenden und als Datenspeicher für Metriken fungieren, wenn SiteScope mit einem HP Operations Manager- oder BSM-Gateway-Server integriert wird.

Details zum Senden von Ereignissen und zum Melden von Metrikdaten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

Klicken Sie auf **Weiter**, um die Installation abzuschließen.

8. Die Übersichtsseite wird mit dem Konfigurationsstatus angezeigt.

Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Nach einer Aktualisierung können Sie SiteScope mithilfe der Datei **go.bat** aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\bin** ausführen. Dadurch wird verhindert, dass SiteScope automatisch neu gestartet wird, wenn es länger als 15 Minuten dauert, bis die Monitore gestartet werden.

Ausführen des Konfigurationswerkzeugs auf Linux-Plattformen

Das Konfigurationswerkzeug ist ein praktisches Dienstprogramm für das Verschieben von Konfigurationsdaten von einer SiteScope-Installation in eine andere. Sie können SiteScope-Daten wie Vorlagen, Protokolle, Monitorkonfigurationsdateien, Skripts, Serverzertifikate usw. aus Ihrer aktuellen SiteScope-Installation exportieren und später in SiteScope importieren. Sie können den Assistenten auch verwenden, um die von dem SiteScope-Server verwendeten Ports zu ändern und die Installation des HP Operations Agent abzuschließen.

Wenn Sie während des Installationsvorgangs SiteScope-Daten exportiert haben, können Sie die Daten mithilfe des Konfigurationswerkzeugs importieren. Alternativ können Sie Daten mithilfe des Konfigurationswerkzeugs unabhängig aus Ihrer aktuellen SiteScope-Installation exportieren. Wenn Sie in vorherigen SiteScope-Versionen Konfigurationsdateien erstellt oder geändert haben, müssen Sie diese u. U. in das aktuelle SiteScope-Verzeichnis importieren.

Hinweis:

- Sie können das Konfigurationswerkzeug auf Linux-Plattformen auch im Konsolenmodus ausführen. Weitere Informationen finden Sie unter "Ausführen des Konfigurationswerkzeugs im Konsolenmodus" auf Seite 165.
- Die Option zum Installieren und Deinstallieren von HP Operations Agent direkt aus SiteScope wurde aus dem Konfigurationswerkzeug entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.
- Wenn Sie Konfigurationsdaten von einer SiteScope-Installation auf eine andere verschieben, müssen Sie darauf achten, dass sich der SiteScope-Server, von dem Sie die Konfigurationsdaten übernehmen, in derselben Zeitzone befindet wie der SiteScope-Server, auf den die Daten importiert werden sollen.
- Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann

zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.

- Dateien aus den folgenden Ordnern können nicht überschrieben werden, wenn Konfigurationsdaten importiert werden: **templates.os**, **templates.post**, **templates.health**, **templates.applications** und **conf\ems**.
- Das SiteScope-Konfigurationswerkzeug unterstützt beim Exportieren von Daten das Einbeziehen von Serverzertifikaten und Skripts. Informationen über die Einbeziehung von Serverzertifikaten und Skripts beim Exportieren von Daten aus früheren SiteScope-Versionen finden Sie unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.
- Wenn Sie SiteScope in einer Umgebung mit hoher Auslastung verwenden, die mehr als 4 GB Speicher benötigt, sollten Sie die JVM-Heap-Größe auf dem Server manuell erhöhen.
  a. Öffnen Sie die Datei **SiteScope/bin/start-service**, um diese zu bearbeiten.
  b. Geben Sie in der letzten Zeile für den Parameter **-Xmx4096m** einen höheren Wert ein als erforderlich, bis maximal **-Xmx8192m** (für 8 GB).

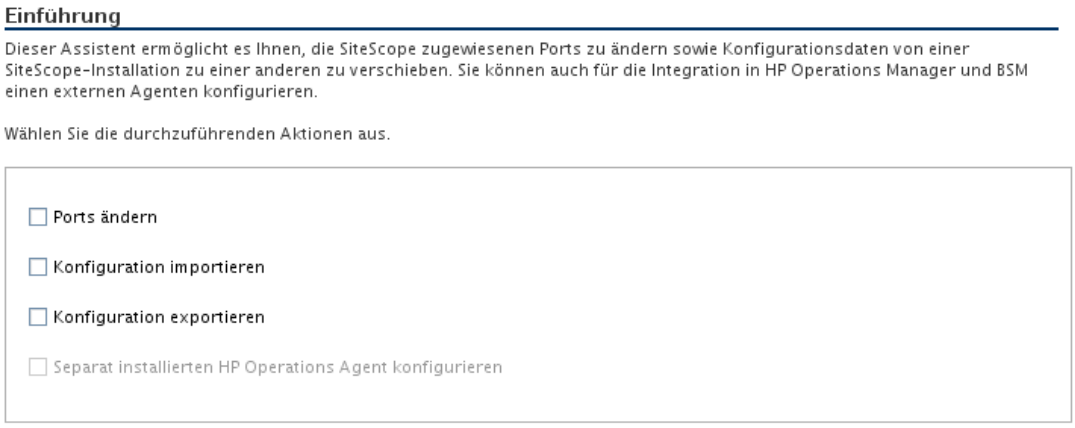
So führen Sie das SiteScope-Konfigurationswerkzeug aus:

1. Führen Sie auf dem SiteScope-Server einen der folgenden Schritte aus:
   a. Führen Sie im Grafikmodus `<SiteScope-Installationsverzeichnis>/bin/config_tool.sh` aus.
   b. Führen Sie im Konsolenmodus `<SiteScope-Installationsverzeichnis>/bin/config_tool.sh -i console` aus.

   Der SiteScope-Konfigurationsassistent wird angezeigt.

   Klicken Sie auf **Weiter**.

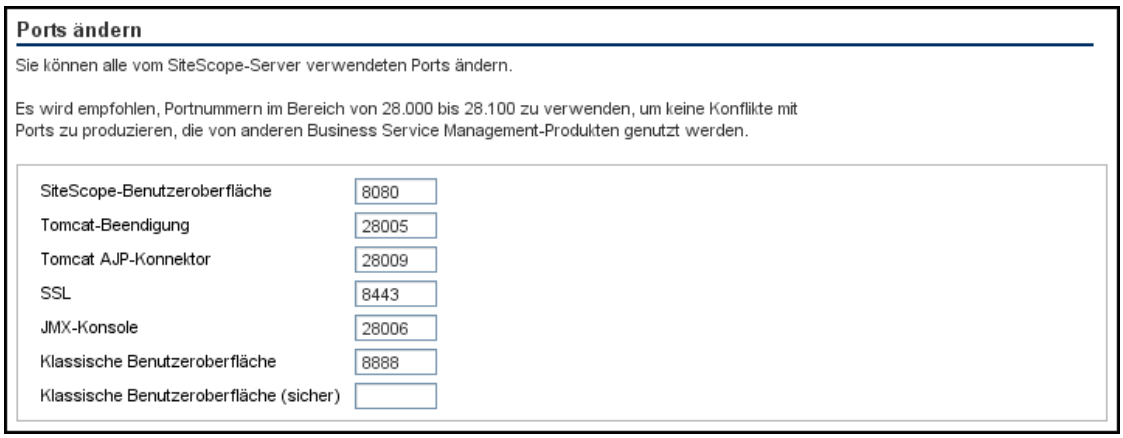
2. Wählen Sie die Aktionen aus, die Sie auf der Seite **Einführung** durchführen möchten, und klicken Sie dann auf **Weiter**.



- **Ports ändern.** Ermöglicht das Ändern aller Ports, die von dem SiteScope-Server verwendet werden. Details finden Sie unter Schritt 3.
- **Konfiguration importieren.** Ermöglicht das Importieren von Konfigurationsdaten aus einer exportierten Konfigurationsdatendatei (.zip) oder aus einer bestehenden SiteScope-Installation. Details finden Sie unter Schritt 5.
- **Konfiguration exportieren.** Ermöglicht das Exportieren von SiteScope-Daten wie Vorlagen, Protokolle, Monitorkonfigurationsdateien aus Ihrer aktuellen SiteScope-Installation und den späteren Import in SiteScope. Details finden Sie unter Schritt 4.
- **Separat installierten HP Operations Agent konfigurieren.** Erforderlich, um die Installation des HP Operations Agent abzuschließen. Mithilfe des Agenten kann SiteScope Ereignisse versenden und als Datenspeicher für Metriken fungieren, wenn SiteScope mit einem HP Operations Manager- oder BSM-Gateway-Server integriert wird. Details finden Sie unter Schritt 6.

  Hinweis: Diese Option ist deaktiviert, wenn HP Operations Agent 11.14 nicht auf dem SiteScope-Server installiert wurde. Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

3. Wenn Sie die Option **Ports ändern** auswählen, wird die Seite **Ports ändern** angezeigt.

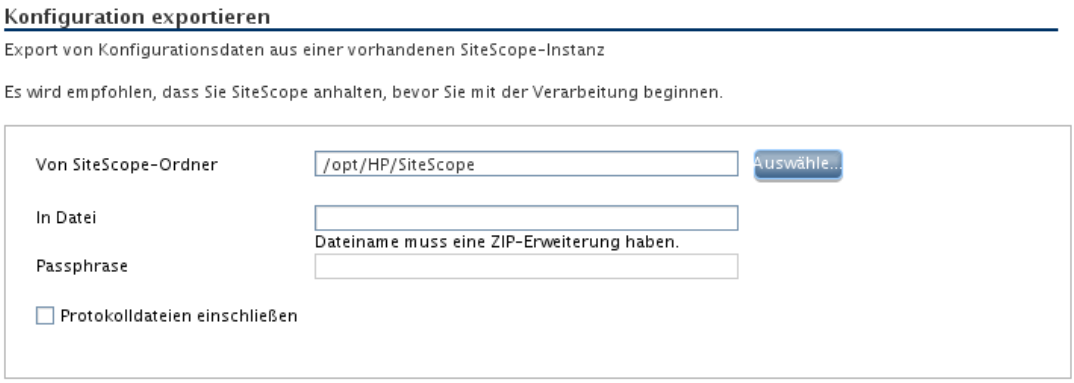


Ändern Sie die Ports, die von dem SiteScope-Server verwendet werden, wie gewünscht. Für die Portnummern muss ein numerischer Wert im Bereich 1-65534 eingegeben werden. Ein Port ist für alle Komponenten obligatorisch, mit Ausnahme der klassischen Benutzeroberfläche.

> **Hinweis:** Es wird empfohlen, Ports aus dem Bereich 28000-28100 zu verwenden, damit keine Konflikte mit Ports auftreten, die von anderen Business Service Management-Instanzen verwendet werden.

Klicken Sie auf **Weiter**, um die Portänderung abzuschließen.

4. Wenn Sie die Option **Konfiguration exportieren** ausgewählt haben, wird die Seite für den Export der Konfiguration angezeigt.

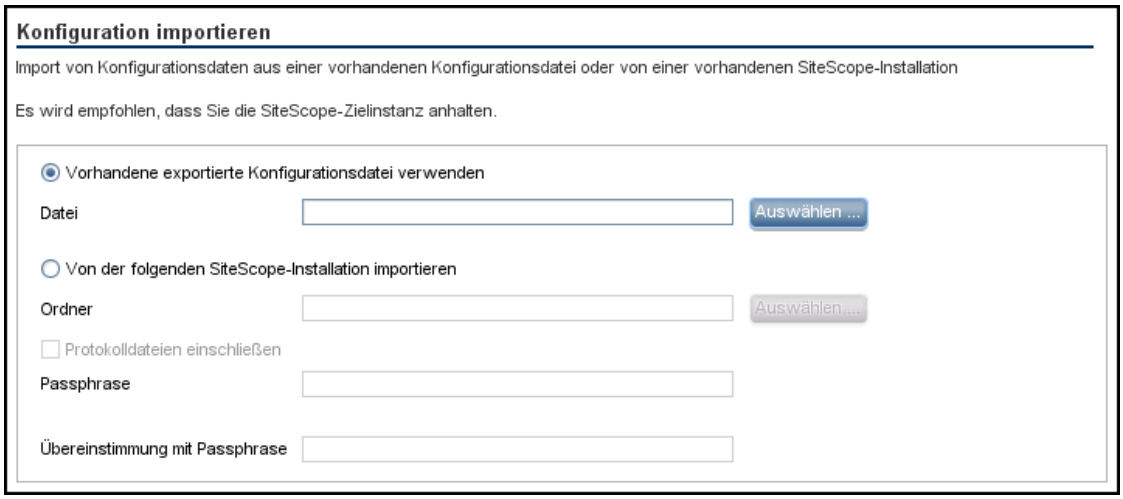


Hinweis: Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten exportieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen" auf Seite 243.

- Akzeptieren Sie in **Von SiteScope-Ordner** das im Textfeld angegebene Standardverzeichnis oder geben Sie den vollständigen Pfad des SiteScope-Installationsverzeichnisses ein. Wenn Sie beispielsweise den aufgeführten Verzeichnispfad nicht akzeptieren möchten und der Installationsverzeichnispfad `/opt/9_0/SiteScope` lautet, geben Sie `/opt/9_0/SiteScope` ein.
- Geben Sie unter **In Datei** das Verzeichnis, in das die Benutzerdatendatei exportiert werden soll (das Verzeichnis muss vorhanden sein), und den Namen für die exportierte Benutzerdatendatei ein. Der Name muss auf **.zip** enden.
- Wenn SiteScope für das Ausführen der Datenverschlüsselung der Schlüsselverwaltung konfiguriert wurde, geben Sie die Passphrase für den KeyStore des SiteScope-Servers im Feld **Passphrase** ein. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208. Dieses Feld ist deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.
- Wenn Sie auch Protokolldateien exportieren wollen, wählen Sie die Option **Protokolldateien einschließen** aus.

Klicken Sie auf **Weiter**, um den Export abzuschließen.

5. Wenn Sie die Option **Konfiguration importieren** ausgewählt haben, wird die Seite für den Import der Konfiguration angezeigt.



Hinweis: Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten importieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen" auf Seite 243.

- Wenn Sie **Vorhandene exportierte Konfigurationsdatei verwenden** auswählen, geben Sie den Namen der zu importierenden Benutzerdatendatei ein.
- Wenn Sie **Von der folgenden SiteScope-Installation importieren** auswählen, geben Sie das SiteScope-Installationsverzeichnis an, in das Sie die Benutzerdatendatei importieren möchten.
- Wenn Sie auch Protokolldateien importieren möchten, wählen Sie die Option **Protokolldateien einschließen** aus.
- Wenn SiteScope für das Ausführen der Datenverschlüsselung der Schlüsselverwaltung konfiguriert wurde, geben Sie die Passphrase für den KeyStore des SiteScope-Servers im Feld **Passphrase** ein. Bestätigen Sie die Passphrase, indem Sie dieselbe Passphrase in das Feld **Übereinstimmung mit Passphrase** eingeben. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208. Diese Felder sind deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

Klicken Sie auf **Weiter**, um den Import abzuschließen.

6. Wenn Sie die Option **Separat installierten HP Operations Agent konfigurieren** ausgewählt haben, wird die Seite **HP Operations Agent konfigurieren** angezeigt.

   Wählen Sie **HP Operations Agent konfigurieren** aus. Dies ist erforderlich, um die Installation des HP Operations Agent abzuschließen. Mithilfe des Agenten kann SiteScope Ereignisse versenden und als Datenspeicher für Metriken fungieren, wenn SiteScope mit einem HP Operations Manager- oder BSM-Gateway-Server integriert wird.

   Details zum Senden von Ereignissen und zum Melden von Metrikdaten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

   Klicken Sie auf **Weiter**, um den Konfigurationsvorgang abzuschließen.

7. Die Seite **Übersicht** wird angezeigt.

Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Ausführen des Konfigurationswerkzeugs im Konsolenmodus

Sie können das Konfigurationswerkzeug über eine Befehlszeile oder den Konsolenmodus ausführen. Verwenden Sie diese Option, wenn Sie SiteScope auf einem Remoteserver konfigurieren oder andere Gründe vorliegen, die gegen die Verwendung der Benutzeroberfläche sprechen.

Hinweis:

- Die Option zum Installieren und Deinstallieren von HP Operations Agent direkt aus SiteScope wurde aus dem Konfigurationswerkzeug entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.
- Dateien aus den folgenden Ordnern können nicht überschrieben werden, wenn Konfigurationsdaten importiert werden: **templates.os**, **templates.post**, **templates.health**, **templates.applications** und **conf\ems**.
- Wenn Sie SiteScope in einer Umgebung mit hoher Auslastung verwenden, die mehr als 4 GB Speicher benötigt, sollten Sie die JVM-Heap-Größe auf dem Server manuell erhöhen.

a. Öffnen Sie die Datei **SiteScope/bin/start-service**, um diese zu bearbeiten.

b. Geben Sie in der letzten Zeile für den Parameter **-Xmx4096m** einen höheren Wert ein als erforderlich, bis maximal **-Xmx8192m** (für 8 GB).

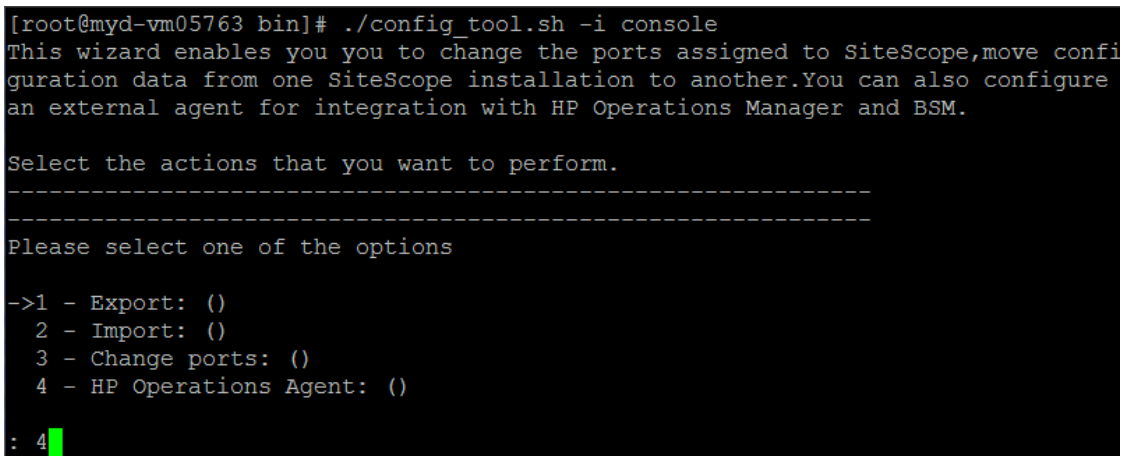
So führen Sie das Konfigurationswerkzeug im Konsolenmodus aus:

Hinweis: In der folgenden Vorgehensweise wird anhand von Screenshots gezeigt, wie Sie das Konfigurationswerkzeug in einer Linux-Umgebung ausführen.

1. Führen Sie den folgenden Befehl aus:

   `/bin/config_tool.sh -i console` unter Linux bzw. `<SiteScope-Stammverzeichnis>\bin\config_tool.bat -i console` unter Windows.

2. Der Auswahlbildschirm für die Konfiguration wird angezeigt.



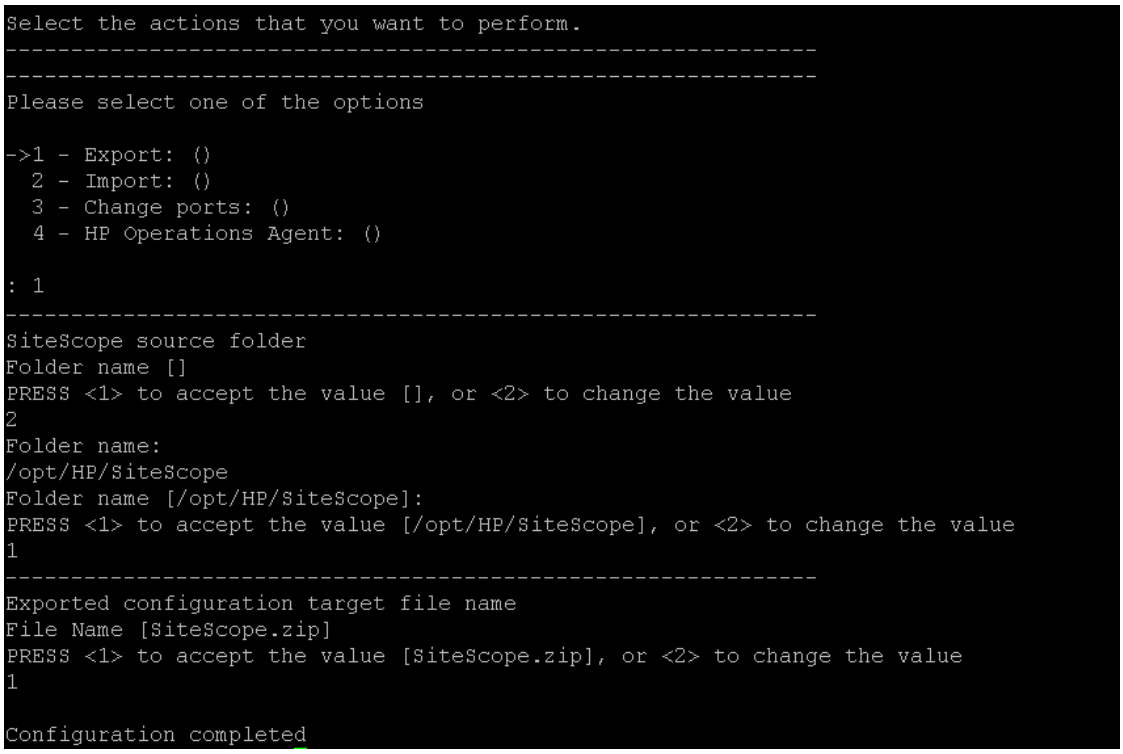
   Wählen Sie die Konfigurationsaktion aus, die Sie durchführen möchten.

   - Geben Sie die Zahl `1` ein, um SiteScope-Daten zu exportieren.
   - Geben Sie die Zahl `2` ein, um Konfigurationsdaten aus einer exportierten Konfigurationsdatendatei (.zip) oder einer bestehenden SiteScope-Installation zu importieren.
   - Geben Sie die Zahl `3` ein, um die vom SiteScope-Server verwendeten Ports zu ändern.
   - Geben Sie die Zahl `4` ein, um die Installation des HP Operations Agent abzuschließen (der Agent

ermöglicht es SiteScope, Metrik- und Ereignisdaten an HP Operations Manager und BSM-Anwendungen zu übermitteln).

Drücken Sie die EINGABETASTE, um fortzufahren.

3. Wenn Sie die Option **Export** ausgewählt haben, wird die Seite für den Export der Konfiguration angezeigt.



- Nehmen Sie für **SiteScope source folder** folgende Eingaben vor:
  - Geben Sie die Zahl 1 ein, um das in [ ] angegebene Standardverzeichnis zu akzeptieren.
  - Geben Sie die Zahl 2 ein, um den Wert zu ändern, und geben Sie den vollständigen Pfad des SiteScope-Installationsverzeichnisses ein. Wenn Sie beispielsweise den angezeigten Verzeichnispfad nicht akzeptieren möchten und der Installationsverzeichnispfad /opt/HP/SiteScope lautet, geben Sie /opt/HP/SiteScope ein.

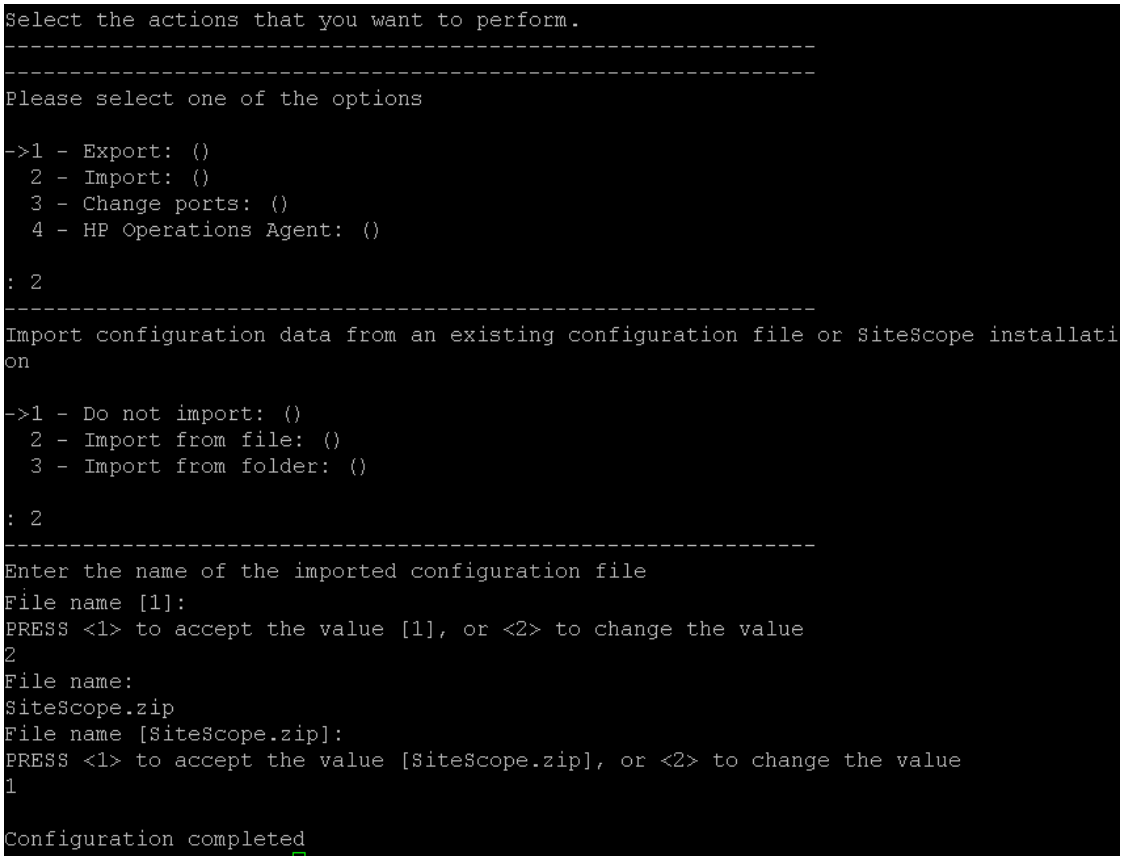
  Drücken Sie die EINGABETASTE, um mit der Installation fortzufahren.

- Nehmen Sie für **Exported configuration target file name** folgende Eingaben vor:

- Geben Sie die Zahl `1` ein, um die Daten in eine Datei namens **SiteScope.zip** zu exportieren.
- Geben Sie die Zahl `2` ein, um den Namen der exportierten Benutzerdatendatei zu ändern. Der Name muss auf **.zip** enden.

Drücken Sie die `EINGABETASTE`, um den Exportvorgang abzuschließen.

4. Wenn Sie die Option **Import** ausgewählt haben, wird die Seite für den Import der Konfiguration angezeigt.



Wählen Sie eine Option für die Konfigurationsdaten aus:

- Geben Sie die Zahl `1` ein, wenn Sie keine Konfigurationsdaten importieren möchten.
- Geben Sie die Zahl `2` ein, um Konfigurationsdaten aus einer Datei zu importieren. Nehmen Sie bei Auswahl dieser Option folgende Eingaben vor:

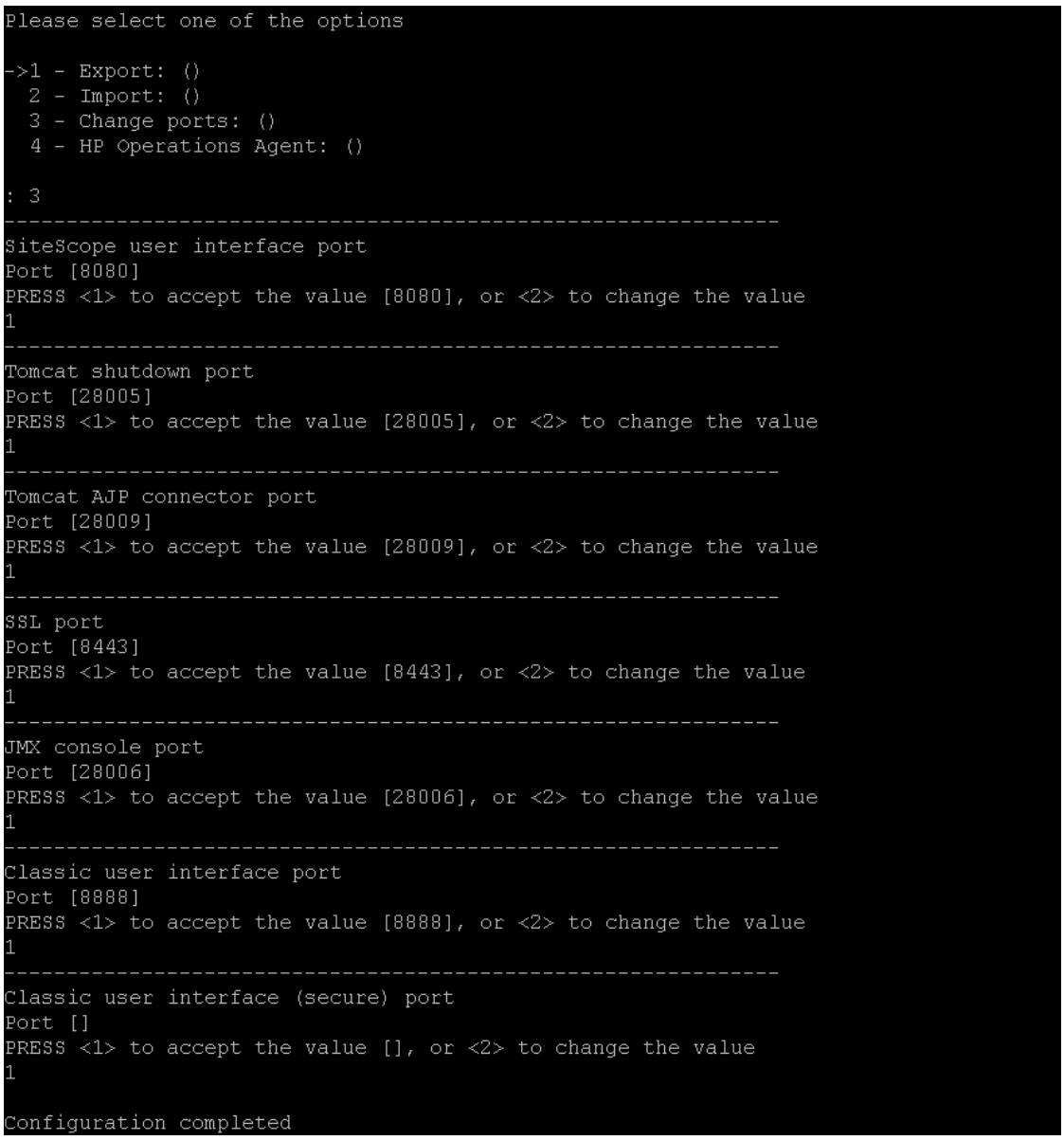
- Geben Sie die Zahl `1` ein, um den in [ ] angegebenen Standarddateinamen zu akzeptieren.
- Geben Sie die Zahl `2` ein, um den Wert zu ändern, und geben Sie den Namen der Datei ein, aus der die Konfigurationsdaten importiert werden sollen. Geben Sie die Zahl `1` ein, um den Namen zu übernehmen.

- Geben Sie die Zahl `3` ein, um Konfigurationsdaten aus einem SiteScope-Installationsverzeichnis zu importieren. Nehmen Sie bei Auswahl dieser Option folgende Eingaben vor:
  - Geben Sie die Zahl `1` ein, um das in [ ] angegebene Standardverzeichnis zu akzeptieren.
  - Geben Sie die Zahl `2` ein, um den Wert zu ändern, und geben Sie das SiteScope-Installationsverzeichnis ein, aus dem die Benutzerdatendatei importiert werden soll. Geben Sie die Zahl `1` ein, um den Namen zu akzeptieren.

  Drücken Sie die `EINGABETASTE`, um den Importvorgang abzuschließen.

  Hinweis: Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.

5. Wenn Sie die Option **Ports ändern** auswählen, wird die Seite zum Ändern der Ports angezeigt.



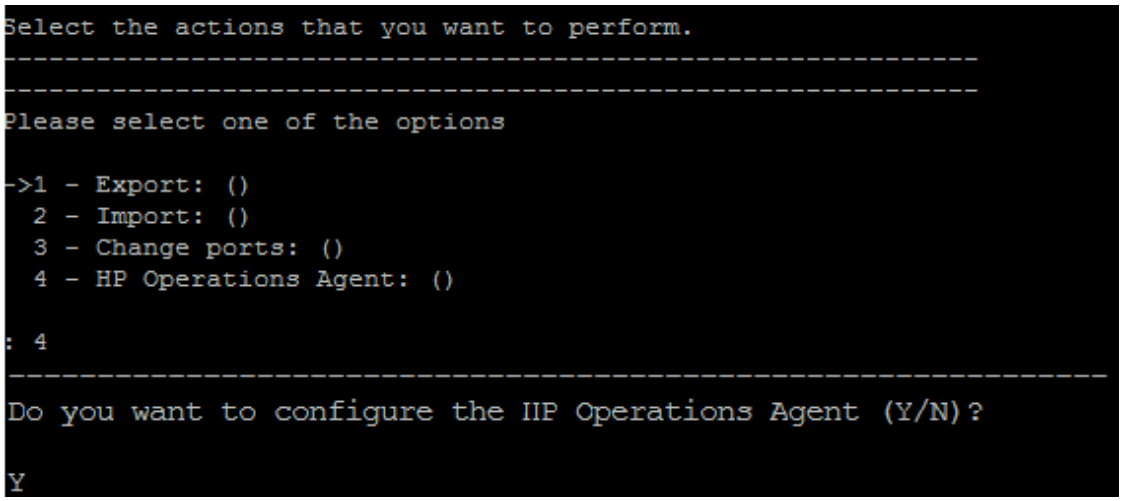
Ändern Sie die Ports, die von dem SiteScope-Server verwendet werden, wie gewünscht. Für die Portnummern muss ein numerischer Wert im Bereich 1-65534 eingegeben werden. Ein Port ist für alle Komponenten obligatorisch, mit Ausnahme der klassischen Benutzeroberfläche.

Hinweis: Es wird empfohlen, Ports aus dem Bereich 28000-28100 zu verwenden, damit keine

Konflikte mit Ports auftreten, die von anderen BSM-Instanzen verwendet werden.

Drücken Sie die EINGABETASTE, um die Portänderung abzuschließen.

6. Wenn Sie die Option **HP Operations Agent** ausgewählt haben, wird die Seite für den HP Operations Agent angezeigt.



Geben Sie Y ein, um die Installation des HP Operations Agent abzuschließen.

Nach dem die Installation des Agenten abgeschlossen ist, sollte der SiteScope-Server neu gestartet werden.

Details zum Melden von Metrikdaten mithilfe des HP Operations Agent finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

Hinweis: HP Operations Agent ist nicht erforderlich, wenn Metrikdaten mithilfe der Profildatenbank in BSM für Leistungsdiagramme grafisch aufbereitet werden. Die Profildatenbank in BSM ist die empfohlene Option, da sie eine wesentlich robustere und skalierbare Datenquelle ist und keine Konfiguration der HP Operations-Integration erforderlich ist.

Ausführen des Konfigurationswerkzeugs im unbeaufsichtigten Modus

Sie können das Konfigurationswerkzeug von SiteScope im unbeaufsichtigten Modus ausführen. Auf diese Weise haben Sie die Möglichkeit, eine Sicherungskopie der aktuellen SiteScope-Konfigurationsdaten zu erstellen, ohne dazu die Bildschirme des Konfigurationswerkzeugs nacheinander aufzurufen und dort Ihre Eingaben zu machen. Stattdessen werden allen Konfigurationsparametern Werte zugewiesen, die Sie in einer Antwortdatei festlegen.

Überlegungen vor dem Ausführen einer unbeaufsichtigten Konfiguration

Vor der dem Durchführen der unbeaufsichtigten Konfiguration sollten Sie die folgenden Punkte berücksichtigen:

- Beim Durchführen einer Konfiguration im unbeaufsichtigten Modus werden keine Meldungen angezeigt. Stattdessen können Sie in den Protokolldateien Konfigurationsinformationen anzeigen, einschließlich der Information, ob die Konfiguration erfolgreich war. Die Konfigurationsprotokolldateien befindet sich unter:
  - **%tmp%\HPSiteScope_config_tool.log** auf Windows-Plattformen
  - **/tmp/HPSiteScope_config_tool.log** auf Linux-Plattformen
- Wenn Sie Konfigurationsdaten von einer SiteScope-Installation auf eine andere verschieben, müssen Sie darauf achten, dass sich der SiteScope-Server, von dem Sie die Konfigurationsdaten übernehmen, in derselben Zeitzone befindet wie der SiteScope-Server, auf den die Daten importiert werden sollen.
- Wenn die importierte Konfiguration abgelaufene Zertifikate enthält, werden diese im standardmäßigen SiteScope-Keystore beim Konfigurationsimport zusammengeführt. Dies kann zu einem Fehlerstatus beim SSL-Zertifikat-Monitor führen. Um dies zu vermeiden, sollten Sie alle abgelaufenen Zertifikate löschen, bevor Sie Konfigurationsdaten exportieren.
- Beim Importieren von Konfigurationen in dieselbe SiteScope-Version müssen Sie alle Vorlagenbeispielbehälter umbenennen oder löschen, damit die neuen Vorlagenbeispiele importiert werden können.

- Sie müssen den SiteScope-Dienst anhalten, bevor Sie Daten exportieren oder importieren, und ihn anschließend erneut starten. Weitere Informationen finden Sie unter "Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen" auf Seite 242 und "Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen" auf Seite 243.

- Dateien aus den folgenden Ordnern können nicht überschrieben werden, wenn Konfigurationsdaten importiert werden: **templates.os**, **templates.post**, **templates.health**, **templates.applications** und **conf\ems**.

- Bei Auswahl der Option zum Exportieren der Konfigurationsdaten:

  - Sie sollten eine Sicherungskopie des Verzeichnisses erstellen und nach einer Aktualisierung in das SiteScope-Verzeichnis kopieren, sodass Ihnen alte Reports angezeigt werden können, da das Verzeichnis **\htdocs** beim Exportieren von SiteScope-Daten nicht kopiert wird.

  - Das Konfigurationswerkzeug unterstützt beim Exportieren von Daten das Einbeziehen von Serverzertifikaten und Skripts. Informationen über die Einbeziehung von Serverzertifikaten und Skripts beim Exportieren von Daten aus früheren SiteScope-Versionen finden Sie unter "Aktualisieren einer vorhandenen SiteScope-Installation" auf Seite 89.

- Bei Auswahl der Dimensionierungsoption (nur auf Windows-Plattformen):

  - Die Dimensionierung kann nur geändert werden, wenn der physische Speicher des SiteScope-Servers größer ist als die maximale JVM-Heap-Größe (Xmx), die vom Konfigurationswerkzeug konfiguriert wurde (4 GB).

  - Wenn Sie SiteScope durch Ausführen der Datei **go.bat** im Verzeichnis **<SiteScope-Installation>\bin** starten, öffnen Sie **go.bat** und erhöhen Sie den Wert für den Parameter **–Xmx4096m** nach Bedarf, jedoch höchstens auf **–Xmx8192m** (für 8 GB).

- Wenn Sie die Option zum Ändern der Ports ausgewählt haben, wird empfohlen, Ports aus dem Bereich 28000-28100 zu verwenden, damit keine Konflikte mit Ports auftreten, die von anderen Business Service Management-Produkten verwendet werden.

- Wenn Sie SiteScope in einer Umgebung mit hoher Auslastung verwenden, die mehr als 4 GB Speicher benötigt, sollten Sie die JVM-Heap-Größe auf dem Server manuell erhöhen.

  a. Öffnen Sie die Datei **SiteScope/bin/start-service**, um diese zu bearbeiten.

  b. Geben Sie in der letzten Zeile für den Parameter **-Xmx4096m** einen höheren Wert ein als erforderlich, bis maximal **-Xmx8192m** (für 8 GB).

- Die Option zum Installieren und Deinstallieren von HP Operations Agent direkt aus SiteScope wurde aus dem Konfigurationswerkzeug entfernt. Stattdessen müssen Sie den Agenten manuell installieren und konfigurieren. Der Agent ist für das Senden von Ereignissen und Speichern von Metrikdaten erforderlich, wenn SiteScope mit HPOM oder BSM integriert ist (außer bei der grafischen Darstellung von Metrikdaten in Leistungsdiagrammen mit der Profildatenbank in BSM). Details zum Installieren und Konfigurieren des Agenten finden Sie im Handbuch zur Integration von SiteScope mit HP Operations Manager-Produkten in der SiteScope-Hilfe oder auf der Website für HP Software-Integrationen.

Ausführen einer unbeaufsichtigten Konfiguration

Sie führen eine unbeaufsichtigte Konfiguration mithilfe der Datei **configtoolparams.txt** aus. Da diese Datei ein besonderes Format aufweist, sollten Sie die Datei für die unbeaufsichtigte Konfiguration auf Grundlage der Beispieldatei im Verzeichnis **<SiteScope-Installationsverzeichnis>\examples\silent_config_tool** erstellen.

So führen Sie eine unbeaufsichtigte Installation für SiteScope aus:

1. Navigieren Sie zur Datei **configtoolparams.txt** im Ordner **<SiteScope-Installationsverzeichnis>\examples\silent_config_tool**.
2. Erstellen Sie eine Kopie der Datei und speichern Sie sie in einem Verzeichnis Ihrer Wahl.
3. Öffnen Sie die Datei, nehmen Sie die gewünschten Änderungen vor (befolgen Sie die Anweisungen aus der Beispielsdatei) und speichern Sie Datei dann.
4. Führen Sie das Konfiguration an der Befehlszeile mit den Kennzeichen **-i silent** und **-f <answers file>** aus.

   Beispiel:

   `config_tool -i silent -f c:\configtoolparams.txt` (Windows)

   oder

   `./config_tool.sh -i silent -f /opt/configtoolparams.txt` (Linux)

Kapitel 16: Deinstallieren von SiteScope

Dieses Kapitel umfasst die folgenden Themen:

Deinstallieren von SiteScope auf einer Windows-Plattform

Sie können SiteScope 11.30 und alle Minor-Minor-Versionen (Patches), die darüber hinaus installiert wurden, oder eine eigenständige SiteScope Minor-Minor-Version nur vom Server deinstallieren. Wird SiteScope auf einer Windows-Plattform ausgeführt, beinhaltet die SiteScope-Installation ein Programm für die Deinstallation der SiteScope-Software vom Computer.

Deinstallieren von SiteScope und allen Minor-Minor-Versionen, die darüber hinaus installiert wurden

1. Halten Sie den SiteScope-Dienst an.

    a. Wählen Sie **Start > Alle Programme > Verwaltung > Dienste** aus. Das Dialogfeld **Dienste** wird geöffnet.

    b. Wählen Sie aus der Liste der Dienste den Eintrag **SiteScope** aus. Wird SiteScope ausgeführt, klicken Sie mit der rechten Maustaste, um das Menü **Aktion** anzuzeigen, und wählen Sie **Beenden** aus. Warten Sie, bis die Statusanzeige des Diensts anzeigt, dass dieser beendet wurde, und schließen Sie das Fenster **Dienste**.

2. Deinstallieren Sie SiteScope.

    a. Wählen Sie **Start > Alle Programme > HP SiteScope > HP SiteScope deinstallieren** aus.

    b. Wählen Sie im Bildschirm für die Auswahl des Gebietsschemas die gewünschte Sprache aus und klicken Sie auf **OK**.

    c. Wählen Sie im Bildschirm für die Anwendungswartung **Deinstallieren** aus und klicken Sie auf **Weiter**.

d. Klicken Sie im Bildschirm mit der Übersicht über die Deinstallation auf **Deinstallieren**.

Alle Softwarekomponenten und deren Deinstallationsverlauf werden auf der Seite während der Deinstallation angezeigt.

Nach Abschluss des Deinstallationsprozesses wird das Fenster **Deinstallation abgeschlossen** mit einer Zusammenfassung zum Deinstallationsprozess geöffnet.

e. Klicken Sie im Fenster **Deinstallation abgeschlossen** auf **Fertig**, um das Deinstallationsprogramm zu schließen.

Über den Link **Protokolldatei anzeigen** können Sie auf das Deinstallationsprotkoll zugreifen, das über einen Webbrowser geöffnet wird. Details zu den entfernten Paketen erhalten Sie, indem Sie zur Registerkarte **Details** wechseln.

3. Aufheben der Konfiguration und Deinstallieren des HP Operations Agent

Wenn der HP Operations Agent auf dem SiteScope-Server installiert wurde und entfernt werden soll, müssen Sie die Konfiguration aufheben und dann den Agenten deinstallieren.

a. Führen Sie den folgenden Befehl aus, um die Konfiguration von HP Operations Agent manuell aufzuheben:

i. `msiexec /x <SiteScope-Stammverzeichnis>\installation\components\oa_policy_signing_tool\win64\HPOprIAPA-09.00.111-Win5.2_64-release.msi /quiet`

ii. `<SiteScope-Stammverzeichnis>\installation\components\oa_template_management\all\install.bat -remove windows64`

b. Informationen zum Deinstallieren des Agenten, der auf dem SiteScope-Server installiert ist, finden Sie im Installationshandbuch zu HP Operations Agent 11.14 (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01001255).

4. Starten Sie den Computer nach Abschluss der Deinstallation neu, wenn Sie dazu aufgefordert werden.

Deinstallieren von SiteScope auf einer Linux-Plattform

Sie können SiteScope 11.30 und alle Minor-Minor-Versionen (Patches), die darüber hinaus installiert wurden, oder eine eigenständige SiteScope Minor-Minor-Version nur vom Server deinstallieren. Wird SiteScope auf einer Linux-Plattform ausgeführt, beinhaltet die SiteScope-Installation ein Skript für die Deinstallation der SiteScope-Software vom Computer. Wenn Sie das Skript nicht ausführen können, können Sie die SiteScope-Dateien und -Verzeichnisse manuell löschen.

Deinstallieren von SiteScope und allen Minor-Minor-Versionen, die darüber hinaus installiert wurden

1. Melden Sie sich bei dem Computer, auf dem SiteScope ausgeführt wird, mit dem Konto an, das über die Berechtigung zum Ausführen von Skripts im SiteScope-Verzeichnis verfügt. Normalerweise handelt es sich dabei um das Konto, unter dem SiteScope ausgeführt wird.

2. Beenden Sie SiteScope, indem Sie das Skript **stop shell** im Verzeichnis **<Installationspfad>/SiteScope** ausführen. Im Folgenden finden Sie eine Befehlszeilenbeispiel für die Ausführung des Skripts: **SiteScope/stop**.

   Es wird eine Meldung angezeigt, dass SiteScope beendet wurde.

3. Wenn Sie im X Windows-Modus arbeiten, führen Sie den folgenden Befehl aus: **/opt/HP/SiteScope/installation/bin/uninstall.sh**

4. Im Konsolenmodus sollte SiteScope 11.30 über folgenden Befehl deinstalliert werden: **/opt/HP/SiteScope/installation/bin/uninstall.sh –i console**.

5. Das HP Software-Installationsprogramm wird gestartet. Geben Sie das Gebietsschema an und drücken Sie dann die EINGABETASTE.

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Preparing CONSOLE Mode Installation...

===============================================================================
Choose Locale...
----------------

    1- Deutsch
  ->2- English
    3- Fran?ais

CHOOSE LOCALE BY NUMBER: 2
===============================================================================
HP Software Installer
---------------------


PRESS <ENTER> TO CONTINUE: 2
```

6. Geben Sie 1 ein und drücken Sie die Eingabetaste, um die Deinstallation von SiteScope zu bestätigen.

```
===============================================================================
Maintenance Selection
---------------------

Modify, repair or uninstall the application
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- Uninstall        Uninstall the application from your computer.

Please select one of the options...: 1
```

7. Es werden Meldungen für den Deinstallationsstatus für das Paket angezeigt und die Deinstallation wird abgeschlossen:

```
===============================================================================
Uninstallation Complete
-----------------------


The uninstallation has been successfully completed.
```

8. Aufheben der Konfiguration und Deinstallieren des HP Operations Agent

Wenn der HP Operations Agent auf dem SiteScope-Server installiert wurde und entfernt werden soll, müssen Sie die Konfiguration aufheben und dann den Agenten deinstallieren.

a. Führen Sie unter Linux folgende Befehle aus, um die Konfiguration von HP Operations Agent manuell aufzuheben:

   i. `rpm -e HPOprIAPA`

   ii. `<SiteScope-Stammverzeichnis>\installation\components\oa_template_management\all\install.sh -remove linux64`

b. Informationen zum Deinstallieren des Agenten, der auf dem SiteScope-Server installiert ist, finden Sie im Installationshandbuch zu HP Operations Agent 11.14 (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01001255).

Teil 4: Sicheres Ausführen von SiteScope

Kapitel 17: Optimieren der Sicherheit der SiteScope-Plattform

Dieses Kapitel umfasst die folgenden Themen:

Übersicht

Dieses Kapitel beschreibt mehrere Konfigurations- und Einrichtungsoptionen, anhand derer sich die Sicherheit der SiteScope-Plattform optimieren lässt.

Als Überwachungswerkzeug für die Systemverfügbarkeit hat SiteScope u.U. Zugriff auf Systeminformationen, mit denen die Systemsicherheit gefährdet werden könnte, falls keine Maßnahmen zu deren Sicherung ergriffen werden. Sie sollten die Konfigurations- und Einrichtungsoptionen in diesem Abschnitt zum Schutz der SiteScope-Plattform verwenden.

Achtung: Es gibt zwei aktive Webserver für zwei Versionen der SiteScope-Produktschnittstelle: Der SiteScope-Webserver und der Apache Tomcat-Server, der mit SiteScope bereitgestellt wird. Um den vollständigen Zugriff auf SiteScope zu begrenzen, müssen Sie die jeweiligen Einstellungen für

beide Server anwenden.

Festlegen der SiteScope-Benutzereinstellungen

SiteScope-Benutzerprofile dienen dazu, einen Benutzernamen und ein Kennwort für den Zugriff auf die SiteScope-Schnittstelle anzufordern. Nach der Installation ist der Zugriff auf SiteScope normalerweise für alle Benutzer mit HTTP-Zugriff auf den Server möglich, auf dem SiteScope ausgeführt wird.

Standardmäßig wird SiteScope mit nur einem Benutzerkonto installiert. Für dieses Konto ist weder ein Standardbenutzername noch ein Konto definiert. Es handelt sich dabei um das Administratorkonto.

Sie sollten einen Benutzernamen und ein Kennwort für dieses Konto festlegen, wenn Sie das Produkt installiert haben und darauf zugreifen. Sie können auch andere Benutzerkontoprofile erstellen, um zu steuern, wie andere Benutzer auf das Konto zugreifen und welche Aktionen sie durchführen können. Weitere Informationen zum Erstellen von Benutzerkonten finden Sie im Abschnitt zu den Voreinstellungen für die Benutzerverwaltung unter "Verwenden von SiteScope" in der SiteScope-Hilfe.

Kennwortverschlüsselung

Alle SiteScope-Kennwörter werden mithilfe einer Methode namens Triple Data Encryption Standard (TDES) verschlüsselt. TDES wendet den Datenverschlüsselungsalgorithmus drei Mal hintereinander auf alle 64-Bit-Blöcke Text an und verwendet dabei zwei oder drei verschiedene Schlüssel. Dadurch wird es nicht autorisierten Benutzer extrem schwer gemacht, das ursprüngliche Kennwort zu reproduzieren.

Verwenden von TLS (Transport Layer Security), der Transportschichtsicherheit für den Zugriff auf SiteScope

Sie können SiteScope für die Verwendung von TLS zur Steuerung des Zugriffs auf die Produktschnittstelle konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Kommunikation über eine sichere Verbindung" auf Seite 189.

Hinweis: TLS (Transport Layer Security) ist der neue Name für SSL (Secure Sockets Layer). Die SiteScope-Benutzeroberfläche beinhaltet immer noch Hinweise auf SSL. Die Begriffe sind in SiteScope austauschbar.

Smartcard-Authentifizierung

Smartcards sind physische Geräte, die für die Identifizierung von Benutzern in sicheren Systemen verwendet werden. Diese Karten können verwendet werden, um Zertifikate zu speichern, die die Identität des Benutzers überprüfen und den Zugriff auf sichere Umgebungen ermöglichen.

SiteScope unterstützt die Benutzerauthentifizierung mit Smartcards. Wenn die Smartcard-Authentifizierung konfiguriert ist, können Sie sich ohne gültige Smartcard nicht bei SiteScope anmelden. Es gibt unterschiedliche arten von Smartcards, die mit SiteScope benutzt werden können, u. a.:

- **CAC.** Die "Common Access Card" (oder CAC-Karte) ist eine Smartcard, die vom US-Verteidigungsministerium eingesetzt wird. Sie eignet sich für alle möglichen Aufgaben, die innerhalb des Militärs auf Regierungssystemen ausgeführt werden müssen.

- **PIV.** Genau wie ihre Kollegen beim Militär benötigen auch Beamte und Bedienstete des Bundes sowie externe Mitarbeiter in zivilen Behörden Smartcards. Sie verwenden einen ähnlichen Standard, die so genannte PIV-Karte (Personal Identification Verification). Die Karten unterscheiden sich geringfügig von CAC-Karten und haben abhängig von der Ausgabestelle unterschiedliche Informationen aufgedruckt. Für sie werden andere CA-Server (Certificate Authority, Zertifizierungsstelle) verwendet als für CAC-Karten. PIV-Karten werden mit den Daten personalisiert, die das PIV-System benötigt, um dem Inhaber Zugang zu staatlichen Einrichtungen und Informationssystemen zu gewähren, angemessene Sicherheit für alle in Frage kommenden behördlichen Applikationen zu garantieren sowie Interoperabilität zwischen den unterschiedlichen staatlichen Einrichtungen zu gewährleisten, welche mit den Standards arbeiten.

Details zur Konfiguration der Smartcard-Authentifizierung finden Sie unter "Konfigurieren der Smartcard-Authentifizierung" auf Seite 189.

Hinweis: Es gibt eine Vielzahl unterschiedlicher Smartcard-Anbieter. Um zu gewährleisten, dass alle Varianten für die Nutzung von Clientzertifikaten unterstützt werden, können Sie die folgenden Parameter in der Datei **<SiteScope-Stammverzeichnis>\groups\master.config** nutzen:

- _clientCertificateAuthJITCComplianceEnforcementEnabled
- _clientCertificateAuthSmartCardEnforcementEnabled
- _clientCertificateAuthIsGetUidFromSubject

- _clientCertificateAuthAllowLocalUsers
- _clientCertificateSubjectAlternativeNamesGeneralName
- _clientCertificateAuthEnabled

JITC-Zertifizierung (Joint Interoperability Test Command)

Das JITC ist eine US-Militäreinrichtung, die Technologien aus unterschiedlichen Zweigen des Militärs und ziviler Behörden testet. Das JITC übernimmt die Überprüfung, Bewertung und Zertifizierung von netzwerkzentrierten militärischen Funktionen, bevor diese erworben und eingesetzt werden.

SiteScope wird derzeit vom JITC getestet und bewertet. Die JITC-Zertifizierung ist eine der Common Criteria-Zertifizierungen, die für die Authentifizierung per CAC und Smartcard erforderlich sind.

Hinweis: Sobald die Bewertung abgeschlossen ist, werden die Ergebnisse in diesem Abschnitt veröffentlicht.

Common Criteria-Zertifizierung

Mit HP SiteScope solle eine branchenführende Überwachungssoftware bereitgestellt werden, die sich an Branchenstandards und staatlichen Zertifizierungsprogrammen orientiert.

HP SiteScope durchläuft derzeit die Common Criteria-Zertifizierung mit Vertrauenswürdigkeitsstufe (Evaluation Assurance Level, EAL) 2+. Zertifizierungen wie Common Criteria sind fundamental wichtig für Sicherheitsmaßnahmen auf Regierungsebene. Zusätzlich zum Schutz von Regierungskunden vor zunehmenden Datenangriffen und -diebstahl unterstützen diese Sicherheitszertifikate auch die globalen Geschäftskunden von HP.

Die "Common Criteria for Information Technology Security Evaluation", gemeinsame Kriterien für Sicherheit in der Informationstechnologie (abgekürzt Common Criteria), sind ein internationaler Standard für die Computersicherheitszertifizierung. Common Criteria ist eine Bewertung, ob das Produkt die versprochenen Funktionen bereitstellt und auf einer sicheren und stabilen Generierung beruht. Die Ergebnisse werden von unabhängigen Testlaboren überprüft und bewertet. Es ist seitens der US-Regierung darüber hinaus für den staatlichen Erwerb von Sicherheitsprodukten erforderlich.

FIPS 140-2-Konformität

Als Teil der Common Criteria-Zertifizierung kann SiteScope für die Ausführung im FIPS 140-2-konformen Modus konfiguriert werden. FIPS 140-2, d. h. der Federal Information Processing Standard 140-2, ist eine Zusammenstellung von Sicherheitsanforderungen für kryptografische Module. FIPS 140-2 wird vom CMVP (Cryptographic Module Validation Program) beaufsichtigt, einem gemeinsamen Programm der US-Regierung und der kanadischen Regierung.

SiteScope 11.30 ist zur Zeit die einzige Version von SiteScope, die für den FIPS 140-2-konformen Modus konfiguriert werden kann.

Weitere Informationen zu FIPS 140-2 und zum Konfigurieren von SiteScope für den FIPS 140-2-konformen Modus finden Sie unter "Konfigurieren von SiteScope für den Betrieb im FIPS 140-2-konformen Modus" auf Seite 197.

Verschlüsseln von Daten mit einem benutzerdefinierten Schlüssel

Standardmäßig verwendet SiteScope einen Standardverschlüsselungsalgorithmus für die Verschlüsselung von persistenten Daten (dazu gehören Konfigurationsdaten aller definierter Monitore, Gruppen, Warnungen, Vorlagen und viele andere SiteScope-Entitäten). Sie können die Schlüsselverwaltung im Hardening-Tool verwenden, um die kryptografischen Schlüssel zu ändern, die für die Verschlüsselung von Persistenzdaten verwendet werden.

Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 208.

Empfehlungen für das Sichern von Benutzerkonten

Die folgende Tabelle gibt einen Überblick über die in SiteScope vorhandenen Konten und welche Maßnahmen Sie zu ihrer Sicherung ergreifen können.

Benutzerkonto	Beschreibung	Sicherungsmaßnahmen
Standard (Administrator)	Standardmäßig wird SiteScope mit nur einem Benutzerkonto installiert. Für dieses Konto ist weder ein Standardbenutzername noch ein Konto definiert.	Um den Zugriff auf dieses Konto und seine Berechtigungen einzuschränken, empfehlen wir, das Kontoprofil nach der Installation zu bearbeiten und einen Benutzernamen und ein Kennwort für die Anmeldung hinzuzufügen. SiteScope zeigt dann eine Anmeldeseite an, bevor Sie auf SiteScope zugreifen können. Sie sollten darüber hinaus weitere Benutzerkontoprofile erstellen, um zu kontrollieren, wie andere Benutzer auf das Produkt zugreifen und welche Aktionen sie durchführen können. Weitere Informationen finden Sie im Abschnitt "Voreinstellungen für Benutzerverwaltung" unter "Verwenden von SiteScope" in der SiteScope-Hilfe. **Hinweis:** Um weitere Konten erstellen zu können, müssen Sie zunächst das Administrator-Kontoprofil bearbeiten und einen Benutzeranmeldenamen und ein Kennwort eingeben.
Integration Viewer	Standardmäßig stellt SiteScope den Benutzertyp **Integration Viewer** bereit, der für den Drilldown von HPOM-Ereignissen verwendet wird. Hierbei handelt es sich um einen regulären Benutzer, dem Berechtigungen zum Anzeigen und zum Aktualisieren von Gruppen und Monitoren gewährt wurden. Weitere Informationen finden Sie unter "Integration von SiteScope mit HP Operations Manager-Produkten".	Wenn Sie über eine HPOM- oder BSM-Integration arbeiten, wird empfohlen, das vorgegebene Anmeldekennwort für das Integration Viewer-Kontoprofil zu ändern. Wenn Sie über keine HPOM-/BSM-Integration verfügen, können Sie diesen Benutzertypen deaktivieren oder löschen.

Benutzerkonto	Beschreibung	Sicherungsmaßnahmen
SiteScope-Dienstbenutzer	**Für Windows:** Standardmäßig wird SiteScope für die Ausführung als **lokales Systemkonto** installiert (gilt nicht bei Linux-Installationen). Dieses Konto verfügt über weitreichende Privilegien auf dem lokalen Computer und über Zugriff auf meisten Systemobjekte. Wird SiteScope unter einem lokalen Systemkonto ausgeführt, versucht es, eine Verbindung zu Remoteservern unter Verwendung der in SiteScope konfigurierten Anmeldeinformationen des Servers herzustellen. **Für Linux:** SiteScope muss vom Root-Benutzer in einer Linux-Umgebung installiert werden.	**Für Windows:** Wir empfehlen, den SiteScope-Dienst so zu ändern, dass eine Anmeldung als Benutzer mit Domänenadministratorberechtigungen durchgeführt wird. So erhält SiteScope Zugriffsberechtigungen für das Überwachen von Serverdaten innerhalb der Domäne. Geben Sie ein Konto und ein Kennwort (bestätigen Sie das Kennwort) für den Zugriff auf die Remoteserver ein. Verwenden Sie in einer Domänenumgebung hierfür den Domänenadministrator und in einer Nicht-Domänenumgebung den integrierten Administrator-Benutzer. Sie können diese Einstellung während oder nach der Installation ändern (siehe Abschnitt zur SiteScope-Installation). Informationen hierzu finden Sie unter "Installation mithilfe des Installationsassistenten" auf Seite 116. **Für Linux:** Nachdem SiteScope installiert wurde, können Sie ein Nicht-Root-Benutzerkonto mit den Berechtigungen zum Ausführen von SiteScope erstellen (sofern der SiteScope-Webserver nicht auf einem privilegierten Port ausgeführt wird; in diesem Fall sollte die Ausführung durch den Root-Benutzer erfolgen). Details zum Konfigurieren eines Nicht-Root-Benutzers mit Berechtigungen zum Ausführen von SiteScope finden Sie unter "Empfehlungen für das Sichern von Benutzerkonten" auf Seite 185.

Benutzerkonto	Beschreibung	Sicherungsmaßnahmen
JMX-Benutzer	JMX hat standardmäßig Remotezugriff auf den SiteScope-Server (die Verbindung über das JMX-Protokoll kann mit dem Hardening-Tool konfiguriert werden).	Für eine vollständige Sicherung von SiteScope wird empfohlen, den JMX-Remotezugriff im Hardening-Tool zu deaktivieren. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zur Konfiguration des JMX-Remote-Zugriffs" auf Seite 228.
API-Benutzer	Normalerweise gibt es diesen Benutzertypen nicht (SiteScope verfügt über eine Reihe von APIs, für die keine Authentifizierung erforderlich ist).	Sollte es erforderlich sein, unbenutzte API-Benutzer zu deaktivieren, wählen Sie **Voreinstellungen > Infrastrukturvoreinstellungen > Benutzerdefinierte Einstellungen** und legen Sie die Option **Alte APIs deaktivieren** auf `true` fest.

Konfigurieren eines Warnungsbanners für die Anzeige bei der Anmeldung

Sie können SiteScope so konfigurieren, dass eine Warnmeldung angezeigt, dass sich Benutzer bei SiteScope in einem sicheren System anmelden.

So konfigurieren Sie eine Meldung für die Anzeige bei der Anmeldung:

1. Öffnen Sie die Datei **<SiteScope-Stammverzeichnis>\templates.fips\banner.txt** in einem Texteditor und geben Sie den Text ein, der im Anmeldefenster angezeigt werden soll.
2. Öffnen Sie die Datei **<SiteScope-Stammverzeichnis>\groups\master.config** in einem Texteditor und ändern Sie den Wert der Eigenschaft **_isLogonWarningBannerDisplayed=** in **true**.

   Sobald sich ein Benutzer bei SiteScope anmeldet, wird die Benachrichtigungsmeldung angezeigt. Der Benutzer muss die Meldung bestätigen, bevor er SiteScope verwenden kann.

Kapitel 18: Konfigurieren von SiteScope für die Kommunikation über eine sichere Verbindung

Dieses Kapitel umfasst die folgenden Themen:

Konfigurieren von SiteScope für das Anfordern einer sicheren Verbindung

Sie können SiteScope so konfigurieren, dass ein sicherer Zugang zu den Oberflächen (Benutzeroberfläche und API) erforderlich ist. Gehen Sie hierzu wie folgt vor:

1. Erhalten des Serverzertifikats, das für den vollqualifizierte Domänenname (Fully Qualified Domain Name, FQDN) des SiteScope-Servers ausgegeben wurde
2. Konfigurieren von SiteScope für die Antwort auf Zugriffsanforderungen nur über einen sicheren Kanal.

Dazu haben Sie folgende Möglichkeiten.

- Verwenden des Hardening-Tools für die Konfiguration von SiteScope, um diese Konfiguration durchzuführen (empfohlene Methode). Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für sichere Verbindungen" auf Seite 219.
- Manuelles Konfigurieren von SiteScope für die Verwendung von TLS. Weitere Informationen finden Sie unter "Manuelles Konfigurieren von SiteScope für das Verwenden einer sicheren Verbindung" auf Seite 268.

Konfigurieren der Smartcard-Authentifizierung

Smartcards sind physische Geräte, die für die Identifizierung von Benutzern in sicheren Systemen verwendet werden. Diese Karten können verwendet werden, um Zertifikate zu speichern, die die

Identität des Benutzers überprüfen und den Zugriff auf sichere Umgebungen ermöglichen.

SiteScope unterstützt die Benutzerauthentifizierung mit Smartcards. Wenn die Smartcard-Authentifizierung konfiguriert ist, können Sie sich ohne gültige Smartcard nicht bei SiteScope anmelden.

SiteScope kann so konfiguriert werden, dass diese Zertifikate anstelle des Standardmodells verwendet werden, bei dem der einzelne Benutzer manuell einen Benutzernamen und ein Kennwort angeben muss. Sie definieren eine Methode, den Benutzernamen vom Zertifikat, das auf jeder Karte gespeichert ist, zu extrahieren.

Wenn SiteScope für die Smartcard-Authentifizierung konfiguriert ist, können sich Benutzer nur mit gültiger Smartcard bei SiteScope anmelden. Die Option zur Anmeldung mit der manuellen Eingabe von Benutzernamen und Kennwort ist für alle Benutzer gesperrt, bis die Smartcard-Konfiguration deaktiviert wird.

Wenn die Smartcard-Authentifizierung in BSM konfiguriert ist und SiteScope in BSM integriert werden soll, müssen Sie die SiteScope-Smartcard-Authentifizierung für die Authentifizierung des BSM-Clientzertifikats konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verbindung mit einem BSM-Server, der eine sichere Verbindung erfordert" auf Seite 214.

Wenn die Smartcard-Authentifizierung in SiteScope konfiguriert ist und BSM mit SiteScope verbunden werden soll, müssen Sie BSM für die Authentifizierung mit dem Clientzertifikat in SiteScope konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verbindung mit einem BSM-Server, der eine sichere Verbindung erfordert" auf Seite 214.

Hinweis: Wenn die Smartcard-Authentifizierung aktiviert ist, wird nur der Internet Explorer unter einem Windows-Betriebssystem als Browser unterstützt.

Wenn die Smartcard-Authentifizierung deaktiviert ist, die Clientzertifikatauthentifizierung jedoch aktiviert ist, finden Sie zum Verwenden von SiteScope in Firefox weitere Informationen unter "Verwenden von Firefox, wenn die Clientzertifizierung aktiviert ist" auf Seite 192.

Tipp: Weitere Informationen zu Smartcards finden Sie im Konfigurationshandbuch zur Smartcard-Authentifizierung (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01134341).

Konfigurieren von SiteScope für das Anfordern der Authentifizierung des Clientzertifikats

Wenn Sie SiteScope für die Ausführung über TLS konfiguriert haben (siehe "Konfigurieren von SiteScope für das Anfordern einer sicheren Verbindung" auf Seite 189), können Sie anschließend SiteScope und den öffentlichen SiteScope-API-Client so konfigurieren, dass eine Clientzertifikatauthentifizierung erforderlich ist.

Verwenden Sie hierfür das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit). Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools für das Konfigurieren von SiteScope und der Clientzertifikatauthentifizierung von öffentlichen SiteScope-APIs" auf Seite 227.

Kapitel 19: Erweiterte Hardening-Konfiguration

Dieses Kapitel umfasst die folgenden Themen:

Konfigurieren von SiteScope zum Überprüfen der Zertifikatsperrung

Sie können das Hardening-Tool für die Konfiguration von SiteScope verwenden, um das erneute Aufrufen von Clientzertifikaten zu überprüfen. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für das Überprüfen der Zertifikatssperre" auf Seite 221.

Verwenden von Firefox, wenn die Clientzertifizierung aktiviert ist

Wenn die Smartcard-Authentifizierung deaktiviert ist, die Clientzertifikatauthentifizierung jedoch aktiviert ist, müssen Sie zum Öffnen der SiteScope-Benutzeroberfläche in Firefox wie folgt vorgehen.

1. Importieren Sie Ihr persönliches Zertifikat wie nachfolgend beschrieben in Firefox:

    a. Wechseln Sie in Firefox zu **Extras** > **Optionen** > **Erweitert** > **Zertifikate** > **Zertifikate anzeigen**. Das Dialogfeld **Zertifikat-Manager** wird geöffnet.

b. Klicken Sie auf **Importieren...** und öffnen Sie Ihr persönliches Zertifikat im Dateiformat **.pfx** (oder **.p12**). Das Dialogfeld zur Kennworteingabe wird geöffnet.

c. Geben Sie das Kennwort ein, das für die Verschlüsselung des Zertifikatsicherung verschlüsselt wurde, und klicken Sie auf **OK**. Das Zertifikat wird im Dialogfeld **Zertifikat-Manager** angezeigt und es wird bestätigt, dass es zu Firefox hinzugefügt wird.

2. Importieren Sie Ihr persönliches Zertifikat wie nachfolgend beschrieben in die Client-JRE:

a. Öffnen Sie in der JRE die Java-Systemsteuerung.

b. Wechseln Sie zu **Sicherheit** > **Zertifikate** und wählen Sie die Clientauthentifizierung als Zertifikatstyp aus.

c. Klicken Sie auf **Importieren** und öffnen Sie das Clientzertifikat, das Sie in Firefox importiert haben.

d. Klicken Sie auf **OK**. Das persönliche Zertifikat wird in der JRE angezeigt.

3. Geben Sie den SiteScope-URL in Firefox ein. Das Dialogfeld zur Benutzeridentifizierung wird angezeigt. Wählen Sie das persönliche Zertifikat aus, das Sie in Schritt 1 erstellt haben, zur Identifizierung aus.

Importieren von Zertifikaten der Zertifizierungsstelle in TrustStores von SiteScope

Damit SiteScope einem Clientzertifikat vertrauen kann, muss SiteScope der Zertifizierungsstelle vertrauen, die das Clientzertifikat herausgegeben hat. Damit SiteScope einer Zertifizierungsstelle vertrauen kann, muss das Zertifikat der Zertifizierungsstelle auf dem SiteScope-Server und in den Haupt-TrustStores gespeichert werden.

Der TrustStore des SiteScope-Servers ist für die Authentifizierung aller eingehender Verbindungsanforderungen von Clients (API und Browser) verantwortlich.

Der Haupt-TrustStore von SiteScope ist ein Java-TrustStore der Zertifizierungsstelle, der sich im Java-Verzeichnis im SiteScope-Installationsverzeichnis befindet. Dieser TrustStore ist für das SiteScope-Zertifikatemanagement verantwortlich.

Sie verwenden das Hardening-Tool für den Import von Zertifikaten der Zertifizierungsstelle in SiteScope-Server und Haupt-TrustStores. Weitere Informationen finden Sie unter "Verwenden des

Hardening-Tools zum Importieren von Zertifikaten der Zertifizierungsstelle in SiteScope-TrustStores" auf Seite 223.

Deaktivieren des Remotezugriffs auf JMX

JMX verfügt standardmäßig über Remotezugriff auf SiteScope. Sie können diesen Zugriff deaktivieren.

Hinweis: Für eine vollständige Sicherung von SiteScope wird empfohlen, den JMX-Remotezugriff zu deaktivieren.

Sie verwenden das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) für die Konfiguration des JMX-Remotezugriffs. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zur Konfiguration des JMX-Remote-Zugriffs" auf Seite 228.

Wiederherstellen einer gesicherten Konfiguration

Wenn Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) ausführen, wird die bestehende SiteScope-Konfiguration automatisch gesichert. Informationen zum Wiederherstellen einer gesicherten Konfiguration finden Sie unter "Verwenden des Hardening-Tools für das Wiederherstellen einer gesicherten Konfiguration" auf Seite 229.

Konfigurieren von Framingfiltern in SiteScope

Hinweis: Dieses Thema ist nur relevant, wenn SiteScope 11.30 IP1 installiert ist.

Ein Frame ist ein Teil einer Webseite oder eines Browserfensters, in dem Inhalt unabhängig von seinem Container angezeigt wird und der die Möglichkeit zum unabhängigen Laden von Inhalten bietet. Das Framing ist für SiteScope standardmäßig aktiviert.

Wenn anderen Sites das Framing von SiteScope nicht möglich sein soll oder Sie nur das teilweise Framing zulassen möchten, müssen Sie folgendermaßen vorgehen:

1. Öffnen Sie die Datei **master.config** unter **<SiteScope-Stammverzeichnis>\groups** und konfigurieren Sie die Eigenschaften **_disableFramingFiltering** wie erforderlich.

   - **True.** Das Filtern ist deaktiviert, sodass das Framing von SiteScope für jede Webseite zulässig ist. (Dies ist die Standardeinstellung.)

- **False.** Das Filtern ist aktiviert, wodurch das Framing von SiteScope für Webseiten verhindert wird. Dies schließt HP Produkte wie BSM, HPOM und Performance Center ein. Die gehostete Benutzeroberfläche von BSM ist beispielsweise nicht funktionsfähig.
- **Smart.** Ermöglicht das teilweise Framing von SiteScope gemäß den in der Eigenschaft **_ framingFilteringPlugsClasses** aufgelisteten Plugs.

2. Wenn Sie das teilweise Framing verwenden, müssen Sie die Plugs, die durch den Filter angewendet werden sollen, erstellen und zur Eigenschaft **_framingFilteringPlugsClasses** hinzufügen.

   a. Navigieren Sie zur Eigenschaft **_framingFilteringPlugsClasses** in der Datei **master.config**. Standardmäßig schließt diese Eigenschaft die folgenden Standard-Plugs ein:

      - `com.mercury.sitescope.web.request.framing.plugs.LWSSOPlug`. Lässt Anforderungen zu, die mit einem LW-SSO-Token (Lightweight Single Sign-On) gesendet werden.
      - `com.mercury.sitescope.web.request.framing.plugs.BSMPlug`. Lässt Anforderungen zu, die von der SAM-Verwaltung von BSM gesendet werden.
      - `com.mercury.sitescope.web.request.framing.plugs.PerformanceCenterPlug`. Lässt Anforderungen von Performance Center zu.

      Sie können jedes beliebige Standard-Plug deaktivieren, indem sie es aus der Eigenschaft entfernen.

   b. So fügen Sie eigene Plugs hinzu

      i. Schreiben Sie das Plug, das die Schnittstelle implementieren muss: `com.mercury.sitescope.web.request.framing.IFramingPlug`.

      Diese Schnittstelle befindet sich in **<SiteScope-Stammverzeichnis>\WEB-INF\lib\ss_ webaccess.jar**. Diese JAR-Datei muss im Klassenpfad angegeben sein, um das Plug zu kompilieren.

      Nachfolgend sehen Sie ein Beispiel für ein Plug, das das Framing für einen Parameter mit dem Anforderungsnamen *exampleParameter* zulässt, wenn dieser Parameter auf **True** festgelegt ist:

```
package com.company.sitescope.examples.plug
import javax.servlet.ServletRequest;
import com.mercury.sitescope.web.request.framing.IFramingPlug;
```

```
public class ExamplePlug implements IFramingPlug{
    @Override
       public boolean isAuthorized(ServletRequest request) {
          //Add the code that will determine whether this request comes from an
authorized product.
          if (request == null){
               return false;
           }
           HttpServletRequest httpServletRequest = (HttpServletRequest)request;
           if (httpServletRequest.getParameter("exampleParameter") == null){
           return false;
           }

           return "true".equalsIgnoreCase((String)httpServletRequest.getParameter
("exampleParameter"));
           }
}
```

ii. Fügen Sie den vollständig qualifizierten Klassennamen zur Eigenschaft **_ framingFilteringPlugsClasses** in der Datei **master.config** (durch ein Komma getrennt) hinzu.

`com.company.sitescope.examples.plug.ExamplePlug` sollte beispielsweise zur Liste hinzugefügt werden.

iii. Erstellen Sie eine JAR-Datei, die alle Ihre Plugs enthält, und fügen Sie sie zum Ordner **<SiteScope-Stammverzeichnis>\WEB-INF\lib** hinzu.

3. Starten Sie SiteScope neu (dies ist erforderlich, nachdem Änderungen an der Datei **master.config** vorgenommen wurden).

Kapitel 20: Konfigurieren von SiteScope für den Betrieb im FIPS 140-2-konformen Modus

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über die FIPS 140-2-Konformität

Bei FIPS 140-2 (Federal Information Processing Standard) handelt es sich um einen Zertifizierungsstandard der US- und kanadischen Regierung für Verschlüsselungs- und kryptografische Module, in denen jede einzelne Verschlüsselungskomponeten in der Gesamtlösung eine unabhängige Zertifizierung benötigt. Die Standards wurden entwickelt, um Verfahren, Architektur, Algorithmen und andere Techniken zu definieren, die in Computersystemen verwendet werden. Der vollständige FIPS-Text steht online über das National Institute of Standards and Technology (NIST) zur Verfügung.

Für eine Ausführung im FIPS 140-2-konformen Modus muss der SiteScope-Administrator diesen mithilfe des Hardening-Tools von SiteScope aktivieren. SiteScope führt Selbsttests beim Start aus, führt den Integrationstest für kryptografische Module durch und stellt dann das Schlüsselmaterial wieder her. An diesem Punkt wird SiteScope im FIPS 140-2-Modus ausgeführt.

Gründe für das Aktivieren des FIPS-Modus:

Ihre Organisation muss in den folgenden Fällen möglicherweise SiteScope im FIPS-Modus verwenden:

- Ihre Organisation ist eine Abteilung oder ein Auftragnehmer der Regierung.
- Sie möchten Ihre Sicherheit erhöhen, um Ihr Unternehmen vor zunehmenden Datenangriffen und vor Datendiebstahl schützen.

Softwareanforderungen

FIPS-Konformität setzt voraus, dass Ihr Betriebssystem und Ihr Browser bestimmte Bedingungen für Version und Einstellungen erfüllen.

Während in SiteScope alle Browser unterstützt werden, können im FIPS-Modus nicht alle Betriebssystemversionen die kryptografischen Anforderungen von FIPS erfüllen. Dies bedeutet, dass einige Betriebssysteme, die SiteScope normalerweise unterstützt, nicht im FIPS-Modus unterstützt werden.

Für die Ausführung im FIPS-Modus muss SiteScope unter einem der folgenden Betriebssysteme installiert werden:

• Windows Server 2008 R2 (64-Bit)

• Windows Server 2012 R2 (64-Bit)

JDBC-Treiber

Wenn SiteScope im FIPS-Modus ausgeführt wird, sollten Sie den JDBC-Treiber anstelle der Standardtreiber verwenden, die mit SiteScope geliefert werden.

Verbindung von SiteScope mit Nicht-FIPS-konformen Applikationen

Wenn SiteScope mit einer Applikation verbunden ist, die einen nicht von FIPS genehmigten Algorithmus verwendet, ist die Verbindung zwischen SiteScope und dieser Applikation nicht FIPS-konform (auch wenn der FIPS 140-2-Modus in SiteScope aktiviert wurde).

Aktivieren des FIPS 140-2-konformen Modus

Wenn SiteScope im FIPS 140-2-konformen Modus mit einer sicheren Verbindung ausgeführt werden soll, müssen Sie die folgenden Schritte ausführen:

- "Schritt 1: Konfigurieren der LDAP-Integration" auf der nächsten Seite
- "Schritt 2: Konfigurieren des Windows-Betriebssystems für den FIPS 140-2-konformen Modus" auf der nächsten Seite
- "Schritt 3: Ausführen von SiteScopeHardeningToolRuntime " auf Seite 201
- "Schritt 4: Deaktivieren des JMX-Remotezugriffs auf den SiteScope-Server " auf Seite 202
- "Schritt 5: Konfigurieren von SSL" auf Seite 202
- "Schritt 6: Konfigurieren der Clientauthentifizierung" auf Seite 204

Hinweis: Wenn Sie planen, eine Datenverschlüsselung der Schlüsselverwaltung zu aktivieren (eine stärkere Verschlüsselung, als die Standardmethode), müssen Sie dies nach dem Aktivieren des FIPS 140-2-konformen Modus durchführen. Wurde die Datenverschlüsselung der Schlüsselverwaltung bereits konfiguriert, müssen Sie den unter "Aktivieren oder Deaktivieren des FIPS-konformen Modus nach dem Ändern des Verschlüsselungsschlüssels" auf Seite 211 beschriebenen Schritten folgen.

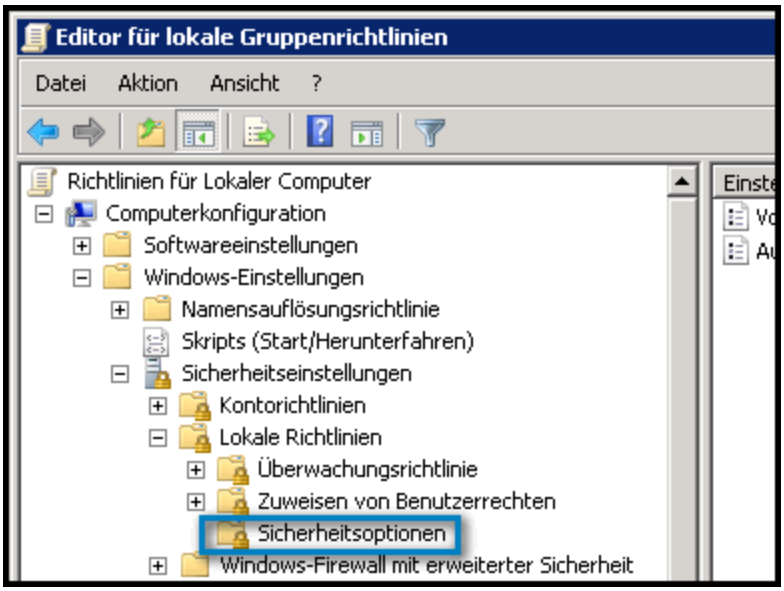
Schritt 1: Konfigurieren der LDAP-Integration

Die LDAP-Benutzerauthentifizierung muss aktiviert werden, um sich bei SiteScope mithilfe von Clientzertifikaten anmelden zu können.

1. Konfigurieren Sie den LDAP-Server in SiteScope. Weitere Informationen finden Sie unter "Einrichten von SiteScope zur Verwendung der LDAP-Authentifizierung" im SiteScope-Benutzerhandbuch in der SiteScope-Hilfe.
2. Erstellen Sie eine neue Rolle in der SiteScope-Benutzerverwaltung für LDAP-Benutzer.
3. Ändern Sie den SiteScope-Anmeldenamen des Administrators in die E-Mail-Adresse des LDAP-Benutzers. Diese sollte dem Benutzer im Clientzertifikat entsprechen (wie in Schritt 3 unter "Schritt 6: Konfigurieren der Clientauthentifizierung" auf Seite 204 eingegeben). Geben Sie kein Kennwort ein.

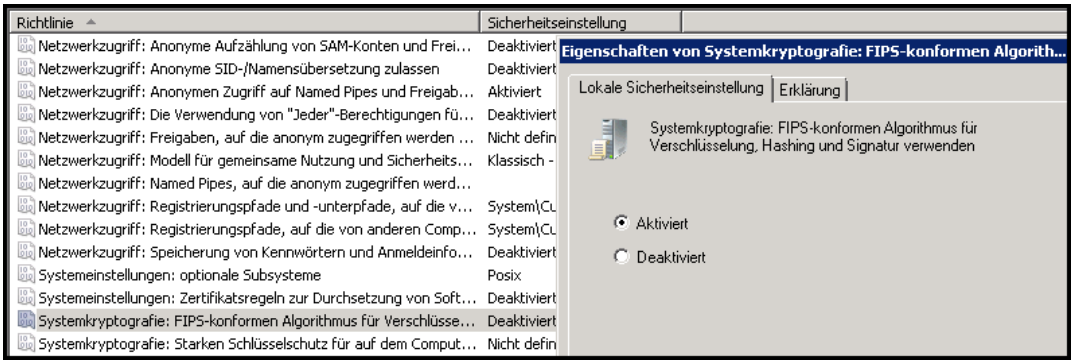
Schritt 2: Konfigurieren des Windows-Betriebssystems für den FIPS 140-2-konformen Modus

1. Konfigurieren Sie das Windows-Betriebssystems für den FIPS 140-2-konformen Modus.
    a. Verwenden Sie die Administrator-Anmeldeinformationen für die Anmeldung am Computer.
    b. Klicken Sie auf **Start** und **Ausführen**. Geben Sie `gpedit.msc` ein und drücken Sie dann die `EINGABETASTE`. Der lokale Gruppenrichtlinien-Editor wird geöffnet.
    c. Doppelklicken Sie im lokalen Gruppenrichtlinien-Editor auf **Windows-Einstellungen** unter dem Knoten **Computerkonfiguration** und doppelklicken Sie dann auf **Sicherheitseinstellungen**.
    d. Doppelklicken Sie unter **Sicherheitseinstellungen** auf **Lokale Richtlinien** und klicken Sie dann auf **Sicherheitsoptionen**.



e. Doppelklicken Sie im Abschnitt mit den Details auf **Systemkryptographie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**.

f. Unter **Systemkryptographie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden** klicken Sie auf **Aktiviert** und anschließend auf **OK**, um das Dialogfeld zu schließen.



g. Schließen Sie den lokalen Gruppenrichtlinien-Editor.

h. Stellen Sie sicher, dass diese Sicherheitsoption aktiviert wurde.

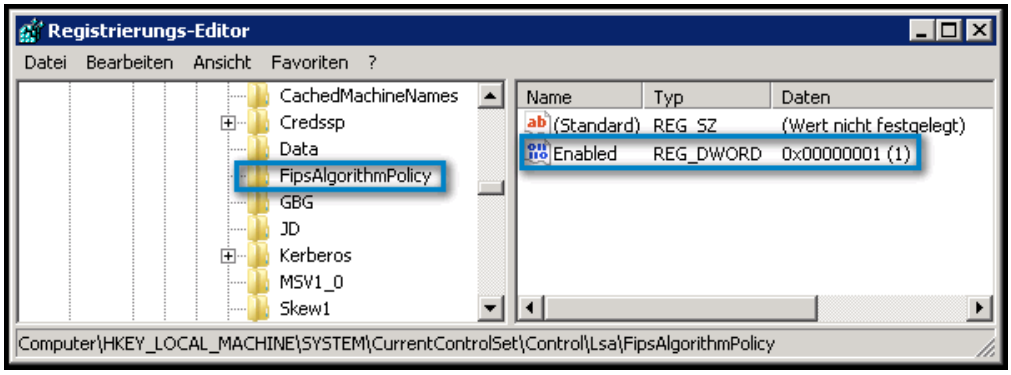
   i. Öffnen Sie den Registrierungs-Editor. Klicken Sie auf **Start** und **Ausführen**. Geben Sie `regedit` ein und drücken Sie dann die `EINGABETASTE`. Der Registrierungs-Editor wird geöffnet.

   ii. Suchen Sie den folgenden Schlüssel und überprüfen Sie den Wert.

- Schlüssel:
  HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled.

  Dieser Registrierungswert zeigt die aktuelle FIPS-Einstellung. Ist dieser Wert aktiviert, ist der Wert 1. Bei deaktivierter Einstellung ist der Wert 0.

- Wert: **1**.

iii. 

Tipp: Weitere Informationen finden Sie unter:

- http://technet.microsoft.com/en-us/library/cc750357.aspx
- http://support.microsoft.com/kb/811833

Schritt 3: Ausführen von SiteScopeHardeningToolRuntime

1. Kopieren Sie die Datei **SiteScopeHardeningToolRuntime.zip** aus dem Verzeichnis **\Tools** des SiteScope-Installationspakets auf den SiteScope-Server.

   a. Extrahieren Sie den Inhalt der Datei in den Ordner **<SiteScope-Stammverzeichnis>\tools\SiteScopeHardeningTool**.

   b. Starten Sie das Hardening-Tool, indem Sie folgenden Befehl über die Befehlszeile ausführen:

   ```
   <SiteScope_
   Stammverzeichnis>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

Schritt 4: Deaktivieren des JMX-Remotezugriffs auf den SiteScope-Server

Verwenden Sie das Hardening-Tool zum Deaktivieren des JMX-Remotezugriffs auf den SiteScope-Server:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.
2. Wählen Sie die Option zum Konfigurieren des JMX-Remotezugriffs aus.
3. Folgen Sie den Anweisungen im Tool für das Deaktivieren des JMX-Remotezugriffs.

   Tipp: Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Schritt 5: Konfigurieren von SSL

1. Starten Sie das Hardening-Tool, indem Sie folgenden Befehl über die Befehlszeile ausführen:

   ```
   <SiteScope_
   Stammverzeichnis>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

2. Geben Sie `1` ein, um die Option **SiteScope hardening configuration** auszuwählen.
3. Geben Sie einen Namen ein, der für die erstellte Sicherungsdatei verwendet werden soll. Dies ist erforderlich, wenn Sie den FIPS 140-2-konformen Modus deaktivieren müssen und die vorherige SiteScope-Konfiguration wiederherstellen müssen, die vor dem Ausführen des Hardening-Tools bestand. Weitere Informationen finden Sie unter "Deaktivieren des FIPS 140-2-konformen Modus" auf Seite 205.
4. Geben Sie `2` ein, um die Option **Configure SiteScope Standalone to work over SSL (https)** auszuwählen.
5. Geben Sie `Y` ein, um zu bestätigen, dass SiteScope für die Verwendung mit SSL konfiguriert werden soll.
6. Geben Sie `Y` ein, um zu bestätigen, dass SiteScope im FIPS 140-2-konformen Modus ausgeführt

werden soll.

7. Wenn der FIPS 140-2-konforme Modus erfolgreich konfiguriert wurde, wählen Sie eine der folgenden Methoden aus, um den SiteScope-Server-Keystore zu erstellen, der das SiteScope-Serverzertifikat aufnehmen soll:

   - **Importieren eines Server-Keystore im .pkcs12-Format**

     Das Werkzeug fordert Sie auf, einen Alias auszuwählen, in dem sich der Schlüssel für die SiteScope SSL-Authentifizierung befindet.

     Hinweis: Wenn Sie den SiteScope- und den öffentlichen SiteScope-API-Client später für die Clientauthentifizierung konfigurieren (siehe "Konfigurieren von SiteScope für das Anfordern der Authentifizierung des Clientzertifikats" auf Seite 191), verwendet SiteScope diesen Alias für den Export des Schlüssels in den Client-TrustStore der SiteScope-API.

     Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

   - **Erstellen Sie einen Server-Keystore, indem Sie eine Anforderung auf einem zertifizierten Server der Zertifizierungsstelle signieren.**

     Wenn Sie diese Option auswählen, wird ein neuer Keystore und eine Schlüsselanforderung an eine Zertifizierungsstelle für ein signiertes Zertifikat erstellt. Das erstellte Zertifikat wird anschließend in den Keystore importiert.

     Das Werkzeug fordert Sie auf, die Parameter des Server-Keystores einzugeben. Für den allgemeinen Namen müssen Sie denselben URL eingeben, der auf Ihrem Computer verwendet wurde, einschließlich des FQDN, sofern verwendet (z. B. `ihrserver.domäne.com`). Für den Alias-Namen müssen Sie den Namen Ihres Computers angeben (z. B. `ihrserver`).

8. Kopieren Sie das signierte SiteScope-Serverzertifikat, um ein signiertes Zertifikat von dem Server Ihrer Zertifizierungsstelle zu erstellen.

9. Geben Sie den vollständigen Pfad zum signierten Zertifikat ein, den Sie vom Server der Zertifizierungsstelle erhalten haben.

10. Geben Sie den vollständigen Pfad auf das Stamm-CA-Zertifikat ein, das für die Ausgabe des obigen Zertifikats verwendet wurde.

11. Geben Sie `yes` ein, um dem Zertifikat zu vertrauen, das Sie von dem Server der Zertifizierungsstelle erhalten haben. Das Zertifikat wird zum Keystore des SiteScope-Servers

hinzugefügt.

Schritt 6: Konfigurieren der Clientauthentifizierung

1. Geben Sie ein Kennwort für die Clientauthentifizierung des TrustStore des SiteScope-Servers ein. Das Kennwort muss aus mindestens 6 Zeichen bestehen und darf keine Sonderzeichen enthalten. Das Standardkennwort lautet `changeit`.

2. Geben Sie `Y` ein, um zu bestätigen, dass die Clientauthentifizierung konfiguriert werden soll.

   Wenn Sie die Clientauthentifizierung aktivieren, führt SiteScope die vollständige Clientauthentifizierung beim Handshaking durch und extrahiert ein Clientzertifikat. Dieses Clientzertifikat wird anhand des Benutzerverwaltungssystem (LDAP) von SiteScope überprüft. Weitere Informationen finden Sie unter "Schritt 1: Konfigurieren der LDAP-Integration" auf Seite 199.

3. Geben Sie eine Benutzernameneigenschaft für das Clientzertifikat in das AlternativeSubjectName-Feld ein. Der Standardbenutzername ist `Other Name`.

4. Geben Sie `Y` ein, um zu bestätigen, dass die Smartcard-Authentifizierung konfiguriert werden soll.

   Wenn Sie die Smartcard-Authentifizierung aktivieren, überprüft SiteScope, dass das Clientzertifikat von einem Hardwaregerät stammt, und fügt das Zertifikat zum SiteScope-TrustStore hinzu.

   Weitere Informationen zur Smartcard-Authentifizierung finden Sie unter "Konfigurieren der Smartcard-Authentifizierung" auf Seite 189.

5. Geben Sie `Y` ein, um zu bestätigen, dass Sie CA-Zertifkate zum SiteScope-TrustStore hinzufügen möchten.

   Hinweis: Damit SiteScope einem Clientzertifikat vertrauen kann, muss SiteScope der Zertifizierungsstelle vertrauen, die das Clientzertifikat herausgegeben hat. Damit SiteScope einer Zertifizierungsstelle vertrauen kann, muss das Zertifikat der Zertifizierungsstelle in den SiteScope-TrustStore importiert werden.

6. Geben Sie den vollständigen Pfad für das CA-Zertifikat im CER-Format ein.

7. Das CA-Zertifikat wird zum SiteScope-TrustStore hinzugefügt.

Wenn das Zertifikat bereits im Keystore besteht, wird eine Meldung angezeigt. Geben Sie yes ein, um zu bestätigen, dass Sie das Zertifkat zum SiteScope-TrustStore hinzufügen möchten.

8. (Optional) Um zusätzliche CA-Zertifikate zum TrustStore des SiteScope-Servers hinzuzufügen, geben Sie Y ein und wiederholen die Schritte 1-3.

   Hinweis: Es sind keine zusätzlichen CA-Zertifikate erforderlich.

9. Geben Sie Q ein, um das Verfahren für das Hardening-Tool abzuschließen.

Deaktivieren des FIPS 140-2-konformen Modus

Wenn der FIPS 140-2-konforme Modus aktiviert wurde und Sie eine sichere Verbindung verwenden, können Sie die Option zum Deaktivieren von FIPS im Hardening-Tool nicht verwenden, um den FIPS 140-2-konformen Modus zu deaktivieren. Stattdessen müssen Sie die vorherige SiteScope-Konfiguration wiederherstellen, die vor der Aktivierung des FIPS-Modus verwendet wurde.

Wenn der FIPS 140-2-konforme Modus aktiviert wurde und Sie eine nicht-sichere Verbindung verwenden, können Sie die Option zum Deaktivieren von FIPS im Hardening-Tool verwenden.

Deaktivieren des FIPS 140-2-konformen Modus für eine sichere Verbindung

1. Starten Sie das Hardening-Tool, indem Sie folgenden Befehl über die Befehlszeile ausführen:

   ```
   <SiteScope_
   Stammverzeichnis>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

2. Geben Sie 2 ein, um die Option **Restore SiteScope configuration from backup** auszuwählen.

3. Geben Sie die Zahl der Sicherungskonfiguration ein, die aus der Liste der verfügbaren Sicherungen wiederhergestellt werden soll.

4. Geben Sie y ein, um zu bestätigen, dass die ausgewählte Sicherungskonfiguration wiederhergestellt werden soll.

5. Geben Sie Q ein, um das Verfahren für das Hardening-Tool abzuschließen.

Deaktivieren des FIPS 140-2-konformen Modus für eine nicht-sichere Verbindung

1. Starten Sie das Hardening-Tool, indem Sie folgenden Befehl über die Befehlszeile ausführen:

   ```
   <SiteScope_
   Stammverzeichnis>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

2. Geben Sie `1` ein, um die Option **SiteScope hardening configuration** auszuwählen.
3. Wenn Sie im Tool dazu aufgefordert werden, wählen Sie die Option **Configure FIPS 140-2 compliancy for a non-secure connection** aus.
4. Geben Sie eine `2` ein, um den FIPS 140-2-konformen Modus zu deaktivieren.
5. Geben Sie `y` ein, um zu bestätigen, dass der FIPS 140-2-konforme Modus deaktiviert werden soll.
6. Geben Sie `Q` ein, um das Verfahren für das Hardening-Tool abzuschließen.

Fehlerbehebung und Einschränkungen

Einschränkungen:

- Nur SSH2 wird für SSH-Verbindungen unterstützt, wenn SiteScope im FIPS 140-2-Modus ausgeführt wird.
- Die Option **SSL statt TLS verwenden** aus den URL-Monitoren, dem URL-Werkzeug und dem Dialogfeld **Neuer HTTP-Empfänger/HTTP-Empfänger bearbeiten** wird ignoriert, wenn SiteScope im FIPS 140-2-Modus ausgeführt wird (Authentifizierung mit TLS ist im FIPS 140-2-Modus obligatorisch).

Fehlerbehebung:

- **Problem:** Es kann kein Zertifikat aus einem Remotehost mithilfe des Zertifikatemanagement in SiteScope importiert werden, wenn der FIPS 140-2-Modus aktiviert wurde.

  Problemumgehung: Importieren Sie das Zertifikat aus einer Datei; entweder aus der Seite des Zertifikatemanagements auf der SiteScope-Benutzeroberfläche oder manuell mithilfe des folgenden Befehls:

  ```
  keytool -import -file <vertrauenswürdige Zertifikatdatei> -alias
  ```

```
<vertrauenswürdiger Zertifikatname> -keypass <Kennwort> -keystore
<Truststore-Datei (SiteScope\java\lib\security\cacerts)>
-storepass <Kennwort> -providername JsafeJCE –storetype PKCS12
```

Kapitel 21: Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung

Dieses Kapitel umfasst die folgenden Themen:

Schlüsselverwaltung - Übersicht

Standardmäßig verwendet SiteScope einen Standardverschlüsselungsalgorithmus für die Verschlüsselung von persistenten Daten (zu den persistenten Daten gehören Konfigurationsdaten aller definierter Monitore, Gruppen, Warnungen, Vorlagen und viele andere SiteScope-Entitäten aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\persistency**).

Sie können die Verschlüsselungsoption für die Schlüsselverwaltung im Hardening-Tool verwenden, um den kryptografischen Schlüssel zu ändern, der in SiteScope zur Verschlüsselung von Persistenzdaten verwendet wird. Das Ändern der kryptografischen Schlüssel ermöglicht eine stärkere Verschlüsselung als die Standardverschlüsselung in SiteScope.

Die Verwendung der Schlüsselverwaltung für die Datenverschlüsselung wird in den folgenden SiteScope-Werkzeugen unterstützt: Hardening-Tool, Persistency Viewer und Persistency Logger. Die Schlüsselverwaltung für die Datenverschlüsselung kann auch für die Verwendung von SiteScope im FIPS 140-2-konformen Modus konfiguriert werden.

Wenn Sie Schlüsselverwaltung aktiviert ist, konfigurieren Sie SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung. Geben Sie dazu eine Passphrase ein, die von SiteScope verwendet wird, um einen neuen Schlüssel zu erstellen und die persistenten Daten zu verschlüsseln. Sie müssen die Passphrase eingeben, wenn Sie die SiteScope-Persistenzdaten aus der

aktuellen SiteScope-Instanz für einen späteren Import in SiteScope exportieren. Wenn Sie die Persistenzdaten importieren (während der Installation oder nach der Installation mit dem SiteScope-Konfigurationswerkzeug), müssen Sie dieselbe Passphrase für den SiteScope-Serverschlüssel eingeben. Beachten Sie, dass der Schlüssel nicht in der Persistenz gespeichert wird.

- Wenn Sie den FIPS 140-2-konformen Modus aktivieren oder deaktivieren möchten (siehe "Konfigurieren von SiteScope für den Betrieb im FIPS 140-2-konformen Modus" auf Seite 197), müssen Sie dies vornehmen, bevor Sie die Datenverschlüsselung der Schlüsselverwaltung aktivieren, um nicht die Datenverschlüsselung der Schlüsselverwaltung zu deaktivieren und anschließend wieder zu aktivieren.
- Wenn Sie den FIPS 140-2-konformen Modus aktivieren oder deaktivieren möchten, nachdem Sie die kryptografischen Schlüssel für die Verschlüsselung von SiteScope-Daten geändert haben, folgen Sie den Schritten unter "Aktivieren oder Deaktivieren des FIPS-konformen Modus nach dem Ändern des Verschlüsselungsschlüssels" auf Seite 211.

Fehlerbehebung und Einschränkungen

- Die Datenverschlüsselung der Schlüsselverwaltung wird nicht in SiteScope-Instanzen unterstützt, die auf Linux-Plattformen installiert sind.
- Die Datenverschlüsselung der Schlüsselverwaltung wird nicht unterstützt, wenn SiteScope Failover verwendet wird, um die Überwachung der Sicherungsinfrastruktur für die primäre SiteScope-Instanz (weder auf dem primären SiteScope-Server noch auf dem SiteScope Failover-Server) bereitzustellen. Wenn Sie SiteScope Failover mit einer SiteScope-Instanz verwenden, die die Verschlüsselung mit dem Standardschlüssel verwendet, und dann SiteScope für die Datenverschlüsselung der Schlüsselverwaltung mit dem Hardening-Tool konfigurieren, erhalten Sie einen Fehler des Typs UNEXPECTED_SHUTDOWN im Protokoll **high_availability.log** beim Spiegeln der Konfiguration.

Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung

Mithilfe der Schlüsselverwaltung können Sie die kryptografischen Schlüssel, die für das Verschlüsseln der SiteScope-Konfigurationsdaten (Persistenzdaten) verwendet werden, verwalten und ändern.

Hinweis: Wenn Sie SiteScope im FIPS 140-2-konformen Modus verwenden möchten (siehe "Übersicht über die FIPS 140-2-Konformität" auf Seite 197), müssen Sie den FIPS 140-2-konformen Modus konfigurieren, bevor Sie den kryptografischen Schlüssel ändern, um nicht die Datenverschlüsselung der Schlüsselverwaltung zu deaktivieren und anschließend wieder zu aktivieren. Wenn Sie den FIPS-Modus ändern müssen, nachdem Sie den Verschlüsselungsschlüssel angepasst haben, folgen Sie den unter "Aktivieren oder Deaktivieren des FIPS-konformen Modus nach dem Ändern des Verschlüsselungsschlüssels" auf der nächsten Seite beschriebenen Schritten.

1. Installieren Sie SiteScope.

   Weitere Informationen finden Sie unter "Installationsworkflow" auf Seite 103.

2. Starten Sie SiteScope (um SiteScope-Persistenzdaten zu generieren).

3. Beenden Sie SiteScope.

4. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus.

   a. Wenn Sie im Werkzeug dazu aufgefordert werden, wählen Sie die Option **Enable or re-encrypt key management data encryption** aus.

   b. Geben Sie `1` ein, um die Persistenzdaten mit einem benutzerdefinierten Schlüssel zu verschlüsseln oder erneut zu verschlüsseln. Das Ändern der kryptografischen Schlüssel für das Verschlüsseln der Konfiguration ermöglicht eine stärkere Verschlüsselung als die Standardverschlüsselung in SiteScope.

      Zum Wiederherstellen der Persistenzdaten in der Verschlüsselung mit dem Standardschlüssel geben Sie `2` ein.

   c. Bestätigen Sie, dass Sie die Persistenzdaten mit einem benutzerdefinierten Schlüssel verschlüsseln oder erneut verschlüsseln möchten.

   d. Geben Sie einen neue Passphrase ein, die für den benutzerdefinierten Schlüssel verwendet werden soll (bei dieser Passphrase handelt es sich nicht um die bereits verwendete Passphrase, sondern sie ist für die neue Iteration der Verschlüsselung gedacht). Die Passphrase darf kein Leerzeichen oder auskommentierte Zeichen enthalten.

      SiteScope generiert einen neuen Schlüssel und verwendet diesen für die Verschlüsselung der persistenten Daten.

Hinweis: Sie müssen diese Passphrase eingeben, wenn Sie den SiteScope-Konfigurationsassistenten oder das SiteScope-Konfigurationswerkzeug für den Export oder Import von SiteScope-Konfigurationsdaten verwenden, die mit diesem benutzerdefinierten Schlüssel verschlüsselt wurden. Beachten Sie dass die Passphrase nicht mit der .zip-Datei in der exportierten Konfiguration gespeichert wird.

5. Starten Sie SiteScope.

Aktivieren oder Deaktivieren des FIPS-konformen Modus nach dem Ändern des Verschlüsselungsschlüssels

Wenn Sie den FIPS 140-2-konformen Modus aktivieren oder deaktivieren möchten, nachdem Sie den SiteScope-Serverschlüssel für das Verschlüsseln von Daten geändert haben, müssen Sie Folgendes durchführen:

Hinweis: Wenn diese Schritte nicht in der unten aufgeführten Reihenfolge durchgeführt werden, kann es bei SiteScope zu Datenverlust kommen.

1. Deaktivieren Sie die Schlüsselverwaltung für die Datenverschlüsselung (siehe Schritt 4 unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 209 und geben Sie eine `2` ein, um die Standardverschlüsselung wiederherzustellen).

2. Aktivieren/deaktivieren Sie den FIPS 140-2-konformen Modus. Weitere Informationen finden Sie unter "Aktivieren des FIPS 140-2-konformen Modus" auf Seite 198.

3. Deaktivieren Sie die Schlüsselverwaltung für die Datenverschlüsselung (Fortsetzung von Schritt 4 unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 209 und geben Sie eine `1` ein, um die persistente Daten mit einem benutzerdefinierten Schlüssel zu verschlüsseln).

Exportieren und Importieren von Konfigurationsdaten beim Verwenden eines benutzerdefinierten Schlüssels für die Datenverschlüsselung

Wenn SiteScope für die Verwendung der Schlüsselverwaltung für die Datenverschlüsselung konfiguriert wird, geben Sie eine Passphrase ein, die SiteScope für die Generierung eines neuen Schlüssels verwendet. SiteScope verwendet diesen Schlüssel für die Verschlüsselung von persistenten Daten. Wenn Sie diese verschlüsselten Daten später in SiteScope exportieren oder importieren, müssen Sie dieselbe Passphrase für den SiteScope-Serverschlüssel verwenden.

1. Exportieren Sie die SiteScope-Konfigurationsdaten aus der aktuellen SiteScope-Instanz für einen späteren Import in SiteScope.

   - Bei Verwendung des SiteScope-Konfigurationswerkzeugs:

     i. Geben Sie im Bildschirm **Konfiguration exportieren** die Passphrase ein, die für den SiteScope-Server-KeyStore im Feld **Passphrase** verwendet wurde. Dieses Feld ist deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

     ii. Klicken Sie auf **Weiter**, um den Export abzuschließen. Die Konfigurationsdaten werden mithilfe des benutzerdefinierten Schlüssels verschlüsselt und exportiert.

     Hinweis: Diese Eingabefelder sind deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

   - Bei Verwendung des Konfigurationswerkzeugs im Konsolenmodus: Geben Sie im Bildschirm **Konfiguration exportieren** die Passphrase nach Aufforderung ein, die für den SiteScope-Server-KeyStore verwendet wurde, und drücken Sie die EINGABETASTE, um die Exportoperation abzuschließen.

   - Unter Verwendung des unbeaufsichtigten Modus: Geben Sie die Passphrase der Datenverschlüsselung der Schlüsselverwaltung in den entsprechenden Abschnitt der Datei **ovinstallparams.ini** ein.

2. Importieren Sie SiteScope-Konfigurationsdaten.

   - Benutzeroberfläche (während der Installation im SiteScope-Konfigurationsassistenten oder nach der Installation im SiteScope-Konfigurationswerkzeug):

i. Geben Sie im Bildschirm **Konfiguration importieren** den Namen der zu importierenden Benutzerdatendatei (ZIP) ein oder geben Sie das SiteScope-Installationsverzeichnis an, aus dem die Benutzerdatendatei importiert werden soll.

ii. Geben Sie im Feld **Passphrase** die Passphrase ein, die für den KeyStore des SiteScope-Servers verwendet werden soll. Bestätigen Sie die Passphrase, indem Sie dieselbe Passphrase in das Feld **Übereinstimmung mit Passphrase** eingeben.

> **Hinweis:** Diese Felder sind deaktiviert, wenn die SiteScope-Standardverschlüsselung verwendet wird.

iii. Klicken Sie auf **Weiter**, um den Import abzuschließen.

- Konsolenmodus (während der Installation oder nach der Installation mit dem Konfigurationswerkzeug): Geben Sie im Bildschirm **Konfiguration importieren** die Passphrase nach Aufforderung ein, die für den SiteScope-Serverschlüssel verwendet wurde, und drücken Sie die EINGABETASTE, um die Importoperation abzuschließen.
- Unbeaufsichtigte Installation: Geben Sie die Passphrase für den benutzerdefinierten Schlüssel ein, der für die Datenverschlüsselung verwendet wurde, in den entsprechenden Abschnitt der Datei **ovinstallparams.ini** ein.

Die importierten Konfigurationsdaten werden mithilfe des benutzerdefinierten Schlüssels verschlüsselt.

Kapitel 22: Konfigurieren von SiteScope für die Kommunikation mit BSM über eine sichere Verbindung

Dieses Kapitel umfasst die folgenden Themen:

Konfigurieren von SiteScope für die Verbindung mit einem BSM-Server, der eine sichere Verbindung erfordert

Damit SiteScope mit einem BSM-Server kommunizieren kann, der eine sichere Verbindung erfordert, müssen Sie zunächst eine Vertrauensstellung zwischen SiteScope und BSM konfigurieren. Dies bedeutet, dass SiteScope der Zertifizierungsstelle, die das BSM-Serverzertifikat ausgegeben hat, vertrauen muss. Damit SiteScope einer Zertifizierungsstelle vertrauen kann, muss das Zertifikat der Zertifizierungsstelle auf dem SiteScope-Server und in den Haupt-TrustStores gespeichert werden. Weitere Informationen finden Sie unter "Importieren von Zertifikaten der Zertifizierungsstelle in TrustStores von SiteScope" auf Seite 193.

Konfigurieren von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert

Sie können SiteScope für Verbindungen mit einem BSM-Server konfigurieren, der ein Clientzertifikat benötigt. Hierbei muss das BSM-Serverzertifikat in einen SiteScope-Keystore importiert werden.

Verwenden Sie hierfür das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit). Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zur Konfiguration von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert" auf Seite 224.

Sie können diesen Vorgang (siehe "Konfigurieren von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert" auf Seite 278) auch manuell ausführen.

Konfigurieren von BSM für Verbindungen mit SiteScope, wenn SiteScope ein Clientzertifikat benötigt

Führen Sie in BSM die folgenden Konfigurationsschritte sowohl auf dem Gateway- und dem Datenverarbeitungsserver aus:

1. Kopieren Sie die Datei **<SiteScope-Stammverzeichnis>\templates.certificates\BSMClientKeystore** auf dem SiteScope-Computer an einen beliebigen Speicherort auf dem BSM-Computer.

2. Beenden Sie BSM.

3. Fügen Sie folgende Zeile zur Datei **<HP BSM-Stammverzeichnis>\EjbContainer\bin\product_run.bat** hinzu:

   ```
   set SECURITY_OPTS=-Djavax.net.ssl.keyStore=FULL_PATH_TO_COPIED_
   BSMClientKeyStore_File -Djavax.net.ssl.keyStorePassword=PASSWORD_FOR_
   BSMClientKeyStore_File -Djavax.net.ssl.keyStoreType=JKS

   set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
   ```

   wobei `FULL_PATH_TO_COPIED_BSMClientKeyStore_File` ein Keystore-Pfad und `PASSWORD_FOR_BSMClientKeyStore_File` das Keystore-Kennwort ist.

4. Starten Sie BSM neu.

5. Konfigurieren Sie BSM und SiteScope in System Availability Management (SAM) Administration.

6. Geben Sie unter **SAM Administration > New/Edit SiteScope > Distributed Settings** für die Eigenschaft **Gateway Server name/IP address** den vollqualifizierten Domänennamen (FQDN) des sicheren Reverse-Proxys ein.

Kapitel 23: Verwenden des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)

Das Hardening-Tool ist ein Befehlszeilen-Tool, mit dem Sie SiteScope so konfigurieren können, dass eine teilweise oder vollständige Sicherheitsoptimierung ausgeführt wird.

Hinweis: Jedes Mal, wenn Sie das Tool ausführen, wird ein vollständige Sicherung der vorhandenen SiteScope-Konfiguration erstellt, die jederzeit wiederhergestellt werden kann. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools für das Wiederherstellen einer gesicherten Konfiguration" auf Seite 229.

Mit dem Hardening-Tool können Sie die folgenden Aufgaben erledigen:

Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)

In diesem Thema wird beschrieben, wie das Hardening-Tool geöffnet und ausgeführt wird. Damit die anderen in den Themen dieses Kapitels beschriebenen Aufgaben ausgeführt werden können, müssen Sie zunächst die Schritte in diesem Thema ausführen.

1. Wenn Sie die LDAP-Benutzerauthentifizierung aktivieren möchten (erforderlich für die Anmeldung an SiteScope nur mit Clientzertifikaten), konfigurieren Sie die LDAP-Integration, bevor Sie das Tool ausführen:

   a. Konfigurieren Sie den LDAP-Server in SiteScope. Weitere Informationen finden Sie unter "Einrichten von SiteScope zur Verwendung der LDAP-Authentifizierung" im Handbuch Verwenden von SiteScope in der SiteScope-Hilfe.

   b. Erstellen Sie eine neue Rolle in der SiteScope-Benutzerverwaltung für LDAP-Benutzer.

   c. Ändern Sie den SiteScope-Anmeldenamen des Administrators in die E-Mail-Adresse eines LDAP-Benutzers. Geben Sie kein Kennwort ein.

2. Halten Sie den SiteScope-Dienst an:

   Windows:

   - Wenn Sie SiteScope über **go.bat** ausführen, schließen Sie das Befehlszeilenterminal oder drücken Sie **STRG+C**.
   - Wenn Sie SiteScope als Dienst ausführen:

     i. Suchen Sie im Windows-Explorer nach **Dienste**. Das Fenster mit den Komponentendiensten wird geöffnet.

     ii. Wählen Sie im linken Bereich **Dienste (Lokal)** aus.

     iii. Wählen Sie aus der Liste der Dienste im mittleren Bereich **HP SiteScope** aus.

     iv. Klicken Sie im linken Bereich der Dienstliste auf **Dienst beenden**.

   Linux:

Führen Sie den folgenden Befehl über die Befehlszeile aus:

```
cd /opt/HP/SiteScope/
./stop
```

> **Achtung:** Führen Sie das Hardening-Tool nicht aus, während SiteScope ausgeführt wird.

3. Starten Sie das Tool, indem Sie folgenden Befehl über die Befehlszeile ausführen:

   Windows:

   ```
   <SiteScope_
   Stammverzeichnis>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
   ```

   Linux:

   ```
   ./opt/HP/SiteScope/tools/SiteScopeHardeningTool/runSSLConfiguration.sh
   ```

   Das Hardening-Tool wird geöffnet.

4. Wenn Sie im Tool dazu aufgefordert werden, wählen Sie die Option **SiteScope hardening configuration** aus. Die bestehende SiteScope-Konfiguration wird automatisch gesichert.

5. Wenn Sie aufgefordert werden, geben Sie eine Sicherungsbeschreibung ein, mit der eine einfache Wiedererkennung gewährleistet ist, wenn die Sicherung später zur Wiederherstellung verwendet wird. Informationen zum Wiederherstellen einer gesicherten Konfiguration finden Sie unter "Verwenden des Hardening-Tools für das Wiederherstellen einer gesicherten Konfiguration" auf Seite 229.

   > **Hinweis:** Wenn Sie das Hardening-Tool verwenden, wird die Tomcat-Konfigurationsdatei **server.xml** im Verzeichnis **/opt/HP/SiteScope/Tomcat/conf** überschrieben und alle Änderungen, die an dieser Datei vor dem Ausführen des Tools durchgeführt wurden, werden entfernt. Zum Wiederherstellen dieser Änderungen müssen Sie diese erneut in der Datei durchführen, nachdem das Tool ausgeführt wurde.

6. Wählen Sie eine Aufgabe oder eine Kombination der Aufgaben aus dem Tool aus.

   Weitere Informationen zum Ausführen des Hardening-Tools zum Durchführen von Konfigurationsaufgaben finden Sie in den anderen Themen dieses Kapitels.

Hinweis: Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für sichere Verbindungen

Hinweis: Wenn Sie vorhaben, SiteScope im FIPS 140-2-konformen Modus auszuführen, befolgen Sie die Vorgehensweisen unter "Aktivieren des FIPS 140-2-konformen Modus" auf Seite 198.

Mit dem Hardening-Tool können Sie SiteScope so konfigurieren, dass das System eine sichere Verbindung (https) anfordert.

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.

2. Wenn Sie im Tool dazu aufgefordert werden, wählen Sie die Option **Configure SiteScope Standalone to work over SSL (https)** aus.

   Alternativ können Sie auch alle im Tool verfügbaren Konfigurationsvorgänge für die Sicherheitsoptimierung auf einmal ausführen. Wählen Sie hierzu die Option **Full SiteScope hardening configuration (all of the configuration options)** aus.

3. Bestätigen Sie, dass SiteScope für die Verwendung mit SSL konfiguriert werden soll.

4. Bestätigen Sie, dass SiteScope für den FIPS 140-2-konformen Modus konfiguriert werden soll. Weitere Informationen finden Sie unter "Aktivieren des FIPS 140-2-konformen Modus" auf Seite 198.

5. Wählen Sie eine der folgenden Methoden aus, um den SiteScope-Server-Keystore zu erstellen, der das SiteScope-Serverzertifikat aufnehmen soll:

   - **Importieren Sie einen Server-Keystore im .jks-Format.**

     Das Werkzeug fordert Sie auf, einen Alias auszuwählen, in dem sich der Schlüssel für die SiteScope SSL-Authentifizierung befindet.

> **Hinweis:** Wenn Sie den SiteScope- und den öffentlichen SiteScope-API-Client später für die Clientauthentifizierung konfigurieren (siehe "Konfigurieren von SiteScope für das Anfordern der Authentifizierung des Clientzertifikats" auf Seite 191), verwendet SiteScope diesen Alias für den Export des Schlüssels in den Client-TrustStore der SiteScope-API.

Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

- **Erstellen Sie einen Server-Keystore, indem Sie eine Anforderung auf einem zertifizierten Server der Zertifizierungsstelle signieren.**

  Wenn Sie diese Option auswählen, wird ein neuer Keystore und eine Schlüsselanforderung an eine Zertifizierungsstelle für ein signiertes Zertifikat erstellt. Das erstellte Zertifikat wird anschließend in den Keystore importiert.

  Das Werkzeug fordert Sie auf, die Parameter des Server-Keystores einzugeben. Wir empfehlen, für den allgemeinen Namen den URL einzugeben, der auf Ihrem Computer verwendet wird, (z. B. `ihrserver.domäne.com`). Für den Alias-Namen müssen Sie den Namen Ihres Computers angeben (z. B. `ihrserver`).

- **Importieren Sie einen Server-Keystore aus einem Serverzertifikat in das .pfx-Format.**

  Wenn Sie diese Option auswählen, wird ein Keystore aus einem Zertifikat im **.pfx**-Format erstellt. Dieses Zertifikat muss den privaten Schlüssel enthalten.

  Mit dem Hardening-Tool wird sichergestellt, dass das Keystore-Kennwort und der private Schlüssel immer identisch sind, wenn ein Keystore erstellt wird.

6. Geben Sie eine Benutzernameneigenschaft für das Clientzertifikat ein. Der Standardbenutzername ist `Other Name`.

   Das Serverzertifikat wird in den Server-Keystore importiert. Der Zertifikatalias wird im Tool angezeigt.

7. Bestätigen Sie, dass die SiteScope-Clientauthentifizierung aktiviert werden soll.

   Wenn Sie die TLS-Clientauthentifizierung aktivieren, führt SiteScope die vollständige TLS-Clientauthentifizierung beim TLS-Handshaking durch und extrahiert ein Clientzertifikat. Dieses Clientzertifikat wird anhand des Benutzerverwaltungssystem von SiteScope überprüft.

8. Bestätigen Sie, dass die Smartcard-Authentifizierung aktiviert werden soll.

Wenn Sie die Smartcard-Authentifizierung aktivieren, überprüft SiteScope, dass das Clientzertifikat von einem Hardwaregerät stammt. Weitere Informationen zur Smartcard-Authentifizierung finden Sie unter "Konfigurieren der Smartcard-Authentifizierung" auf Seite 189.

9. Geben Sie ein Kennwort für den TrustStore des SiteScope-Servers ein. Das Standardkennwort lautet `changeit`.

   Damit SiteScope einem Clientzertifikat vertrauen kann, muss SiteScope der Zertifizierungsstelle vertrauen, die das Clientzertifikat herausgegeben hat. Damit SiteScope einer Zertifizierungsstelle vertrauen kann, muss das Zertifikat der Zertifizierungsstelle auf dem SiteScope-Server und in den Haupt-TrustStores gespeichert werden. Informationen dazu, wie Sie Zertifikate der Zertifizierungsstelle in SiteScope-TrustStores importieren, finden Sie unter "Verwenden des Hardening-Tools zum Importieren von Zertifikaten der Zertifizierungsstelle in SiteScope-TrustStores" auf Seite 223.

10. Geben Sie `Q` ein, um das Verfahren für das Hardening-Tool abzuschließen.

Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für das Überprüfen der Zertifikatssperre

Mit dem Hardening-Tool können Sie SiteScope so konfigurieren, dass die Sperrung von Clientzertifikaten anhand der folgenden Methoden überprüft wird.

- **Zertifikatsperrliste (CRL)**

  Ermöglicht Ihnen, die Sperrung von Clientzertifikaten anhand einer Sperrliste (CRL) zu prüfen. Der URL für die CRL ist Teil der Client-Zertifikateigenschaften. Die Liste wird auf den lokalen Server heruntergeladen. Sie werden aufgefordert, eine Lebensdauer für die auf dem lokalen Server gespeicherte CRL einzugeben.

  In der folgenden Tabelle werden die Werte für die CRL-Lebensdauer erläutert.

CRL-Wert	Beschreibung
-1	Die CRL wird lokal gespeichert und nur bei Änderungen auf dem Server neu geladen. Dieser Wert empfiehlt sich, um die Leistung zu optimieren.

CRL-Wert	Beschreibung
0	Die CRL wird bei jeder angeforderten Überprüfung neu geladen.
≥1	Die CRL -Lebensdauer in Sekunden. Die CRL wird nach Ablauf dieses Intervalls neu geladen.

- **Online Certificate Status Protocol (OCSP)**

  Ermöglicht Ihnen, die Sperrung von Clientzertifikaten per Abfrage eines Remoteservers zu prüfen. SiteScope übermittelt die Seriennummer des Clientzertifikats an den Remoteserver und wartet auf eine Antwort. Die standardmäßige OCSP-Antwort-URL ist in den Client-Zertifikatseigenschaften festgelegt, Sie können diesen Wert jedoch ändern.

Sie können die Sperrung von Clientzertifikaten entweder per CRL oder per CRL und OCSP überprüfen.

So überprüfen Sie die Sperrung eines Clientzertifikats:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.

2. Wählen Sie die Option **Configure SiteScope SSL certificate revocation verification via CRL and OCSP** aus.

3. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

   Sie werden aufgefordert, den HTTP-Proxy für die Weiterleitung zu aktivieren.

   Bei aktiviertem HTTP-Proxy werden alle Anforderungen für Zertifikatssperrungen über den Proxyserver an CRL- und OCSP-URLs umgeleitet.

   Falls erforderlich, können Sie SiteScope auch für die Einhaltung von FIPS, Publication 140-2, (Federal Information Processing Standard) konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für den Betrieb im FIPS 140-2-konformen Modus" auf Seite 197.

   Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwenden des Hardening-Tools zum Importieren von Zertifikaten der Zertifizierungsstelle in SiteScope-TrustStores

Informationen dazu, wie Sie Zertifikate der Zertifizierungsstelle in SiteScope-TrustStores importieren finden Sie unter "Importieren von Zertifikaten der Zertifizierungsstelle in TrustStores von SiteScope" auf Seite 193.

So importieren Sie Zertifikate der Zertifizierungsstelle in SiteScope-TrustStores:

1. Voraussetzungen (wenn SiteScope für die Verwendung einer sicheren Verbindung konfiguriert wurde)

   Vor dem Import von Zertifikaten der Zertifizierungsstelle in SiteScope-TrustStores, müssen Sie SiteScope für die Verwendung von TLS konfigurieren, indem Sie ein SiteScope-Serverzertifikat in den Keystore auf dem SiteScope-Server importieren. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für sichere Verbindungen" auf Seite 219.

2. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.

3. Wenn Sie im Tool dazu aufgefordert werden, wählen Sie die Option **Import CA certificates into SiteScope main and server trustStores** aus.

4. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

Tipps:

- Das Werkzeug akzeptiert nur Dateipfade im regulären Windows-Format. Bei UNIX-Formaten, in denen einem Leerzeichen in einem Dateipfad ein umgekehrter Schrägstrich ("\") vorangestellt ist, der anzeigt, dass ein Leerzeichen folgt, müssen Sie den umgekehrten Schrägstrich

entfernen.

Format	Dateipfad
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** ändern Sie in: **/user/temp dir/certificate.cer**

- Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwenden des Hardening-Tools zur Konfiguration von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert

Sie können das Hardening-Tool verwenden, um die TLS-Authentifizierung für die BSM-Integration zu konfigurieren. Mit dem Tool können Sie SiteScope so konfigurieren, dass BSM mit SiteScope integriert werden kann. Außerdem können Sie mit ihm das SiteScope-Failover für TLS mit Clientzertifikatauthentifizierung konfigurieren. Nutzen Sie in beiden Fällen die im Folgenden beschriebene Vorgehensweise.

Hinweis: Bevor Sie die TLS-Clientauthentifizierung für die BSM-Integration konfigurieren, müssen Sie SiteScope für TLS konfigurieren. Importieren Sie hierzu ein SiteScope-Serverzertifikat in den Keystore auf dem SiteScope-Server. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools zum Konfigurieren von SiteScope für sichere Verbindungen" auf Seite 219.

Wenn Sie dies nicht bereits erledigt haben, werden Sie vom Hardening-Tool aufgefordert, eine vollständige SiteScope-Hardening-Konfiguration auszuführen.

So konfigurieren Sie die TLS-Clientauthentifizierung für die BSM-Integration:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 216.

2. Wählen Sie die Option **Configure SiteScope client certificate authentication for BSM Integration** aus.

3. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

   a. Wenn Sie dazu aufgefordert werden, den vollständigen Pfad im **.cer**-Format zum Zertifikat der Zertifizierungsstelle ein, die das BSM-Serverzertifikat ausgegeben hat. Das BSM-Serverzertifikat wird in den SiteScope-TrustStore importiert.

   b. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie dem BSM-Serverzertifikat vertrauen. Das BSM-Serverzertifikat wird in den Keystore importiert.

   c. Wenn Sie dazu aufgefordert werden, wählen Sie eine der folgenden Methoden aus, um den SiteScope-Server-Keystore zu erstellen, der das SiteScope-Serverzertifikat aufnehmen soll:

      - **Importieren Sie einen Server-Keystore im .jks-Format.**

        Das Werkzeug fordert Sie auf, einen Alias auszuwählen, in dem sich der Schlüssel für die SiteScope TLS-Authentifizierung befindet.

        Hinweis: Wenn Sie den SiteScope- und den öffentlichen SiteScope-API-Client später für die Clientauthentifizierung konfigurieren (siehe "Konfigurieren von SiteScope für das Anfordern der Authentifizierung des Clientzertifikats" auf Seite 191), verwendet SiteScope diesen Alias für den Export des Schlüssels in den Client-TrustStore der SiteScope-API.

      - **Erstellen Sie einen Server-Keystore, indem Sie eine Anforderung auf einem zertifizierten Server der Zertifizierungsstelle signieren.**

        Wenn Sie diese Option auswählen, wird ein neuer Keystore und eine Schlüsselanforderung an eine Zertifizierungsstelle für ein signiertes Zertifikat erstellt. Das erstellte Zertifikat wird anschließend in den Keystore importiert.

        Das Werkzeug fordert Sie auf, die Parameter des Server-Keystores einzugeben. Wir empfehlen, für den allgemeinen Namen den URL einzugeben, der auf Ihrem Computer verwendet wird, (z. B. `ihrserver.domäne.com`). Für den Alias-Namen müssen Sie den Namen Ihres Computers angeben (z. B. `ihrserver`).

      - **Importieren Sie einen Server-Keystore aus einem Serverzertifikat in das .pfx-Format.**

Wenn Sie diese Option auswählen, wird ein Keystore aus einem Zertifikat im **.pfx**-Format erstellt. Dieses Zertifikat muss den privaten Schlüssel enthalten.

Mit dem Hardening-Tool wird sichergestellt, dass das Keystore-Kennwort und der private Schlüssel immer identisch sind, wenn ein Keystore erstellt wird.

d. Geben Sie das Kennwort für den Client-Keystore ein, das zur Authentifizierung von BSM verwendet wird, wenn Sie dazu aufgefordert werden. SiteScope erstellt den Keystore für das BSM-Clientzertifikat.

e. Geben Sie das Kennwort für den Discovery-Agenten **TrustStore MAMTrustStoreExp.jks** ein, wenn Sie dazu aufgefordert werden. Das Standardkennwort lautet `logomania`. Es wird dringend empfohlen, das Standardkennwort nicht zu ändern.

Währen des Konfigurationsvorgangs importiert SiteScope das BSM-Serverzertifikat automatisch in den SiteScope-TrustStore.

f. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie dem BSM-Serverzertifikat vertrauen.

Das BSM-Serverzertifikat wird in den SiteScope-Keystore importiert.

Tipps:

- Das Werkzeug akzeptiert nur Dateipfade im regulären Windows-Format. Bei UNIX-Formaten, in denen einem Leerzeichen in einem Dateipfad ein umgekehrter Schrägstrich ("\") vorangestellt ist, der anzeigt, dass ein Leerzeichen folgt, müssen Sie den umgekehrten Schrägstrich entfernen.

Format	Dateipfad
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** ändern Sie in: **/user/temp dir/certificate.cer**

- Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwendung des Hardening-Tools zur Aktivierung des FIPS 140-2-konformen Modus

Mit dem Hardening-Tool können Sie SiteScope so konfigurieren, dass das System dem FIPS 140-2-Standard entspricht. FIPS 140-2 ist ein vom National Institute of Standards and Technology (NIST) durchgeführtes Programm zur Prüfung kryptografischer Module, das die Sicherheitsanforderungen für kryptografische Module festlegt.

Weitere Informationen finden Sie unter "Aktivieren des FIPS 140-2-konformen Modus" auf Seite 198.

Verwendung des Hardening-Tools zur Aktivierung der Schlüsselverwaltung für die Datenverschlüsselung

Mit der Schlüsselverwaltung im Hardening-Tool können Sie den kryptografischen Schlüssel ändern, der in SiteScope zur Verschlüsselung von Persistenzdaten verwendet wird. Dies ermöglicht eine stärkere Verschlüsselung, als sie die in SiteScope eingesetzte Standardmethode bietet.

Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für die Verwendung eines benutzerdefinierten Schlüssels für die Datenverschlüsselung" auf Seite 209.

Verwenden des Hardening-Tools für das Konfigurieren von SiteScope und der Clientzertifikatauthentifizierung von öffentlichen SiteScope-APIs

Mit dem Hardening-Tool können Sie SiteScope und den öffentlichen SiteScope-API-Client folgendermaßen für die Clientauthentifizierung konfigurieren:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.

2. Wählen Sie die Option **Configure SiteScope and SiteScope public API client for client certificate authentication** aus.

3. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

Tipps:

- Wenn Sie die LDAP-Benutzerauthentifizierung für öffentliche SiteScope-APIs aktivieren, dann wird der aus dem API-Clientzertifikat extrahierte Benutzername durch den LDAP-Server authentifiziert.
- Wenn Sie aufgefordert werden, eine Zertifizierungsstelle für das Clientzertifikat zum TrustStore des SiteScope-Server hinzuzufügen, wird das Zertifikat in den TrustStore des SiteScope-Servers und den Haupt-TrustStore importiert. Die erstellten API-Konfigurationsdateien werden unterhalb des Skriptverzeichnisses im Ordner **API_Configuration** abgelegt.
- Das Werkzeug akzeptiert nur Dateipfade im regulären Windows-Format. Bei UNIX-Formaten, in denen einem Leerzeichen in einem Dateipfad ein umgekehrter Schrägstrich ("\") vorangestellt ist, der anzeigt, dass ein Leerzeichen folgt, müssen Sie den umgekehrten Schrägstrich entfernen.

Format	Dateipfad
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** ändern Sie in: **/user/temp dir/certificate.cer**

- Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwenden des Hardening-Tools zur Konfiguration des JMX-Remote-Zugriffs

Gehen Sie folgendermaßen vor, um mit dem Hardening-den JMX-Remotezugriff auf den SiteScope-Server zu aktivieren bzw. zu deaktivieren:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.

2. Wählen Sie die Option zum Konfigurieren des JMX-Remotezugriffs aus.
3. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

> **Tipp:** Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Verwenden des Hardening-Tools für das Wiederherstellen einer gesicherten Konfiguration

Wenn Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) ausführen, wird die bestehende SiteScope-Konfiguration automatisch gesichert. Sie können das Hardening-Tools für das Wiederherstellen einer gesicherten Konfiguration verwenden:

1. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus. Weitere Informationen finden Sie unter "Ausführen des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 217.
2. Wählen Sie die Option **Restore SiteScope configuration from backup** aus.
3. Folgen Sie den Anweisungen, die im Werkzeug zur Verfügung gestellt werden.

> **Tipps:**
>
> - Sicherungsnamen enthalten Uhrzeit und Datum der Sicherung.
> - Änderungen an der Konfiguration werden erst nach Beenden des Hardening-Tools wirksam.

Einschränkungen und Fehlerbehebungen für das Hardening-Tool

In diesem Abschnitt werden die Fehlerbehebung und die Einschränkungen bei der Arbeit mit dem Hardening-Tool beschrieben.

Einschränkungen

Wenn SiteScope auf einem nichtenglischen Betriebssystem installiert wird, können Sie das Hardening-Tool nicht für die Konfiguration von SiteScope für die Verwendung von TLS verwenden. In diesem Fall verwenden Sie das manuelle Verfahren, das im Handbuch zur Bereitstellung von HP SiteScope im Anhang beschrieben wird.

Fehlerbehebung

- **Im Hardening-Tool werden Dateipfade im UNIX-Format nicht akzeptiert.**

  Ursache: Das Tool akzeptiert nur Dateipfade im regulären Windows-Format.

  Lösung: Bei UNIX-Formaten, in denen einem Leerzeichen in einem Dateipfad ein umgekehrter Schrägstrich ("\") vorangestellt ist, der anzeigt, dass ein Leerzeichen folgt, müssen Sie den umgekehrten Schrägstrich entfernen.

Format	Dateipfad
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** ändern Sie in: **/user/temp dir/certificate.cer**

- **Beim Beenden des Tools wird in einer Fehlermeldung darauf hingewiesen, dass es ein Problem beim Kopieren in eine Datei gab.**

  Ursache: Dieser Fehler tritt auf, wenn das Konfigurationswerkzeug eine der erstellten Konfigurationsdateien nicht finden kann. Der Grund ist, dass das Werkzeug nicht über die Befehlszeile ausgeführt wurde. In diesem Fall werden die erstellten Dateien nicht im Verzeichnis des Konfigurationswerkzeugs abgelegt.

  Lösung:

  a. Löschen Sie im Verzeichnis des Konfigurationswerkzeugs alle erstellten Bibliotheken (z. B. **API_Configuration**, **tmp_<Zahl>**, **BSM_Int**).

  b. Öffnen Sie ein Befehlszeilenterminal.

c. Wechseln Sie über die Befehlszeile in das Verzeichnis des Konfigurationswerkzeugs.

d. Führen Sie das Konfigurationswerkzeug über die Befehlszeile aus: Weitere Informationen finden Sie unter "Verwenden des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 216.

- **Nach dem Konfigurieren der SiteScope-Authentifizierung bietet SiteScope keine Option für ein Authentifizierungszertifikat, wenn auf SiteScope über einen Webbrowser zugegriffen wird, und die Anmeldung schlägt fehl.**

  Ursache: SiteScope-TrustStores enthalten keine Zertifikate der Zertifizierungsstellen (CA-Zertifikate). Auf diese Weise fordert SiteScope keine Clientzertifikate an, die von diesen Zertifizierungsstellen signiert wurden.

  Lösung: Importieren Sie CA-Zertifikate in die Haupt- und Server-TrustStores von SiteScope und fügen sie die benötigten CA-Zertifikate hinzu. Weitere Informationen finden Sie unter "Importieren von Zertifikaten der Zertifizierungsstelle in TrustStores von SiteScope" auf Seite 193.

- **Der Aufruf der öffentlichen SiteScope-API wird mit der Ausnahme `NumberFormatException` beendet**

  Ursache: Der API-Aufruf wurde ausgeführt, wobei der Parameter `–useSSL` auf `false` festgelegt wurde.

  Lösung: Führen Sie den API-Aufruf aus und legen Sie den Parameter `–useSSL` auf `true` fest.

- **Der Aufruf der öffentlichen SiteScope-API wird mit der Ausnahme `ConnectException: Connection refused` beendet.**

  Ursache: Der API-Aufruf versucht, eine Verbindung mit einem Port herzustellen, der kein TLS-Port ist.

  Lösung: Legen Sie den Parameter `–port` auf den Port 8443 der TLS-Authentifizierung fest.

- **Der Aufruf der öffentlichen SiteScope-API schlägt mit `(500) Internal Server Error` fehl.**

  Ursache: Der Parameter `–login` wurde nicht auf den richtigen TLS-Benutzernamen festgelegt.

  Lösung: Legen Sie den Parameter `–login` auf `SITESCOPE_CERTIFICATE_AUTHENTICATED_USER` fest.

- **SiteScope zeigt die folgende Meldung an, wenn Sie versuchen, über einen Browser auf SiteScope zuzugreifen: "Der Benutzer ist kein gültiger SiteScope-Benutzer. Bitte wenden Sie sich an den SiteScope-Administrator."**

  Ursache: Die Client-TLS-Authentifizierung und die Smartcard-Authentifizierung werden aktiviert, während SiteScope für die TLS-Authentifizierung konfiguriert wird, der LDAP-Server wird jedoch nicht in der SiteScope-Benutzerverwaltung festgelegt.

  Lösung 1:

  a. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) aus.

  > **Hinweis:** Wenn Sie sich nur mit Clientzertifikaten bei SiteScope anmelden möchten, müssen Sie zunächst den LDAP-Server in SiteScope konfigurieren, bevor Sie die Verfahren zum Optimieren der Sicherheit durchführen. Nach dem Optimieren der Sicherheit für SiteScope, wird der für die Anmeldung verwendete Benutzername aus dem Clientzertifikat extrahiert und mit dem LADP-Server verglichen. Die folgenden Eigenschaften werden zur Datei **<SiteScope-Stammverzeichnis>\groups\master.config** hinzugefügt (diese Eigenschaften sollten nicht geändert werden):
  >
  > - **_clientCertificateAuthIdentityPropertyName**. Gibt SiteScope darüber Auskunft, wo der Benutzername, der für die Verbindung verwendet wurde, in den Eigenschaften des Clientzertifikats gefunden wird.
  > - **_clientCertificateAuthIsAPIRealLDAPUserRequired**. Weist SiteScope darauf hin, dass die Authentifizierung des Benutzernamens über LDAP durchgeführt wird, wenn SiteScope-APIs aufgerufen werden.
  > - **_clientCertificateAuthUsernamePropertyNameInSubjectField**. Die Eigenschaft, unter der der Benutzername im Clientzertifikat, das für den API-Aufruf verwendet wird, gefunden werden kann.

  b. Stellen Sie die SiteScope-Konfiguration wieder her, die vor dem Ausführen des Werkzeugs gesichert wurde (Informationen hierzu finden Sie unter "Wiederherstellen einer gesicherten Konfiguration" auf Seite 194).

  c. Konfigurieren Sie den LDAP-Server.

  d. Führen Sie das Hardening-Tool (Werkzeug zum Optimieren der Sicherheit) erneut aus.

  Lösung 2:

a. Öffnen Sie die Datei **master.config** unter **<SiteScope-Stammverzeichnis>\groups** und ändern Sie den Wert der folgenden Eigenschaften in **false**:
   - _clientCertificateAuthEnabled
   - _clientCertificateAuthIsAPIRealLDAPUserRequired
   - _clientCertificateAuthSmartCardEnforcementEnabled

b. Starten Sie SiteScope neu.

c. Konfigurieren Sie den LDAP-Server.

d. Öffnen Sie die Datei **master.config**.

e. Legen Sie für die oben aufgeführten Eigenschaften wieder die ursprünglichen Werte fest.

f. Starten Sie SiteScope neu.

Kapitel 24: Konfiguration des USGCB (FDCC)-konformen Desktops

Bei USGCB (United States Government Configuration Baseline), früher als FDCC (Federal Desktop Core Configuration) bekannt, handelt es sich um einen Standard der Desktopkonfiguration, der Unterstützung bei der Verbesserung und Verwaltung von effektiven Konfigurationseinstellungen bietet, die primär Sicherheitsaspekte betreffen.

SiteScope ist mit USGCB (FDCC)-konformen Clients zertifiziert. Zum Aktivieren der Konformität müssen Sie die SiteScope-URL in die Sicherheitszone der vertrauenswürdigen Sites und zur Liste zugelassener Popups hinzufügen. Es wird auch empfohlen, Dateidownloads zuzulassen.

Weitere Informationen zu USGCB (FDCC) finden Sie unter:

- http://usgcb.nist.gov/usgcb/microsoft_content.html
- http://nvd.nist.gov/fdcc/index.cfm

Voraussetzungen:

Installieren Sie die aktuelle JRE-Version, die von SiteScope wie unter "Clientsystemanforderungen" auf Seite 78 aufgelistet unterstützt wird.

Aktivieren des Gruppenrichtlinien-Editors (gpedit.msc) in Windows 7:

1. Fügen Sie den SiteScope-URL zur Sicherheitszone der vertrauenswürdigen Sites hinzu:

    a. Öffnen Sie den Gruppenrichtlinien-Editor, indem Sie den folgenden Befehl ausführen: `run gpedit.msc`.

    b. Navigieren Sie zu: **Computerkonfiguration** > **Administrative Vorlagen** > **Windows-Komponenten** > **Internet Explorer** > **Internetsystemsteuerung** > **Sicherheitsseite**:

        i. Doppelklicken Sie im rechten Abschnitt mit den Einstellungen auf **Liste der Site zu Zonenzuweisungen**, wählen Sie die Option **Aktiviert** aus und klicken Sie auf **Anzeigen**. Klicken Sie im Dialogfeld **Inhalt anzeigen** auf **Hinzufügen**.

        ii. Geben Sie im Feld für den Namen des hinzuzufügenden Elements den Namen des SiteScope-Servers ein. Beispiel: `http://MySiteScope.com`. Wenn Sie SiteScope über HTTPS verwenden, geben Sie `https://MySiteScope.com` ein.

iii. Geben Sie im Feld für den Namen des hinzuzufügenden Elements die Zahl für den Zonentyp ein:

Wert	Zonentyp	Beschreibung
1	Intranetzone	Sites in Ihrem lokalen Netzwerk
2	Zone vertrauenswürdiger Sites	Sites, die zu den vertrauenswürdigen Sites hinzugefügt wurden
3	Internetzone	Sites aus dem Internet
4	Zone für eingeschränkte Sites	Sites, die speziell zu den eingeschränkten Sites hinzugefügt wurden

2. Fügen Sie den SiteScope-URL zur Liste zugelassener Popups hinzu.

   a. Öffnen Sie den Gruppenrichtlinien-Editor, indem Sie den folgenden Befehl ausführen: `run gpedit.msc`.

   b. Navigieren Sie zu: **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer** :

      i. Doppelklicken Sie im rechten Abschnitt mit den Einstellungen auf **Liste zugelassener Popups**, wählen Sie die Option **Aktiviert** aus und klicken Sie auf **Anzeigen**. Klicken Sie im Dialogfeld **Inhalt anzeigen** auf **Hinzufügen**.

      ii. Geben Sie im Feld für den Namen des hinzuzufügenden Elements den Namen des SiteScope-Servers ein. Beispiel: `http://MySiteScope.com`. Wenn Sie SiteScope über HTTPS verwenden, geben Sie `https://MySiteScope.com` ein.

3. Lassen Sie Dateidownloads zu (optional, verwendet für Protokollabruf und Versionshinweise).

   a. Öffnen Sie den Gruppenrichtlinien-Editor, indem Sie den folgenden Befehl ausführen: `run gpedit.msc`.

   b. Navigieren Sie zu: **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Internet Explorer > Sicherheitsfunktionen > Dateidownload einschränken** und doppelklicken Sie im rechten Abschnitt mit den Einstellungen auf **Internet Explorer-Prozess** und wählen Sie die Option **Deaktiviert** aus.

Teil 5: Erste Schritte und Zugriff auf SiteScope

Kapitel 25: Verwaltung nach der Installation

In diesem Kapitel werden Schritte empfohlen, die Sie im Anschluss an die Installation von SiteScope durchführen sollten.

✓	**Schritt**
	Registrieren Sie sich, um Unterstützung zu SiteScope zu erhalten. Weitere Informationen finden Sie unter "Roadmap für die ersten Schritte" auf Seite 43.
	Zum Verbessern der SiteScope-Skalierbarkeit und Leistung, wird empfohlen, Microsoft-Hotfixes zu installieren. Weitere Informationen finden Sie unter "Installieren von Microsoft-Hotfixes" auf Seite 240.
	Wenn Sie von einer früheren SiteScope-Version aktualisieren, verwenden Sie das Konfigurationswerkzeug, um Monitor- und Gruppenkonfigurationsdaten aus der älteren SiteScope-Installation in die neue Installation zu übertragen. Weitere Informationen zur Verwendung des Konfigurationswerkzeugs finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151.
	Melden Sie sich mit einem Webbrowser an der Weboberfläche von SiteScope an. Weitere Informationen finden Sie unter "Verbinden mit SiteScope" auf Seite 244.
	Neue Installationen werden standardmäßig mit der Community-Lizenz aktiviert. Hierdurch kann SiteScope mit eingeschränktem Funktionsumfang zeitlich unbegrenzt genutzt werden. Wenn Sie Ihre SiteScope-Edition auf eine SiteScope-Edition mit vollem Funktionsumfang aktualisieren, können Sie Ihre SiteScope-Lizenzinformationen während oder nach der Installation auf der Seite **Allgemeine Voreinstellungen** eingeben. Eine Anleitung hierzu finden Sie in der SiteScope-Hilfe unter "Verwenden von SiteScope" im Abschnitt "Allgemeine Voreinstellungen". Details zu Lizenzen finden Sie unter "SiteScope-Lizenzen" auf Seite 29.
	Erstellen Sie einen Benutzernamen und ein Kennwort für das SiteScope-Administratorkonto. Dies ist das Standardkonto, das bei der Installation des Produkts aktiv ist. Es verfügt über umfassende Berechtigungen für die Verwaltung von SiteScope und wird von allen Benutzern verwendet, die auf das Produkt zugreifen, sofern Sie keine Einschränkungen für das Konto festlegen. Erstellen und konfigurieren Sie je nach den Anforderungen des Unternehmens andere Benutzerkonten. Details finden Sie im Abschnitt "Voreinstellungen für Benutzerverwaltung" unter "Verwenden von SiteScope" in der SiteScope-Hilfe. Falls für den Administratorbenutzer kein Benutzername und kein Kennwort festgelegt ist, überspringt SiteScope die Anmeldungsseite und meldet sich automatisch an.

✓	Schritt
	Konfigurieren Sie die E-Mail-Servereinstellungen von SiteScope mit der E-Mail-Adresse eines Administrators und legen Sie einen E-Mail-Server fest, den SiteScope zum Weiterleiten von E-Mail-Nachrichten und Warnungen an Benutzer verwenden kann. Details finden Sie im Abschnitt "E-Mail-Voreinstellungen" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
	Konfigurieren Sie Verbindungsprofile für die Remoteserver, die Sie überwachen möchten. Geben Sie die Verbindungsmethode an, die in Abstimmung mit Ihren Sicherheitsanforderungen verwendet werden soll. Details finden Sie im Abschnitt "Remoteserver" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
	Passen Sie ggf. die Protokolleinstellungen an, um festzulegen, wie viele Tage Monitordaten auf dem SiteScope-Server aufbewahrt werden. Standardmäßig löscht SiteScope Protokolle, die älter sind als 40 Tage. Wenn Sie Monitordaten in eine externe Datenbank exportieren wollen, bereiten Sie die Datenbank und die erforderlichen Treiber vor und konfigurieren Sie die Protokolleinstellungen nach Bedarf. Details finden Sie im Abschnitt "Protokollvoreinstellungen" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
	Installieren Sie Middleware-Treiber für Verbindungen mit Remotedatenbanken und Applikationen für die Monitore, die Treiber erfordern.
	Wenn Sie SiteScope zur Datenerfassung für Business Service Management (BSM) verwenden, konfigurieren Sie die BSM-Integration. Details finden Sie im Abschnitt "Arbeiten mit BSM" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
	Wenn Sie SiteScope verwenden, um Ereignisse zu senden oder Metriken für die Verwendung in HP Operations Manager (HPOM) oder in der Operationenverwaltung in BSM zu melden, konfigurieren Sie die HP Operations Manager-Integration. Weitere Informationen finden Sie unter "Integration von SiteScope mit HP Operations Manager-Produkten" auf der HP-Website für die Softwareintegration. • Für HPOM für Windows siehe http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39 • Für HPOM für UNIX siehe http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628
	Entwerfen Sie eine Gruppen- und Monitororganisation auf der Grundlage der Anforderungen und Beschränkungen, die Sie in Ihrer Bewertung der Unternehmenssysteminfrastruktur identifiziert haben.

✓	Schritt
	Erstellen und entwickeln Sie Vorlagen, um die Überwachungsbereitstellung mithilfe standardisierter Gruppenstrukturen, Benennungskonventionen und Konfigurationseinstellungen zu beschleunigen. Details finden Sie in den Abschnitten zu benutzerdefinierten Vorlagen und Lösungsvorlagen unter "Verwenden von SiteScope in der SiteScope-Hilfe.
	Erstellen Sie Abhängigkeiten zwischen Gruppen und wichtigen Monitoren, um redundante Warnungen einzudämmen. Details finden Sie im Abschnitt "Arbeiten mit SiteScope-Gruppen" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
	Stellen Sie SiteScope Systemadministratoren und Unternehmensbeteiligten zur Verfügung.

Nachdem das SiteScope-System mit definierten Benutzern und eingehenden Monitordaten eingerichtet wurde, können Sie damit beginnen, Unternehmens- und Systembenutzern den Zugriff auf sowie die Verwendung von SiteScope-Funktionen für die Report-Erstellung und für Warnungen zu erläutern.

Kapitel 26: Installieren von Microsoft-Hotfixes

Zum Verbessern der SiteScope-Skalierbarkeit und Leistung, wird empfohlen, die folgenden Microsoft-Hotfixes nach der Installation von SiteScope zu installieren.

Hotfix-Download	Beschreibung
http://support.microsoft.com/kb/2847018 http://support.microsoft.com/kb/2775511	Installieren Sie die aktuellen Microsoft-Patchdateien mrxsmb.sys und mrxsmb10.sys oder mrxsmb20.sys auf dem SiteScope-Server, um Leistungsprobleme und Überwachungsaussetzer zu vermeiden, wenn Sie mehrere Perfex-basierte Monitore für denselben Host ausführen.
http://support.microsoft.com/?scid=kb;en-us;942589	Installieren Sie das Microsoft-Hotfix für die Verwendung des Microsoft Exchange-Monitors auf einer 64-Bit-Version von Windows 2003, Windows 2008 oder Windows XP (eine 32-Bit-Applikation kann nicht auf den system32-Ordner eines Computers zugreifen, der unter der 64-Bit-Version von Windows Server 2003 oder 2008 ausgeführt wird).
http://support.microsoft.com/kb/961435	Installieren Sie das Microsoft-Hotfix auf dem Windows-Zielsystem, um die Überwachung von Microsoft Windows Server 2008 mit WMI zu aktivieren.

Darüber hinaus wird empfohlen, die Schritte aus den Artikeln der Microsoft Knowledge Base weiter unten auszuführen, um Probleme mit Berechtigungen und fehlenden oder beschädigten Indikatorwerten zu vermeiden.

Artikel der Microsoft Knowledge Base	Problem/Beschreibung
http://support.microsoft.com/kb/300702/en-us http://support.microsoft.com/kb/164018/en-us	**Verbindung zum Server kann nicht hergestellt werden**: Das Überwachen von Leistungsobjekten auf Windows-Remoteservern erfordert spezielle Zugriffsberechtigungen für Benutzer wie in den Artikeln 300702 und 164018 der Microsoft Knowledge Base beschrieben.

Artikel der Microsoft Knowledge Base	Problem/Beschreibung
http://support.microsoft.com/kb/295292	**WMI-Berechtigungen**: Zum Konfigurieren des WMI-Dienstes für die Remoteüberwachung muss der auf dem WMI-Remoteserver eingegebene Benutzer über Berechtigungen verfügen, mit denen er Statistiken remote über den WMI-Namespace root\CIMV2 lesen kann.
http://support.microsoft.com/kb/300956/en-us	**Fehlende/beschädigte Werte der Leistungsindikatorbibliotheken**: Wenn die erforderlichen Werte der Leistungsindikatorbibliotheken fehlen oder beschädigt sind, befolgen Sie die Anweisungen im Microsoft Knowledge Base-Artikel KB300956, um sie manuell wieder aufzubauen.

Kapitel 27: Erste Schritte mit SiteScope

Dieses Kapitel umfasst die folgenden Themen:

Übersicht über das Starten des SiteScope-Services

Der SiteScope-Prozess wird bei der Installation auf allen Plattformen gestartet.

- Auf Windows-Plattformen wird SiteScope als Dienst hinzugefügt, der bei Neustart des Servers automatisch neu gestartet wird.
- Auf Linux-Plattformen müssen Sie den SiteScope-Prozess neu starten, sobald Sie den Server neu starten, auf dem SiteScope installiert ist.

Sie können den SiteScope-Prozess anhand der in diesem Abschnitt beschriebenen Schritte manuell starten und beenden.

Starten und Beenden des SiteScope-Dienstes auf Windows-Plattformen

SiteScope wird als Dienst auf Microsoft Windows-Plattformen installiert. Standardmäßig wird der SiteScope-Dienst automatisch neu gestartet, sobald der Server neu gestartet wird. Sie können den SiteScope-Dienst über die Option **Dienste** in der Systemsteuerung manuell starten und beenden.

So starten oder beenden Sie den SiteScope-Dienst über die Option "Dienste" in der Systemsteuerung:

1. Öffnen Sie die Option **Dienste** in der Systemsteuerung, indem Sie **Start > Einstellungen > Systemsteuerung > Verwaltung > Dienste** wählen.
2. Wählen Sie den Dienst **SiteScope** aus der Liste der Dienste aus und klicken Sie mit der rechten Maustaste, um das Menü **Aktion** anzuzeigen.
3. Wählen Sie den Befehl **Starten** bzw. **Beenden** aus dem Menü **Aktion** aus.

Netstart und Netstop (Befehle)

Sie können den SiteScope-Dienst auch mithilfe der Befehle **netstart** und **netstop** starten und beenden.

So starten Sie den SiteScope-Dienst mithilfe des Befehls "netstart":

1. Öffnen Sie auf dem Server, auf dem SiteScope installiert ist, ein Befehlseingabefenster.
2. Führen Sie mithilfe der folgenden Syntax das Dienstprogramm **netstart** aus:

   ```
   net start SiteScope
   ```

So beenden Sie den SiteScope-Dienst mithilfe des Befehls "netstop":

1. Öffnen Sie auf dem Server, auf dem SiteScope ausgeführt wird, ein Befehlseingabefenster.
2. Führen Sie mithilfe der folgenden Syntax das Dienstprogramm **netstop** aus:

   ```
   net stop SiteScope
   ```

Starten und Beenden des SiteScope-Prozesses auf Linux-Plattformen

SiteScope besitzt einen Autostart-Prozess, der SiteScope automatisch beim Systemstart startet und SiteScope beendet, wenn das System heruntergefahren wird. Beachten Sie, dass wenn Sie die Berechtigungen für ausführbare SiteScope-Dateien (Start, Stopp) ändern, die Berechtigungen auch in der Datei **/etc/init.d/sitescope** ändern müssen.

Sie können SiteScope auch mithilfe der im Lieferumgang enthaltenen Shellskripts manuell starten und beenden. Sie können SiteScope bei Neustart eines Servers automatisch neu starten, indem Sie ein **init.d**-Skript verwenden.

Hinweis: Obwohl SiteScope unter Linux über ein Root-Benutzerkonto installiert werden muss, ist

nach der Installation die Ausführung mit einem Nicht-Root-Benutzerkonto möglich. Weitere Informationen finden Sie unter "Konfigurieren eines Nicht-Root-Benutzerkontos mit Berechtigungen zum Ausführen von SiteScope" auf Seite 51.

So starten Sie den SiteScope-Prozess unter Linux manuell:

1. Öffnen Sie auf dem Server, auf dem SiteScope installiert ist, ein Terminalfenster.
2. Führen Sie mithilfe der folgenden Syntax das Skript **start command shell** aus.

   ```
   <Installationspfad>/SiteScope/start
   ```

   (Alternativ können Sie auf Linux/UNIX-Systemen den Befehl `service sitescope start` in einem beliebigen Verzeichnis ausführen.)

So beenden Sie den SiteScope-Prozess unter Linux:

1. Öffnen Sie auf dem Server, auf dem SiteScope ausgeführt wird, ein Terminalfenster.
2. Führen Sie mithilfe der folgenden Syntax das Skript **stop command shell** aus.

   ```
   <Installationspfad>/SiteScope/stop
   ```

   ```
   (Alternativ können Sie auf Linux/UNIX-Systemen den Befehl service sitescope
   stop in einem beliebigen Verzeichnis ausführen.)
   ```

Ersetzen Sie in allen oben genannten Befehlen `<Installationspfad>` durch den Pfad, in dem SiteScope installiert ist. Wenn Sie SiteScope beispielsweise im Verzeichnis "/usr" installiert haben, lautet der Befehl zum Beenden von SiteScope wie folgt:

```
/usr/SiteScope/stop
```

Verbinden mit SiteScope

SiteScope ist als Webapplikation konzipiert. Das bedeutet, dass Sie SiteScope über einen Webbrowser mit Zugriff auf den SiteScope-Server anzeigen und verwalten.

SiteScope wird bei der Installation für zwei Ports konfiguriert: 8080 und 8888. Ist ein anderer Dienst für die Verwendung dieser Ports konfiguriert, wird bei der Installation versucht, SiteScope für Antworten an einem anderen Port zu konfigurieren.

Auf Windows-Plattformen fügt der Installationsprozess außerdem eine Verknüpfung zu SiteScope im Menü **Start** > **Alle Programme** für SiteScope hinzu. Der Ordner **Startmenü** wird während der Installation ausgewählt.

Zugriff auf SiteScope:

Geben Sie die SiteScope-Adresse in einen Webbrowser ein. Die Standardadresse lautet: `http://localhost:8080/SiteScope`.

Auf Windows-Plattformen können Sie auch über das Startmenü auf SiteScope zugreifen. Klicken Sie hierzu auf **Start > Alle Programme > HP SiteScope** > **HP SiteScope öffnen**. Wenn Sie den SiteScope-Port nach der Installation von SiteScope ändern, wird der Port über den Link **HP SiteScope öffnen** aktualisiert.

Wird SiteScope das erste Mal bereitgestellt, gibt es eine Verzögerung bei der Initialisierung der Oberflächenelemente. SiteScope wird in der Dashboard-Ansicht geöffnet.

Hinweis:

- Um den Zugriff auf dieses Konto und seine Berechtigungen einzuschränken, müssen Sie das Profil des Administratorkontos bearbeiten und einen Benutzernamen sowie ein Kennwort für die Anmeldung hinzufügen. SiteScope zeigt dann ein Anmeldungsdialogfeld an, bevor Sie auf SiteScope zugreifen können. Informationen zum Bearbeiten des Administrator-Kontoprofils finden Sie im Abschnitt "Voreinstellungen für Benutzerverwaltung" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.
- Bei der Anzeige von SiteScope auf einem anderen Computer sollte ein Computer verwendet werden, auf dem die neueste unterstützte Java Runtime Environment installiert ist.

SiteScope Classic-Oberfläche

Die SiteScope Classic-Oberfläche aus früheren Versionen von SiteScope, die den URL `http://<sitescope-host>:8888` verwendete, ist für die Verwaltung von SiteScope nicht länger verfügbar.

Sie können weiterhin auf bestimmte Seiten in der Classic-Oberfläche zugreifen, wenn diese in der Eigenschaft **_serverFilter** der Datei **master.config** aufgeführt sind. Zu den standardmäßig aufgeführten Seiten gehören **Monitor Summary** und **Alert Report**.

Hinweis: Sie sollten keine Seiten der SiteScope Classic-Oberfläche entfernen, die standardmäßig aktiviert sind, da dies zu Funktionsausfällen führen kann.

Fehlerbehebung und Einschränkungen

Dieser Abschnitt enthält Fehlerbehebungen und Einschränkungen für die folgenden Probleme bei der Anmeldung an SiteScope:

Bestimmte Probleme beim Start:

- "SiteScope wird nicht gestartet und eine Fehlermeldung angezeigt" unten
- "Beim Laden des SiteScope-Applets wird eine NoClassDefFound-Ausnahme ausgelöst" auf der nächsten Seite
- "Probleme beim Laden des Applets von einem 64-Bit-Computer" auf der nächsten Seite
- "SiteScope stürzt ab, wenn derselbe SiteScope-Server in einem Browserfenster in mehr als einer Registerkarte geöffnet wird" auf der nächsten Seite
- "Die Menüleiste von SiteScope wird geöffnet, aber das Applet wird nicht gestartet und es wird ein leerer Bildschirm, eine Fehlermeldung oder ein "x" angezeigt" auf Seite 248
- "Sichern und Wiederherstellen einer SiteScope-Installation, wenn SiteScope nicht gestartet werden kann" auf Seite 248
- "SiteScope kann in Firefox nicht geöffnet werden" auf Seite 251

SiteScope wird nicht gestartet und eine Fehlermeldung angezeigt

Handelt es sich um eine Fehlermeldung wie "The Java Runtime Environment cannot be loaded" oder einen anderen unbekannten Fehler beim Start des SiteScope-Applets, führen Sie die folgenden Schritte durch:

Versuchen Sie nach jedem Schritt erneut, SiteScope zu öffnen. Schlägt SiteScope wieder fehl, fahren Sie mit dem nächsten Schritt fort.

1. Schließen Sie alle Browserfenster.
2. Beenden Sie ggf. alle übrigen Browserprozesse über den Windows Task-Manager.
3. Leeren Sie den lokalen Java-Applet-Cache. Navigieren Sie zu **Start > Systemsteuerung > Java**. Klicken Sie auf der Registerkarte **Allgemein** auf **Einstellungen > Dateien löschen** und klicken Sie dann auf **OK**.

4. Leeren Sie den lokalen Java-Applet-Cache, indem Sie den Inhalt des folgenden Ordners löschen: `C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Sun\Java\Deployment\cache`.

Beim Laden des SiteScope-Applets wird eine NoClassDefFound-Ausnahme ausgelöst

Wenn beim Laden des Applets eine NoClassDefFound-Ausnahme ausgelöst wird, wählen Sie die Option **Temporäre Dateien auf Rechner behalten** in der Java-Konfiguration für Ihren Client aus (**Systemsteuerung** > **Java** > Registerkarte **Allgemein** > **Temporäre Internetdateien** > **Einstellungen**).

Löschen Sie, falls Sicherheitsprobleme es erforderlich machen, die temporären Dateien manuell, wenn Sie das SiteScope-Applet nicht mehr verwenden:

1. Schließen Sie das SiteScope-Applet.
2. Wählen Sie **Start > Systemsteuerung > Java** > Registerkarte **Allgemein** aus.
3. Klicken Sie im Bereich **Temporäre Internetdateien** auf **Einstellungen** und dann auf **Dateien löschen**

Probleme beim Laden des Applets von einem 64-Bit-Computer

Wenn Sie SiteScope auf einem 64-Bit-Computer ausführen, stellen Sie sicher, dass Sie eine Browserversion verwenden, die der JRE-Bitzahl entspricht:

JRE	Browser
64-Bit-JRE	Internet Explorer (64-Bit)
32-Bit-JRE	Internet Explorer (32-Bit)

SiteScope stürzt ab, wenn derselbe SiteScope-Server in einem Browserfenster in mehr als einer Registerkarte geöffnet wird

Wird dieselbe SiteScope-Serverbenutzeroberfläche auf mehr als einer Registerkarte in einem Browserfenster geöffnet, reagiert SiteScope nicht beim Versuch zwischen den SiteScope-Serverregisterkarten zu navigieren.

Mögliche Lösung:

- Schließen Sie die überflüssige Registerkarten und stellen Sie sicher, dass jeweils nur eine Registerkarte für dieselbe SiteScope-Serverbenutzeroberfläche geöffnet ist.
- Alternativ können Sie auch ein neues Browserfenster öffnen.

Die Menüleiste von SiteScope wird geöffnet, aber das Applet wird nicht gestartet und es wird ein leerer Bildschirm, eine Fehlermeldung oder ein "x" angezeigt

Dies kann vorkommen, wenn die Java-Systemsteuerung nicht für die Verwendung des Webbrowsers konfiguriert ist.

Mögliche Lösung:

1. Navigieren Sie zu **Start > Systemsteuerung > Java**. Klicken Sie auf der Registerkarte **Allgemein** auf **Netzwerkeinstellungen**, wählen Sie die Option **Direkte Verbindung** aus und klicken Sie dann auf **OK**.
2. Erweitern Sie auf der Registerkarte **Erweitert** den Ordner **Standard-Java für Browser** (oder **<APPLET>-Tag-Unterstützung**, wenn Sie Java 5 verwenden). Stellen Sie sicher, dass **Microsoft Internet Explorer** und **Mozilla-Familie** ausgewählt sind. Klicken Sie auf **Anwenden** und klicken Sie dann auf **OK**.
3. Starten Sie Ihren Browser neu.

Sichern und Wiederherstellen einer SiteScope-Installation, wenn SiteScope nicht gestartet werden kann

Um die SiteScope-Konfigurationsdaten wiederherzustellen, wenn SiteScope ausfällt und nicht neu gestartet werden kann, sollten Sie eine Sicherung Ihres aktuellen SiteScope-Installationsverzeichnisses und aller entsprechenden Unterverzeichnisse erstellen, bevor Sie eine neue Version von SiteScope installieren. Sie können die aktuelle SiteScope-Installation sichern und mithilfe des Konfigurationswerkzeugs SiteScope-Daten in eine ZIP-Datei exportieren oder die erforderlichen Dateien manuell sichern.

Nach der Neuinstallation von SiteScope, können Sie Monitorkonfigurationsdaten mithilfe des Konfigurationswerkzeugs in SiteScope kopieren (wenn Sie das Tool verwendet haben, um eine Sicherung Ihres Installationsverzeichnisses zu erstellen), oder indem Sie im neuen

Installationsverzeichnis alle Ordner und Dateien löschen, die Sie gesichert haben, und anschließend die gesicherten Ordner und Dateien in das Installationsverzeichnis kopieren.

So sichern Sie die SiteScope-Installation:

1. Beenden Sie SiteScope.

   Hinweis: Auch wenn SiteScope nicht beendet werden muss, empfiehlt sich dies vor dem Erstellen einer Sicherung.

2. Erstellen Sie eine Sicherung Ihrer aktuellen SiteScope-Installation. Wenden Sie dazu einer der folgenden Methoden an:

   - Verwenden des Konfigurationswerkzeugs zum Exportieren Ihrer Konfiguration in eine ZIP-Datei. Weitere Informationen finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151.

   - Kopieren Sie die folgenden Ordner und Dateien der SiteScope-Installation in den Zielspeicher für Ihre Sicherung:

Verzeichnis	Beschreibung
\cache	Enthält Datenbeispiele, die nicht an Business Service Management gemeldet wurden, wenn Business Service Management nicht verfügbar war.
\conf\ems	Enthält wichtige Konfigurations- und Steuerungsdateien, die mit Integrationsmonitortypen verwendet werden. Dies ist nur relevant, wenn Sie SiteScope als Agent verwenden, der Reports für eine andere Applikation von Business Service Management erstellt.
\conf\integration	Enthält Topologiedateien, die für Integrationen mit Business Service Management verwendet werden.
\discovery\scripts\custom	Enthält benutzerdefinierte Discovery-Skripts.
\groups	Enthält Monitor-, Warnungs, Report- und andere wichtige Konfigurationsdaten, die für den Betrieb von SiteScope erforderlich sind.

Verzeichnis	Beschreibung
\htdocs	Enthält geplante Reports und benutzerdefinierte Stylesheets für die SiteScope-Oberfläche. Sichern Sie dieses Verzeichnis und kopieren Sie es in das SiteScope-Verzeichnis (innerhalb derselben SiteScope-Versionen), um zu verhindern, dass die Reportseiten beschädigt und alte Reports angezeigt werden. Dieser Ordner kann nicht gesichert werden, wenn die Konfiguration in eine neuere SiteScope-Version importiert wird.
\logs	Enthält eine Reihe von Protokollen einschließlich datumscodierter Protokolle mit Überwachungsdaten. Führen Sie eine selektive Sicherung der aktuellsten Protokolldateien für Überwachungsdaten zusammen mit den anderen Protokolltypen in diesem Verzeichnis durch. Aus Gründen der Verlaufskontinuität sollten Sie auch die folgenden Protokolle sichern: **error.log**, **RunMonitor.log**, **access.log**, **alert.log** und **monitorCount.log**.
\persistency	Dies ist das Hauptpersistenzverzeichnis des Produkts. Alle definierten Monitore, Gruppen, Warnungen, Vorlagen und viele weitere SiteScope-Entitäten befinden sich in diesem Verzeichnis.
\scripts	Enthält von den Script-Monitoren verwendete Skripts.
\scripts.remote	Enthält Befehlsskripts, die von Script-Monitoren zum Auslösen anderer Skripts auf Remoteservern verwendet werden.
\templates.*	Enthält Daten und Vorlagen für die Anpassung von Monitorfunktion, Warnungsinhalt und anderen Features. Die Unterverzeichnisse dieser Gruppe beginnen alle mit dem Namen **templates**. **Beispiel:** templates.mail, templates.os, templates.webscripts
\WEB-INF\lib\peregrine.jar	Datei, die beim Konfigurieren der HP Service Manager-Integration möglicherweise geändert wurde (neu generiert).

So stellen Sie die SiteScope-Installation wieder her:

1. Führen Sie die Installation von SiteScope erneut durch. Weitere Informationen finden Sie unter "Installationsworkflow" auf Seite 103.

2. Nach der Installation von SiteScope:

   - Wenn Sie zum Erstellen der Sicherung Ihres aktuellen SiteScope-Installationsverzeichnisses das Konfigurationswerkzeug verwendet haben, dann verwenden Sie es auch, um die zuvor erstellte

ZIP-Datei zu importieren. Weitere Informationen finden Sie unter "Verwenden des SiteScope-Konfigurationswerkzeugs" auf Seite 151.

- Wenn Sie jedoch manuell eine Sicherung erstellt haben, müssen Sie im neuen Installationsverzeichnis alle oben aufgeführten Ordner und Dateien löschen, die Sie gesichert haben, und anschließend die gesicherten Ordner und Dateien in das Installationsverzeichnis kopieren.

SiteScope kann in Firefox nicht geöffnet werden

Problem: SiteScope wird einem Firefox-Browser nicht geöffnet, wenn die Smartcard-Authentifizierung deaktiviert, die Authentifizierung per Clientzertifikat jedoch aktiviert ist.

Lösung: Informationen zum Öffnen von SiteScope in einem Firefox-Browser, wenn die Smartcard-Authentifizierung deaktiviert, die Authentifizierung per Clientzertifikat jedoch aktiviert ist, finden Sie unter "Verwenden von Firefox, wenn die Clientzertifizierung aktiviert ist" auf Seite 192.

Anhänge

Anhang A: Integrieren von IIS mit dem Tomcat-Server von SiteScope

Um Internet Information Server (IIS) mit dem in SiteScope enthaltenen Apache Tomcat-Server zu integrieren, müssen Sie Änderungen an den vom Apache Tomcat-Server verwendeten Konfigurationsdateien vornehmen und das virtuelle Verzeichnis im entsprechenden Websiteobjekt der IIS-Konfiguration erstellen.

In diesem Abschnitt wird Folgendes behandelt:

Konfigurieren der Apache Tomcat-Serverdateien

Um die Integration von IIS mit dem Apache Tomcat-Server zu ermöglichen, müssen Sie die Konfigurationsdateien für den in SiteScope enthaltenen Apache Tomcat-Server bearbeiten.

So konfigurieren Sie die Apache Tomcat-Serverdateien:

1. Laden Sie die neuste Version von Java Connector jk von der Apache-Downloadsite für Connector-Dateien herunter. Der URL lautet folgendermaßen:

   http://tomcat.apache.org/download-connectors.cgi

2. Kopieren Sie die Datei **isapi_redirect.dll** in das Verzeichnis **<Tomcat-Installation>\bin\win32**. Standardmäßig wird ein Tomcat-Server als Teil der SiteScope-Installation unter **C:\SiteScope\Tomcat** installiert. Erstellen Sie das Verzeichnis **win32** (falls nicht vorhanden).

3. Führen Sie einen der folgenden Schritte durch:

   - Erstellen Sie im selben Verzeichnis wie die Datei **isapi_redirect.dll** eine Konfigurationsdatei mit dem Namen **isapi_redirect.properties**.

     Beispiel der Datei isapi_redirect.properties:

     ```
     # Configuration file for the Jakarta ISAPI Redirector
     ```

```
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector
log_file=C:\SiteScope\Tomcat\logs\isapi.log

# Log level (debug, info, warn, error or trace)
log_level=info

# Full path to the workers.properties file
worker_file=C:\SiteScope\Tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file
worker_mount_file=C:\SiteScope\Tomcat\conf\uriworkermap.properties
```

Diese Konfiguration verweist auf die Protokolldatei, die im Verzeichnis **<SiteScope-Stammverzeichnis>\Tomcat\logs** untergebracht werden sollte, sowie auf die Worker- und Worker-Mount-Dateien, die im Verzeichnis **<SiteScope-Stammverzeichnis>\Tomcat\conf** gespeichert werden sollten.

- Fügen Sie dieselben Konfigurationseinträge (siehe oben) unter folgendem Pfad der Registrierung hinzu: `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0`

4. Erstellen Sie die Workers-Datei von SiteScope mit dem Namen **workers.properties.minimal** im Verzeichnis **<SiteScope-Stammverzeichnis>\Tomcat\conf**.

Beispiel der workers-Datei von SiteScope:

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
worker.list=ajp13w
worker.ajp13w.type=ajp13
worker.ajp13w.host=localhost
```

```
worker.ajp13w.port=8009
#END
```

Hinweis:

- **worker.ajp13w.port** hängt von der verwendeten Tomcat-Version ab. Öffnen Sie die Datei **<SiteScope-Stammverzeichnis>\Tomcat\conf\server.xml** und suchen Sie nach der Zeichenfolge `<Connector port=`, um festzustellen, welchen Port diese Tomcat-Version verwendet.
- Wenn Sie SiteScope für die Integration mit SiteMinder konfigurieren, ändern Sie den Redirect-Port im Abschnitt <!-- Define an AJP 1.3 Connector on port 8009 --> der Datei **server.xml** von:

  ```
  <!--   <Connector port="18009"
  URIEncoding="UTF-8" enableLookups="false" redirectPort="8443"
  protocol="AJP/1.3" /> -->
  ```

  um in

  ```
  <Connector port="18009"
  URIEncoding="UTF-8" enableLookups="false" redirectPort="80"
  protocol="AJP/1.3" />
  ```

- Befinden sich IIS und Tomcat nicht auf demselben Computer, ändern Sie das Hostattribut in **workers.properties.minimal** so, dass es auf den anderen Computer verweist.

5. Erstellen Sie die Workers-Mount-Datei für SiteScope im Verzeichnis **<SiteScope-Stammverzeichnis>\Tomcat\conf**.

   Dies ist das Beispiel der workers-Datei von SiteScope mit dem Namen uriworkermap.properties (wie im Konfigurationsbeispiel oben):

   ```
   # uriworkermap.properties - IIS
   #
   # This file provides sample mappings for example:
   # ajp13w worker defined in workermap.properties.minimal
   # The general syntax for this file is:
   # [URL]=[Worker name]
   /SiteScope=ajp13w
   /SiteScope/*=ajp13w
   #END
   ```

   In der neuen Syntax sind die beiden Regeln für SiteScope in einer Regel zusammengefasst: `/SiteScope/*=ajp13w`

Die Tomcat-Protokollausgabe wird in die Datei **<SiteScope-Stammverzeichnis>\logs\tomcat.log** geschrieben. Die Einstellungen für die Protokolldatei können über die Datei **<SiteScope-Stammverzeichnis>\Tomcat\common\classes\log4j.properties** konfiguriert werden.

Fehlerbehebung

Problem: Wenn von früheren Versionen von SiteScope aktualisiert wird, wird die Tomcat-Konfigurationsdatei **server.xml** im Verzeichnis **<SiteScope-Stammverzeichnis>\Tomcat\conf** überschrieben und alle Änderungen daran werden entfernt (beispielsweise Änderungen, die beim Konfigurieren von SiteScope für die Verwendung von SSL vorgenommen wurden).

Lösung: Zum Wiederherstellen dieser Änderungen müssen Sie diese erneut in der Datei **server.xml** durchführen, nachdem die Aktualisierung durchgeführt wurde.

a. Beenden Sie SiteScope.

b. Ersetzen Sie die folgenden Dateien:

Ersetzen Sie die Datei	Mit
<SiteScope-Stammverzeichnis>\java\lib\security\cacerts	**<SiteScope-Stammverzeichnis>\installation\HPSiS1122\backup\java\lib\security\cacerts**
<SiteScope-Stammverzeichnis>\java\lib\security\java.security	**<SiteScope-Stammverzeichnis>\installation\HPSiS1122\backup\java\lib\security\java.security**
<SiteScope-Stammverzeichnis>\java\lib\security\javaws.policy	**<SiteScope-Stammverzeichnis>\installation\HPSiS1122\backup\java\lib\security\javaws.policy**
<SiteScope-Stammverzeichnis>\java\lib\security\java.policy	**<SiteScope-Stammverzeichnis>\installation\HPSiS1122\backup\java\lib\security\java.policy**

c. Wenden Sie manuell alle Änderungen in Bezug auf Optimierung und Anpassung erneut an, indem Sie diese aus der Datei **<SiteScope-Stammverzeichnis>\installation\HPSiS1122\backup\Tomcat\conf\server.xml** in die Datei **<SiteScope-Stammverzeichnis>\Tomcat\conf\server.xml** kopieren.

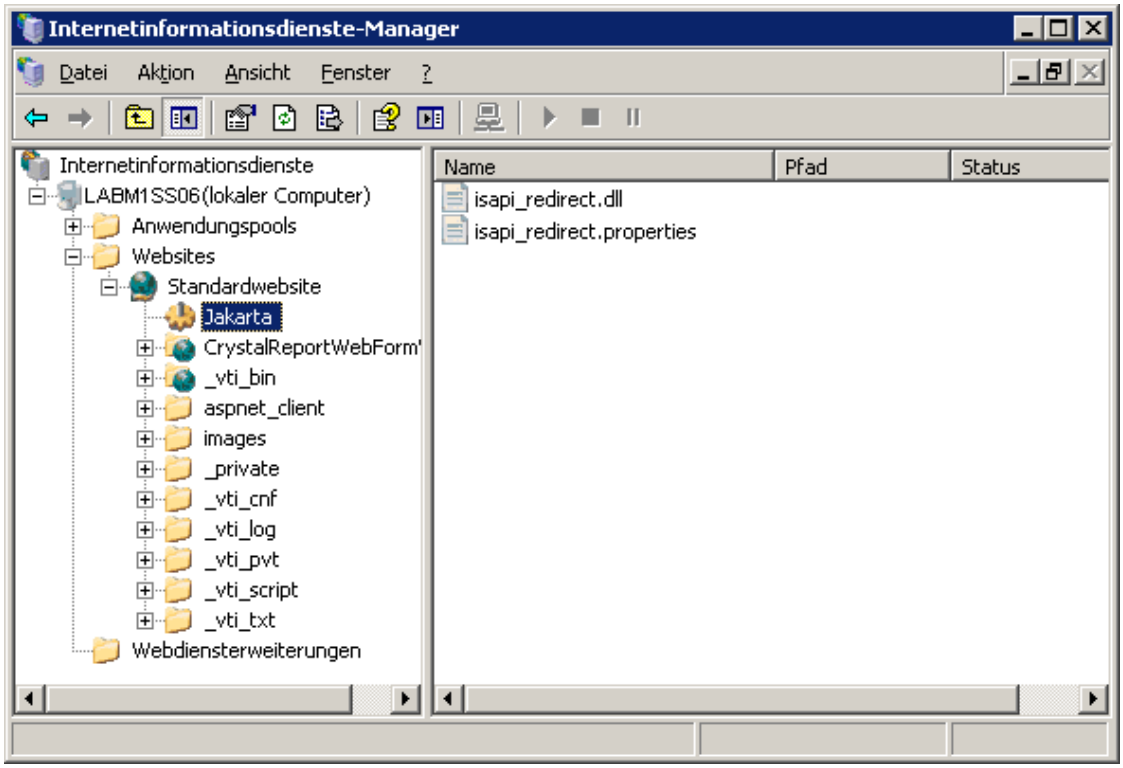
Konfigurieren von IIS

Nachdem Sie Änderungen an den vom Tomcat-Server verwendeten Konfigurationsdateien durchgeführt haben, müssen Sie das virtuelle Verzeichnis im entsprechenden Websiteobjekt der IIS-Konfiguration erstellen.

So konfigurieren Sie IIS:

1. Klicken Sie im Startmenü von Windows auf **Einstellungen > Systemsteuerung > Verwaltung > Internetinformationsdienste-Manager**.

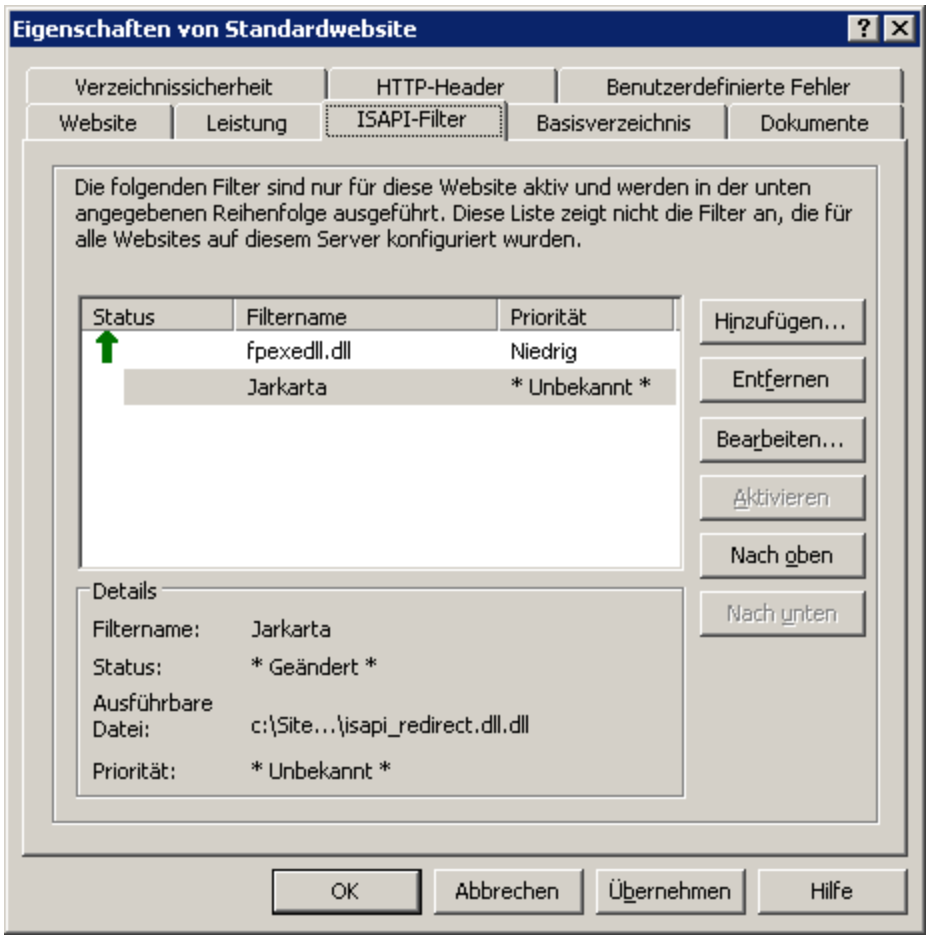
2. Klicken Sie im rechten Bereich mit der Maustaste auf **<Name des lokalen Computers>\Websites\<Name Ihrer Website>** und klicken Sie dann auf **Neu\Virtuelles Verzeichnis**. Geben Sie dem Verzeichnis den Namen **Jakarta** und legen Sie als lokalen Pfad das Verzeichnis mit der Datei **isapi_redirect.dll** fest.



3. Klicken Sie mit der rechten Maustaste auf **<Name Ihrer Website>** und klicken Sie dann auf **Eigenschaften**.

4. Klicken Sie auf die Registerkarte **ISAPI-Filter** und klicken Sie dann auf **Hinzufügen**. Wählen Sie in

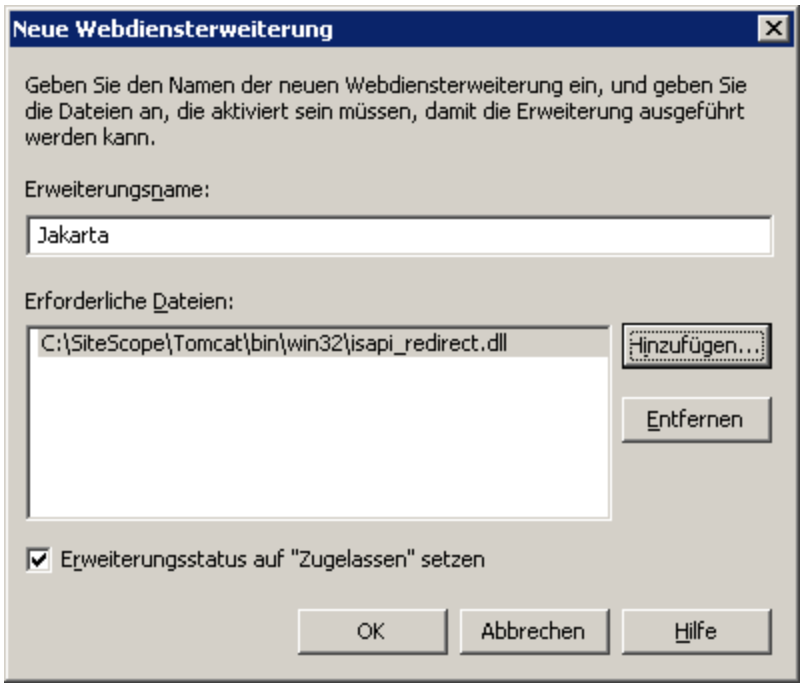
der Spalte **Filtername** den Filter **Jakarta** aus und suchen Sie nach **isapi_redirect.dll**. Der Filter wurde hinzugefügt, ist aber zu diesem Zeitpunkt noch nicht aktiv.



Klicken Sie auf **Übernehmen**.

5. Klicken Sie mit der rechten Maustaste auf **<Name des lokalen Computers>\Webdiensterweiterung** und klicken Sie dann auf **Neue Webdiensterweiterung hinzufügen**. Das Dialogfeld **Neue Webdiensterweiterung** wird geöffnet.

6. Geben Sie im Feld **Erweiterungsname** den Namen `Jakarta` ein und suchen Sie unter **Erforderliche Dateien** die Datei **isapi_redirect.dll**. Aktivieren Sie das Kontrollkästchen **Erweiterungsstatus auf "Zugelassen" setzen**.



Klicken Sie auf **OK**.

7. Starten Sie den IIS-Webserver neu und versuchen Sie, über den Webservice auf die Applikation zuzugreifen.

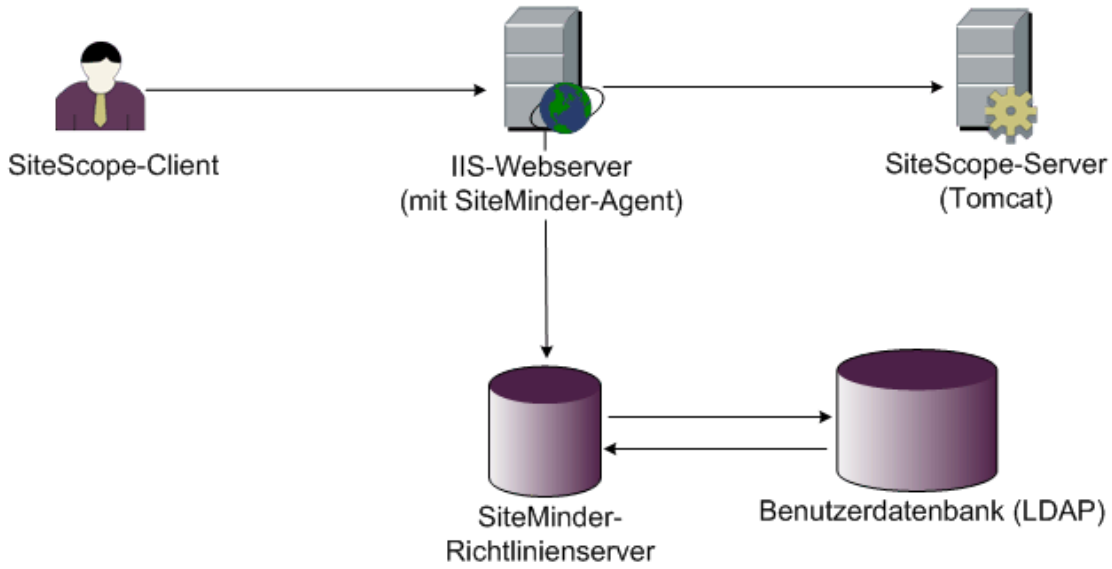
Anhang B: Integrieren von SiteScope mit SiteMinder

SiteScope kann mit SiteMinder, einer Lösung für die Verwaltung sicheren Zugriffs, integriert werden, um die Konfigurationen des Kunden für Benutzer- und Zugriffsverwaltung optimal zu nutzen.

In diesem Abschnitt wird Folgendes behandelt:

Grundlegendes zur Integration mit SiteMinder

Die folgende Abbildung zeigt die Integration von SiteScope mit SiteMinder für die Authentifizierung und Autorisierung von SiteScope-Benutzern.



In dieser Architektur ist ein SiteMinder-Agent auf dem IIS-Webserver konfiguriert, der vor dem Tomcat-Applikationsserver von SiteScope platziert ist. Der SiteMinder-Agent muss sich auf einem Webserver befinden. Der IIS-Webserver ist mit dem SiteMinder-Richtlinienserver verbunden, der alle SiteScope-Benutzer verwaltet (über ein LDAP- oder ähnliches Repository).

Der SiteMinder-Agent fängt den gesamten Verkehr von SiteScope ab und überprüft die Anmeldeinformationen des Benutzers. Die Anmeldeinformationen des Benutzers werden zur Authentifizierung und Autorisierung an den SiteMinder-Richtlinienserver gesendet. Wenn SiteMinder den Benutzer authentifiziert, sendet SiteScope ein Token (über einen speziellen HTTP-Header), in dem genau der Benutzer beschrieben wird, der sich angemeldet und die Autorisierung von SiteMinder erhalten hat.

Hinweis: SiteScope-Client, IIS-Webserver und der Tomcat-Applikationsserver von SiteScope sollten auf demselben Computer konfiguriert werden.

Integrationsanforderungen

In diesem Abschnitt werden die minimalen Systemanforderungen für die Integration von SiteScope mit SiteMinder angezeigt.

Betriebssystem	Windows 2003 Standard/Enterprise SP1
Webserver	IIS 5.0, IIS 6.0

Applikationsserver	Tomcat 5.0.x
Java Connector	Java Connector jk-1.2.21

Integrationsprozess

In diesem Abschnitt wird der SiteMinder-Integrationsprozess beschrieben.

So integrieren Sie SiteScope mit SiteMinder:

1. **Bereiten Sie den SiteMinder-Richtlinienserver vor und konfigurieren Sie ihn.**

   Der SiteMinder-Administrator muss den SiteMinder-Richtlinienserver für die Installation des Webagenten vorbereiten, den Webagenten auf dem IIS-Webserver installieren und den Webagenten konfigurieren.

   Außerdem muss der SiteMinder-Administrator den SiteMinder-Richtlinienserver konfigurieren. Empfehlungen zu den Details der SiteMinder-Konfiguration finden Sie unter "Konfigurieren des SiteMinder-Richtlinienservers" unten.

2. **Konfigurieren Sie SiteScope für die Verwendung von SiteMinder.**

   Zum Aktivieren von SiteScope für die Integration mit SiteMinder müssen Sie Änderungen an den vom Tomcat-Server verwendeten Konfigurationsdateien vornehmen. Weitere Informationen finden Sie unter "Konfigurieren der Apache Tomcat-Serverdateien" auf Seite 253.

3. **Konfigurieren Sie IIS.**

   Sie müssen das virtuelle Verzeichnis im entsprechenden Websiteobjekt der IIS-Konfiguration erstellen. Weitere Informationen finden Sie unter "Konfigurieren von IIS" auf Seite 257.

4. **Definieren Sie Berechtigungen für die verschiedenen SiteScope-Rollen.**

   Nachdem Sie die SiteMinder-Integration aktiviert haben, müssen Sie die Berechtigungen für die verschiedenen Rollen in SiteScope definieren. Weitere Informationen finden Sie unter "Definieren von Berechtigungen für die verschiedenen SiteScope-Rollen" auf Seite 265.

Konfigurieren des SiteMinder-Richtlinienservers

Sie konfigurieren den SiteMinder-Richtlinienserver, indem Sie ein SiteScope-Bereichsobjekt, zwei SiteScope-Regelobjekte für die Authentifizierung und Weiterleitung des Cookies mit zusätzlichen

Attributen und ein SiteScope-Antwortobjekt für die Übertragung zusätzlicher LDAP-Attribute an SiteScope erstellen und SiteScope-Regeln und -Antworten zum Sicherheitsrichtlinienobjekt hinzufügen.

Stellen Sie vor dem Erstellen eines SiteScope-Bereichsobjekts auf dem Richtlinienserver Folgendes sicher:

- Es wurde ein spezieller Administrator über einer Domäne konfiguriert (die wiederum an mindestens ein Benutzerverzeichnis gebunden ist).
- Es wurde mindestens ein Benutzerverzeichnisobjekt konfiguriert. Diese Objekte stellen die Benutzer im LDAP-Verzeichnis oder einem Repository dar.
- Sie haben ein Authentifizierungsschema definiert.

  Eine Domäne ist mit mindestens einem Benutzerverzeichnisobjekt verbunden. Es ist nicht erforderlich, eine spezielle Domäne für den Bereich zu erstellen. Sie können eine vorhandene Domäne verwenden.

So konfigurieren Sie den SiteMinder-Richtlinienserver:

1. Melden Sie sich an der SiteMinder-Verwaltung an.
2. Erstellen Sie einen Bereich und geben Sie folgende Informationen ein:
   - **Name.** Geben Sie einen Namen für den Bereich ein. Beispiel: **SiteScope-Bereich**.
   - **Resource Filter.** Geben Sie **/SiteScope** ein. Alles unter SiteScope ist Teil dieses Bereichs.
3. Klicken Sie mit der rechten Maustaste auf den neuen Bereich und klicken Sie dann auf **Create rule under realm**.
   - Erstellen Sie eine Regel für Authentifizierungszwecke. Geben Sie einen aussagekräftigen Namen für die Regel ein. Beispiel **SiteScope-Regel**. Wählen Sie im Abschnitt **Action** die Option **Web Agent Action** aus und wählen Sie alle HTTP-Anforderungsschemata aus (**Get**, **Post** und **Put**).
   - Erstellen Sie eine zweite Regel für die Weiterleitung von Cookies und anderen Attributen an SiteScope. Geben Sie einen aussagekräftigen Namen für die Regel ein. Beispiel **Benutzerrolle**. Wählen Sie im Abschnitt **Action** die Option **Authentication events** aus und wählen Sie in der Dropdownliste **OnAuthAccept** aus.
4. Erstellen Sie ein SiteScope-Antwortobjekt für die Übertragung der zusätzlichen LDAP-Attribute mit

den relevanten Authentifizierungsinformationen an SiteScope.

a. Klicken Sie mit der rechten Maustaste auf **Responses**, um das Fenster **Response Properties** zu öffnen.

b. Geben Sie einen aussagekräftigen Namen für die Antwort ein. Beispiel: **SiteScope-Rolle**.

c. Klicken Sie unterhalb des Abschnitts **Attribute List** auf die Schaltfläche **Create**, um ein neues Fenster für die Konfiguration einer Attributliste zu öffnen.

d. Wählen Sie im Abschnitt **Attribute Kind** die Option **User Attribute** aus.

e. Wählen Sie im Abschnitt **Attribute Fields** den Eintrag **SITESCOPE_ROLE** als Variablennamen aus und wählen Sie den Attributnamen aus, der als ausgewähltes Feld aus dem vordefinierten Benutzerverzeichnis im Header an SiteScope gesendet werden soll. Dabei handelt es sich um das Benutzerverzeichnisattribut, das bei der Authentifizierung gesendet wird.

Hinweis: Wenn Sie LDAP-Gruppenobjekte oder ein verschachteltes Gruppenobjekt zum Definieren der SiteScope-Rolle verwenden, sollten für das Feld **Attribute Name** spezielle SiteMinder-Variablen verwendet werden. Sie sollten die Variable **SM_USERGROUPS** für reguläre Gruppen verwenden und **SM_USERNESTEDGROUPS**, wenn der HTTP-Header **SITESCOPE_ROLE** die Informationen der verschachtelten Gruppen enthalten soll.

5. Fügen Sie dem Sicherheitsrichtlinienobjekt SiteScope-Regeln und -Antworten hinzu.

a. Klicken Sie auf die Option **Policies**, um eine neue Sicherheitsrichtlinie zu erstellen.

b. Geben Sie einen aussagekräftigen Namen für die Richtlinie ein. Beispiel: **SiteScope-Richtlinie**.

c. Klicken Sie auf die Registerkarte **Users** und fügen Sie die Entitäten hinzu, für die die Richtlinie gilt, bzw. entfernen Sie diese. (Sie können Entitäten nur aus den Benutzerverzeichnissen auswählen, die zu derselben Domäne des Bereichs gehören.)

d. Klicken Sie auf die Registerkarte **Rules** und wählen Sie die beiden in Schritt 3 beschriebenen Regeln aus, **Benutzerrolle** und **SiteScope-Regel**. Fügen Sie außerdem die Antwort **SiteScope-Rolle** hinzu, die zuvor in Schritt 4 als Antwort der Benutzerrolle definiert wurde.

Konfigurieren von SiteScope für die Verwendung von SiteMinder

Zum Aktivieren von SiteScope für die Integration mit SiteMinder müssen Sie Änderungen an den vom Tomcat-Server verwendeten Konfigurationsdateien vornehmen. Informationen zum Konfigurieren der Tomcat-Serverdateien finden Sie unter "Konfigurieren der Apache Tomcat-Serverdateien" auf Seite 253.

Konfigurieren von IIS

Nachdem Sie Änderungen an den vom Tomcat-Server verwendeten Konfigurationsdateien vorgenommen haben, müssen Sie IIS konfigurieren. Informationen zum Konfigurieren von IIS finden Sie in unter "Konfigurieren von IIS" auf Seite 257.

Definieren von Berechtigungen für die verschiedenen SiteScope-Rollen

Nachdem Sie die SiteMinder-Integration aktiviert haben, müssen Sie die Berechtigungen für die verschiedenen Rollen in SiteScope definieren (mit dem Berechtigungsmodell für regelmäßige SiteScope-Benutzer). Die Zuordnung der Benutzer zu diesen Rollen erfolgt außerhalb von SiteScope, z. B. in LDAP-Gruppen. Wird ein neuer SiteScope-Benutzer hinzugefügt, muss dieser nur in SiteMinder definiert werden, da der Benutzer automatisch die Berechtigungen der relevanten SiteScope-Rolle erbt.

Hinweis: Sie müssen sicherstellen, dass das von SiteMinder verwendete SiteScope-Benutzerkonto kein Kennwort erfordert, da SiteMinder die Anmeldung sonst nicht durchführen kann. Details zum Erstellen von Benutzerkonten finden Sie im Abschnitt "Voreinstellungen für Benutzerverwaltung" unter "Verwenden von SiteScope" in der SiteScope-Hilfe.

Anmelden bei SiteScope

Wenn ein Benutzer versucht, sich bei SiteScope anzumelden, wird die Anforderung von SiteMinder abgefangen. Werden die Anmeldeinformationen des Benutzers authentifiziert, wird ein zugewiesener SiteScope-Benutzername und eine Rolle (Gruppe) an SiteScope gesendet, z. B. `Benutzer: Fred, Role: Buchhaltung`). Falls SiteScope den Namen nicht als gültigen Benutzernamen erkennt, aber die

Rolle erkennt, wird der Benutzer über die Rolle bei SiteScope angemeldet (in diesem Fall als `Benutzer: Buchhaltung`).

So melden Sie sich an SiteScope an:

Öffnen Sie den Webbrowser und geben Sie die folgende URL ein:

`http://<Name_des_IIS-Computers>/SiteScope`.

Hinweis: Befinden sich IIS und SiteScope auf demselben Computer, sollten Sie eine Verbindung zu Standardport 80 herstellen, nicht zu Port 8080.

Wenn SiteMinder den Benutzer erfolgreich authentifiziert und die Anmeldung an SiteScope durchgeführt hat, wird SiteScope direkt in der Dashboard-Ansicht geöffnet.

Hinweise und Richtlinien

- Die Namen aller Benutzer, die bei SiteScope angemeldet sind, sind im Überwachungsprotokoll aufgelistet. Dieses befindet sich im Verzeichnis **<SiteScope-Stammverzeichnis>\logs**. Dies ist auch der Fall, wenn der Benutzer unter einem Rollennamen angemeldet ist. Wenn beispielsweise Benutzer `Fred` unter einer Rolle angemeldet ist, weil SiteScope `Fred` nicht als gültigen Benutzer erkannt hat, aber die Rolle erkannt wurde, sind alle Operationen mit dem Benutzernamen `Fred` trotzdem im Überwachungsprotokoll aufgelistet.

- Sie können eine Seite angeben, an die der Browser nach der Abmeldung aus der SiteMinder-Umgebung weitergeleitet wird. (Dabei handelt es sich um die Seite, die geöffnet wird, wenn Sie in SiteScope auf die Schaltfläche **LOGOUT** klicken.) Um die Abmeldungsseite zu aktivieren, öffnen Sie die Datei **master.config** im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** und fügen Sie folgende Zeile hinzu:

  `_siteMinderRedirectPageLogout=<url_to_go_to_after_logout>`

- Das von SiteMinder zur Anmeldung bei SiteScope verwendete Benutzerkonto darf kein Kennwort erfordern, da SiteMinder die Anmeldung sonst nicht durchführen kann. Details zum Einrichten von Benutzerkonten in SiteScope finden Sie im Abschnitt "Voreinstellungen für Benutzerverwaltung" im Kapitel "Verwenden von SiteScope" in der Hilfe zu SiteScope.

- Um zu verhindern, dass Benutzer direkt über die SiteScope-URL auf SiteScope zuzugreifen versuchen, sollten Sie die Deaktivierung der HTTP-Ports 8080 und 8888 auf dem Tomcat-Server während der SiteScope-Installation in Betracht ziehen.

- Um zu verhindern, dass Benutzer nach 30 Minuten ohne Aktivität im Webbrowser bei SiteScope

abgemeldet werden, ändern Sie die Eigenschaft "_keepAliveFromJSP=" in der Datei **master.config** in "=true".

Anhang C: Manuelles Konfigurieren von SiteScope für das Verwenden einer sicheren Verbindung

Sie können SiteScope manuell für eine sichere Verbindung konfigurieren, um den Zugriff auf die SiteScope-Oberfläche zu beschränken.

Es wird empfohlen, das Hardening-Tool für die Konfiguration von SiteScope für die SSL-Verwendung auszuführen. Details finden Sie unter "Verwenden des Hardening-Tools (Werkzeug zum Optimieren der Sicherheit)" auf Seite 216.

In diesem Abschnitt wird Folgendes behandelt:

Vorbereiten von SiteScope auf die Verwendung von TLS

SiteScope wird mit der Datei **Keytool.exe** ausgeliefert. Bei Keytool handelt es sich um ein Dienstprogramm für die Verwaltung von Schlüssel und Zertifikaten. Benutzer können damit ihre eigenen Paare aus privaten und öffentlichen Schlüsseln sowie die dazugehörigen Zertifikate für die Authentifizierung mithilfe digitaler Signaturen verwalten. Außerdem haben Benutzer die Möglichkeit, die öffentlichen Schlüssel anderer Personen und Organisationen, mit denen sie kommunizieren, zwischenzuspeichern. Das Dienstprogramm wird unter **<SiteScope-Installationspfad>\SiteScope\java\bin** installiert.

Achtung: Notieren Sie sich beim Erstellen, Anfordern und Installieren eines digitalen Zertifikats die

Parameter und Befehlszeilenargumente, die Sie in den einzelnen Prozessschritten verwenden. Es ist äußerst wichtig, dass Sie während der gesamten Prozedur dieselben Werte verwenden.

Hinweis:

- SiteScope nutzt ausschließlich Keystores und Truststores im JKS-Format.
- Um die SiteScope Classic-Oberfläche für die Verwendung mit TLS vorzubereiten, müssen Sie sowohl den Tomcat-Server (siehe "Konfigurieren von SiteScope für TLS auf Tomcat" auf Seite 274) als auch die Engine der Classic-Oberfläche (Anweisungen finden Sie "Zugreifen auf SiteScope-Reports und die klassische Benutzeroberfläche mit HTTPS" auf Seite 286) konfigurieren.

Weitere Informationen zu Keytool erhalten Sie auf der Oracle-Website unter (http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html).

Dieser Abschnitt umfasst die folgenden Themen:

- "Verwenden eines Zertifikats von einer Zertifizierungsstelle" unten
- "Verwenden eines selbstsignierten Zertifikats" auf Seite 272

Verwenden eines Zertifikats von einer Zertifizierungsstelle

Sie können ein digitales Zertifikat verwenden, das von einer Zertifizierungsstelle ausgegeben wurde. Dazu benötigen Sie ein digitales Zertifikat, das sich in die von Keytool verwendete Schlüsselspeicherdatei importieren lässt. Falls Ihr Unternehmen derzeit nicht über ein digitales Zertifikat für diesen Zweck verfügt, müssen Sie die Ausgabe eines Zertifikats bei einer Zertifizierungsstelle anfordern.

Anhand der folgenden Schritte erstellen Sie eine Keystore-Datei und eine digitale Zertifikatanforderung.

So verwenden Sie ein Zertifikat von einer Zertifizierungsstelle:

1. Beziehen Sie das Stammzertifikat (und alle anderen abgeleiteten Zertifikate) von einer Zertifizierungsstelle.
2. Importieren Sie das Stammzertifikat (und alle anderen abgeleiteten Zertifikate) nach **<SiteScope-Stammverzeichnis>\java\lib\security\cacerts**, entweder über die Benutzeroberfläche oder über

den folgenden Befehl:

```
keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore
..\lib\security\cacerts -storepass changeit
```

3. Entfernen Sie die Datei **serverKeystore**, die sich im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** befindet. Sie können sie löschen oder einfach in ein anderes Verzeichnis verschieben.

4. Erstellen Sie ein Schlüsselpaar, indem Sie die folgende Befehlszeile aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin directory** ausführen:

```
keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias
yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass
keypass -keyalg "RSA" -validity valdays
```

Hinweis:

- Dieser und alle anderen Befehle müssen in einer Zeile eingegeben werden. Die Zeile ist hier aus Platzgründen aufgeteilt.
- Die Zeichenfolge `serverKeystore`, die beim Erstellen der Zertifikate verwendet wird, muss so wie in der Dokumentation angegeben eingegeben werden, da sonst beim Verwenden von SiteScope Failover mit SSL ein Fehler auftritt.
- Das private Schlüsselkennwort und das Keystore-Kennwort müssen gleich sein, um folgenden Fehler zu vermeiden: `IOException: Cannot recover key`.

Mit diesem Befehl wird eine Datei namens **serverKeystore** im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** erstellt. SiteScope verwendet diese Datei, um die in Ihren sicheren Sitzungen verwendeten Zertifikate zu speichern. Stellen Sie sicher, dass Sie eine Sicherungskopie dieser Datei an einem anderen Speicherort aufbewahren.

Richtlinien und Einschränkungen

- Der Wert einer `-dname`-Option muss die folgende Reihenfolge aufweisen, wobei die kursiv geschriebenen Werte durch Werte Ihrer Wahl ersetzt werden. Die Schlüsselwörter sind Abkürzungen für folgende Werte:

  `CN` = commonName – Allgemeiner Name einer Person (Beispiel: `Peter Mustermann`)

OU = organizationUnit – Kleine Organisationseinheit (Beispiel: `NetAdmin`)

O = organizationName – Name eines Großunternehmens (Beispiel: `ACMe-Systems GmbH`)

L = localityName - Name eines Ortes (einer Stadt) (Beispiel: `Dortmund`)

ST = stateName – Name eines Bundeslands oder Kantons (Beispiel: `Nordrhein-Westfalen`)

C = country – Länderkennzahl aus zwei Buchstaben (Beispiel: `DE`)

- Bei den Unterkomponenten innerhalb der `-dname`-Variable (Zeichenfolge mit definiertem Namen) muss die Groß- oder Kleinschreibung sowie die Reihenfolge berücksichtigt werden, auch wenn Sie nicht alle Unterkomponenten verwenden müssen. Die `-dname`-Variable sollte Ihr Unternehmen darstellen. `CN` ist der Domänenname des Webservers, auf dem SiteScope installiert ist.
- Der Wert von `-storepass` ist ein Kennwort, das zum Schutz der KeyStore-Datei verwendet wird. Dieses Kennwort muss mindestens 6 Zeichen lang sein. Sie benötigen dieses Kennwort, um Zertifikatdaten aus der KeyStore-Datei zu importieren und zu entfernen.
- Bei der `-alias`-Variable handelt es sich um einen Alias oder Spitznamen, über den Sie einen Eintrag im Keystore identifizieren können.

5. Erstellen Sie eine Zertifikatanforderung für diese Keystore-Datei, indem Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** ausführen:

   ```
   keytool -certreq -alias yourAlias -file ..\..\groups\sis.csr -keystore
   ..\..\groups\serverKeystore -storepass passphrase
   ```

   Dieser Befehl erstellt eine Datei mit dem Namen **sis.csr** im Verzeichnis **<SiteScope-Stammverzeichnis>\groups**. Sie verwenden diese Datei, um ein Zertifikat von Ihrer Zertifizierungsstelle anzufordern.

   Wenn Sie Ihr Zertifikat von einer Zertifizierungsstelle erhalten haben (die Antwortnachricht sollte eine Datei mit dem Namen **cert.cer** enthalten), müssen Sie das Zertifikat in die KeyStore-Datei importieren, die Sie anhand der vorhergehenden Schritte erstellt haben. Die Datei sollte den Namen **serverKeystore** haben. Anhand der folgenden Schritte importieren Sie das Zertifikat zur Verwendung mit SiteScope.

6. Importieren Sie die Zertifikatdaten in die KeyStore-Datei, indem Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** ausführen:

```
keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore
..\..\groups\serverKeystore
```

Hinweis: Um beim Import des Zertifikats von einer Zertifizierungsstelle den Fehler `keytool error: java.lang.Exception: Failed to establish chain from reply` zu vermeiden, sollten Sie das Stammzertifikat (und alle anderen abgeleiteten Zertifikate) in **<SiteScope-Stammverzeichnis>\java\lib\security\cacerts** importieren und dazu entweder über die Benutzeroberfläche das Zertifikatemanagement verwenden oder den folgenden Befehl ausführen:

```
keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore
..\lib\security\cacerts -storepass changeit
```

7. Wenn **SiteScope** eine sichere Verbindung verwenden soll, müssen Sie bestimmte Einstellungen oder Konfigurationsdateien in **SiteScope** hinzufügen oder ändern. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für TLS auf Tomcat" auf Seite 274.

Verwenden eines selbstsignierten Zertifikats

Alternativ können Sie für die Konfiguration von SiteScope auch ein selbstsigniertes Zertifikat generieren. Hierzu gibt es folgende Möglichkeiten:

- **SSL-Werkzeug.** Weitere Informationen finden Sie unter "So verwenden Sie das SSL-Werkzeug:" unten.
- **Manuelle Konfiguration.** Verwenden Sie dazu die `-selfcert`-Option, damit das Keytool-Dienstprogramm ein selbstsigniertes Zertifikat generiert. Weitere Informationen finden Sie unter "So generieren Sie ein selbstsigniertes Zertifikat:" auf der nächsten Seite.

Hinweis: In den meisten Fälle empfehlen wir, das SSL-Werkzeug zu nutzen. Sie sollten jedoch die manuelle Konfiguration nutzen, wenn Sie SiteScope auf einer Windows-Plattform für SSL konfigurieren möchten und die Variable `%SITESCOPE_HOME%` nicht nur Verfügung steht (beispielsweise weil SiteScope bereits von einem anderen Speicherort aus mithilfe des Befehls **go.bat** gestartet wurde), oder auf einer Linux-Plattform, wenn SiteScope nicht im Verzeichnis **/opt/HP/SiteScope/** installiert wurde.

So verwenden Sie das SSL-Werkzeug:

1. Geben Sie Folgendes ein, um den SiteScope-Dienst zu beenden:

   ```
   cd /opt/HP/SiteScope/
   ./stop
   ```

2. Geben Sie Folgendes ein, um das SSL-Werkzeug zu starten:

   ```
   cd /opt/HP/SiteScope/tools/SSL/
   ./ssl_tool.sh
   ```

3. Folgen Sie den Anweisungen im SSL-Werkzeug.

So generieren Sie ein selbstsigniertes Zertifikat:

1. Entfernen Sie die Datei **serverKeystore**, die sich im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** befindet. Sie können sie löschen oder einfach in ein anderes Verzeichnis verschieben.

2. Führen Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** aus. Bei den kursiv dargestellten Werten handelt es sich um Variablen, die Sie mit spezifischen Informationen zu Ihrem Unternehmen füllen.

   ```
   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
   O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias
   yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass
   passphrase -keyalg "RSA" -validity valdays
   ```

   Hinweis:

   - Dieser und alle anderen Befehle müssen in einer Zeile eingegeben werden. Die Zeile ist hier aus Platzgründen aufgeteilt.
   - Die Zeichenfolge `serverKeystore`, die beim Erstellen der Zertifikate verwendet wird, muss so wie in der Dokumentation angegeben eingegeben werden, da sonst beim Verwenden von SiteScope Failover mit SSL ein Fehler auftritt.

3. Führen Sie den folgenden Befehl ebenfalls aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** aus.

   ```
   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -
   dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName,
   ```

```
L=yourLocation, ST=yourState, C=yourCountryCode" -keystore
..\..\groups\serverKeystore
```

4. Wenn SiteScope eine gesicherte Verbindung verwenden soll, müssen Sie bestimmte Einstellungen oder Konfigurationsdateien in SiteScope hinzufügen oder ändern. Weitere Informationen finden Sie unter "Konfigurieren von SiteScope für TLS auf Tomcat" unten.

5. Optional können Sie das Zertifikat für die Verwendung in BSM exportieren, indem Sie den folgenden Befehl ausführen:

   ```
   keytool -exportcert -alias yourAlias -file <SiteScope-
   Stammverzeichnis>\certificate_name.cer -keystore ..\..\groups\serverKeystore
   ```

   Geben Sie Ihr Keystore-Kennwort ein, wenn Sie dazu aufgefordert werden.

Konfigurieren von SiteScope für TLS auf Tomcat

Zum Aktivieren von TLS in Tomcat müssen Sie Änderungen an den vom Tomcat-Server verwendeten Konfigurationsdateien vornehmen.

1. Öffnen Sie die Datei **server.xml** unter **<SiteScope-Stammverzeichnis>\Tomcat\conf**.

2. Suchen Sie in der Konfigurationsdatei nach dem folgenden Abschnitt:

   ```
   <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
   <!--
   Connector port="8443" maxHttpHeaderSize="8192"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" disableUploadTimeout="true"
   acceptCount="100" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS"
   compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
   compressableMimeType="text/html,text/xml,text/javascript,text/css,image/x-
   icon,application/json" />
   ->
   ```

3. Ändern Sie den Abschnitt wie folgt:

   ```
   <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

   <Connector port="8443"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" disableUploadTimeout="true"
   ```

```
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
keystoreFile="<SiteScope-Installationspfad>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

<SiteScope-Installationspfad> ist hierbei der Pfad zu Ihrer SiteScope-Installation.

Hinweis:

- Sind auf demselben Server, auf dem SiteScope installiert ist, noch andere HP-Produkte installiert, müssen Sie Port 8443 möglicherweise ändern, um Konflikte zu vermeiden.
- Die Tomcat-Protokollausgabe wird in die Datei **<SiteScope-Stammverzeichnis>\logs\tomcat.log** geschrieben. Die Einstellungen für die Protokolldatei können über die Datei **<SiteScope-Stammverzeichnis>\Tomcat\common\classes\log4j.properties** konfiguriert werden.
- Sie können die Sicherheit auf dem Tomcat-Server durch das Deaktivieren von ineffektiven Verschlüsselungen verstärken. Öffnen Sie dazu **<SiteScope-Stammverzeichnis>\Tomcat\conf\server.xml** und ändern Sie die bestehende Liste wie folgt:

  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true" clientAuth="false"
  sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello" ciphers="SSL_RSA_WITH_RC4_128_SHA,
  TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_
  DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_
  3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"/>]

Tomcat sucht standardmäßig nach einer **.keystore**-Datei im Basisverzeichnis des SiteScope-Benutzers.

Weitere Informationen zur Aktivierung von TLS für den Tomcat-Server finden Sie unter http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html.

4. Sobald Sie Tomcat anhand dieses Beispiels für die Verwendung von TLS aktiviert haben, ist die SiteScope-Schnittstelle unter einem URL mit der folgenden Syntax verfügbar:

   https://<SiteScope_server>:8443/SiteScope (bei dem Link muss die Groß- und Kleinschreibung beachtet werden)

Konfigurieren von SiteScope für Mutual TLS-Konfiguration

Führen Sie die folgenden Schritte aus, wenn der SiteScope-Server ein Clientzertifikat vom Client benötigt.

1. SiteScope sollte mit TLS konfiguriert sein. Details finden Sie unter "Konfigurieren von SiteScope für TLS auf Tomcat" auf Seite 274.

2. Konfigurieren Sie den Tomcat-Server für das Anfordern eines Clientzertifikats, indem Sie den folgenden Abschnitt der Konfigurationsdatei **<SiteScope-Stammverzeichnis>\Tomcat\conf\server.xml** suchen:

```
<Connector port="8443"
       maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
       enableLookups="false" disableUploadTimeout="true"
       acceptCount="100" debug="0" scheme="https" secure="true"
       sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
       keystoreFile="..\groups\serverKeystore"
       keystorePass="changeit"
```

   Fügen Sie die folgenden Attribute hinzu und ändern Sie den Parameter `clientAuth="true"`:

```
        truststoreFile="..\java\lib\security\cacerts"
       truststorePass="changeit"
       truststoreType="JKS"
       clientAuth="true"
/>
```

3. Importieren Sie das Stammzertifikat der Zertifizierungsstelle, die Clientzertifikate an Ihre Organisation ausgibt, in den SiteScope-Truststore (**<SiteScope-Stammverzeichnis>\java\lib\security\cacerts**), indem Sie den folgenden Befehl ausführen:

```
C:\SiteScope\java\>keytool -import -trustcacerts -alias <your alias> -keystore
..\lib\security\
   cacerts -file <Zertifikatdatei>
```

4. Erstellen Sie ein Clientzertifikat oder verwenden Sie ein vorhandenes Zertifikat und importieren Sie dieses in den Browser.

5. Starten Sie SiteScope neu und greifen Sie mit dem folgenden Link darauf zu:

   `https://<server>:8443/SiteScope` (bei dem Link muss die Groß- und Kleinschreibung beachtet werden)

Hinweis:

Für Aufrufe der SiteScope SOAP API ist ebenfalls ein Zertifikat erforderlich. Fügen Sie Folgendes zu Ihrem Java-Code hinzu, um mit einem Clientzertifikat zu antworten:

```
System.setProperty("javax.net.ssl.keyStore",<Pfadname zum Clientzertifikat-Keystore im JKS-Format>);
```

```
System.setProperty("javax.net.ssl.keyStorePassword", >Kennwort des Clientzertifikat-Keystore>);
```

(Optional) `System.setProperty("javax.net.ssl.trustStore", <Pfadname zum Truststore im JKS-Format>);`

oder verwenden Sie die folgenden JVM-Argumente:

```
-Djavax.net.ssl.keyStore=<Pfadname zum Clientzertifikat-Keystore im JKS-Format>
```

```
-Djavax.net.ssl.keyStorePassword=<Kennwort des Clientzertifikat-Keystore>
```

(Optional) `-Djavax.net.ssl.trustStore=<Pfadname zum Truststore im JKS-Format>`

Konfigurieren von SiteScope für die Verbindung mit dem BSM-Server mit TLS-Bereitstellung

Gehen Sie folgendermaßen vor, um SiteScope mit einem BSM-Server zu verbinden und dabei die TLS-Bereitstellung zu verwenden:

1. Stellen Sie die Verbindung mit dem SiteScope-Server her.
2. Importieren Sie das CA-Stammzertifikat oder das BSM-Serverzertifikat mit dem Zertifikatemanagement der SiteScope-Benutzeroberfläche in SiteScope. Details finden Sie im Abschnitt zum Zertifikatemanagement unter Verwenden von SiteScope in der SiteScope-Hilfe.
3. Wenn BSM mit einem Lastenausgleichsmodul konfiguriert ist, importieren Sie die Zertifikate des Load Balance Core und Center-URLs in SiteScope, indem Sie das Zertifikatemanagement in der SiteScope-Benutzeroberfläche verwenden. Details finden Sie im Abschnitt zum Zertifikatemanagement unter Verwenden von SiteScope in der SiteScope-Hilfe.
4. Details zum Importieren des Zertifikats in BSM finden Sie im Abschnitt zur Verwendung von SSL mit SiteScope im BSM Hardening Guide in der BSM Dokumentationsbibliothek.

Konfigurieren von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert

So verbinden Sie SiteScope mit einem BSM-Server, für den ein Clientzertifikat erforderlich ist:

1. Stellen Sie die Verbindung mit dem SiteScope-Server her.
2. Importieren Sie das CA-Stammzertifikat oder das BSM-Serverzertifikat mit dem Zertifikatemanagement der SiteScope-Benutzeroberfläche in SiteScope. Details finden Sie im Abschnitt zum Zertifikatemanagement unter Verwenden von SiteScope in der SiteScope-Hilfe.
3. Wenn Ihnen das Clientzertifikat im JKS-Format vorliegt, kopieren Sie dieses in den Ordner **<SiteScope-Stammverzeichnis>\templates.certificates**, und fahren Sie mit Schritt 11 fort.

   Hinweis:

   - Vergewissern Sie sich, dass das Kennwort für den privaten Schlüssel mindestens 6 Zeichen umfasst und mit dem Keystore-Kennwort identisch ist.
   - Stellen Sie außerdem sicher, dass der obige Keystore das von der Zertifizierungsstelle (CA) ausgestellte Zertifikat enthält.

   Wenn das Clientzertifikat in einem anderen Format vorliegt, führen Sie die folgenden Schritte aus.

4. Erstellen Sie eine Keystore-Datei unter **<Sitescope-Stammverzeichnis>/templates.certificates**, indem Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** ausführen:

   ```
   keytool -genkey -keyalg RSA -alias sis -keystore
   <SiteScope-Stammverzeichnis>\templates.certificates\.ks -storepass
   <Ihr_Keystore_Kennwort>
   ```

   Beispiel:

   ```
   keytool -genkey -keyalg RSA -alias sis -keystore
   C:\SiteScope\templates.certificates\.ks -storepass changeit
   What is your first and last name?
   [Unknown]: domain.name
   ```

```
What is the name of your organizational unit?
[Unknown]: dept
What is the name of your organization?
[Unknown]: XYZ Ltd
What is the name of your City or Locality?
[Unknown]:  New York
What is the name of your State or Province?
[Unknown]:  USA
What is the two-letter country code for this unit?
[Unknown]:  US
Is CN=domain.name, OU=dept, O=XYZ Ltd, L=New York, ST=USA, C=US correct?
[no]:  Ja

Enter key password for <SiteScope>
```

Drücken Sie die `Eingabetaste`, um dasselbe Kennwort wie für die Keystore-Datei zu verwenden.

5. Erstellen Sie eine Zertifikatanforderung für diese Keystore-Datei, indem Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** ausführen:

   ```
   keytool -certreq -alias sis -file c:\sis.csr -keystore
   <SiteScope-Stammverzeichnis>\templates.certificates\.ks -storepass
   <Ihr_Keystore_Kennwort>
   ```

   Beispiel:

   ```
   keytool -certreq -alias sis -file c:\sis.csr -keystore
   C:\SiteScope\templates.certificates\.ks -storepass changeit
   ```

6. Lassen Sie die Zertifikatanforderung von Ihrer Zertifizierungsstelle signieren. Kopieren Sie den Inhalt der Datei **.csr** in das Webformular der Zertifizierungsstelle.

7. Laden Sie das signierte Clientzertifikat im BASE-64-Format in das Verzeichnis **<SiteScope-Stammverzeichnis>\templates.certificates\clientcert.cer** herunter.

8. Laden Sie das Zertifikat der Zertifizierungsstelle im BASE-64-Format nach `c:\` herunter.

9. Importieren Sie das CA-Zertifikat in die JKS-Keystore-Datei, indem Sie den folgenden Befehl ausführen:

   ```
   keytool -import -alias ca -file c:\ca.cer -keystore
   <SiteScope-Stammverzeichnis>\templates.certificates\.ks -storepass
   <Ihr_Keystore_Kennwort>
   ```

Beispiel:

```
keytool -import -alias ca -file c:\ca.cer -keystore
C:\SiteScope\templates.certificates\.ks -storepass changeit
Owner: CN=dept-CA, DC=domain.name
Issuer: CN=dept-CA, DC=domain.name
Serial number: 2c2721eb293d60b4424fe82e37794d2c
Valid from: Tue Jun 17 11:49:31 IDT 2008 until: Mon Jun 17 11:57:06 IDT 2013
Certificate fingerprints:
MD5:  14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
SHA1: 17:2F:4E:76:83:5F:03:BB:A4:B9:96:D4:80:E3:08:94:8C:D5:4A:D5
Trust this certificate? [no]:  Ja
Certificate was added to keystore
```

10. Importieren Sie das Clientzertifikat in die Keystore-Datei, indem Sie den folgenden Befehl ausführen:

    ```
    keytool -import -alias sis -file
    <SiteScope-Stammverzeichnis>\templates.certificates\certnew.cer -keystore
    <SiteScope-Stammverzeichnis>\templates.certificates\.ks -storepass
    <Ihr_Keystore_Kennwort>
    ```

    Beispiel:

    ```
    keytool -import -alias sis -fil
    c:\SiteScope\templates.certificates\certnew.cer -keystore
    C:\SiteScope\templates.certificates\.ks -storepass changeit
    ```

    Die Zertifikatantwort wird in der Keystore-Datei im Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** installiert.

11. Überprüfen Sie den Inhalt der Keystore-Datei, indem Sie den folgenden Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** ausführen und das Keystore-Kennwort eingeben:

    ```
    keytool -list -keystore <SiteScope-Stammverzeichnis>\templates.certificates\.ks
    ```

    Beispiel:

    ```
    keytool -list -keystore C:\SiteScope\templates.certificates\.ks
    Enter keystore password:  changeit

    Keystore type: jks
    ```

```
Keystore provider: SUN

Your keystore contains 2 entries
ca, Mar 8, 2009, trustedCertEntry,
Certificate fingerprint (MD5):
14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
sis, Mar 8, 2009, keyEntry,
Certificate fingerprint (MD5):
C7:70:8B:3C:2D:A9:48:EB:24:8A:46:77:B0:A3:42:E1

C:\SiteScope\java\bin>
```

12. Um diese Keystore-Datei für ein Clientzertifikat zu verwenden, fügen Sie die folgenden Zeilen zu der Datei unter **<SiteScope-Stammverzeichnis>\groups\master.config** hinzu:

    ```
    _urlClientCert=<KeystoreName>

    _urlClientCertPassword=<KeystoreKennwort>
    ```

    Beispiel:

    ```
    _urlClientCert=.ks
    _urlClientCertPassword=changeit
    ```

13. Speichern Sie die an der Datei vorgenommen Änderungen.

14. Klicken Sie in **SiteScope Voreinstellungen > Integrationsvoreinstellungen > Verfügbare Operationen für BSM-Voreinstellungen** auf **Zurücksetzen**, um alle BSM-Einstellungen aus dem SiteScope-Server und alle SiteScope-Konfigurationen aus BSM zu löschen.

15. Starten Sie den SiteScope-Server neu.

16. Wählen Sie in BSM **Admin > System Availability Management** und klicken Sie auf die Schaltfläche **Neuer SiteScope**, um die SiteScope-Instanz hinzuzufügen.

    Hinweis: Schlägt die Verbindung zwischen SiteScope und BSM fehl, überprüfen Sie das **<SiteScope-Stammverzeichnis>\log\bac_integration.log** auf Fehler.

Konfigurieren des Topologie-Discovery-Agenten in SiteScope, wenn für den BSM-Server ein Clientzertifikat erforderlich ist

Nachdem Sie BSM für die Herstellung einer Verbindung mit dem BSM-Gateway-Server unter Verwendung eines Clientzertifikats konfiguriert haben (siehe "Konfigurieren von SiteScope für das Verbinden mit einem BSM-Server, der ein Clientzertifikat erfordert" auf Seite 278), müssen Sie die folgenden Schritte durchführen, damit Discovery Topologie-Reports an den BSM-Server sendet.

1. Erstellen Sie im **<SiteScope-Stammverzeichnis>\WEB-INF\classes** einen Ordner mit dem Namen **security** (sofern dieser nicht bereits existiert).

2. Verschieben Sie die Dateien **MAMTrustStoreExp.jks** und **ssl.properties** aus dem Ordner **<SiteScope-Stammverzeichnis>\WEB-INF\classes** in dne Ordner **<SiteScope-Stammverzeichnis>\WEB-INF\classes\security**.

3. Importieren Sie das CA-Stammzertifikat (oder das BSM-Serverzertifikat) in den Discovery Truststore (**MAMTrustStoreExp.jks**) mit dem folgenden Kennwort (das Standardkennwort für den Discovery Truststore lautet **logomania**; dieses lautet verschlüsselt: [22,-8,116,-119,-107,64,49,93,-69,57,-13,-123,-32,-114,-88,-61]):

   ```
   keytool -import -alias <ihr_CA> -keystore <SiteScope-Stammverzeichnis>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <ihr_keystore_kennwort>
   ```

   Beispiel:

   ```
   keytool -import -alias AMQA_CA -file c:\ca.cer -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania
   ```

   Hinweis: Das Kennwort für den privaten Schlüssel muss mindestens 6 Zeichen umfassen und mit dem Keystore-Kennwort identisch sein.

4. Überprüfen Sie den Inhalt des TrustStore mithilfe des folgenden Befehls:

   ```
   <SiteScope-Stammverzeichnis>\java\bin>keytool -list -keystore <SiteScope-Stammverzeichnis>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass
   ```

```
<ihr_keystore_kennwort<
Keystore type: <Keystore_type>
Keystore provider: <Keystore_provider>
Your keystore contains 2 entries mam, Nov 4, 2004, trustedCertEntry,Certificate
fingerprint (MD5):
<Certificate_fingerprint> amqa_ca, Dec 30, 2010, trustedCertEntry,Certificate
fingerprint (MD5):
<Certificate_fingerprint>
```

Beispiel:

```
C:\SiteScope\java\bin>keytool -list -keystore C:\SiteScope\WEB-
INF\classes\security\MAMTrustStoreExp.jks -storepass logomania

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

mam, Nov 4, 2004, trustedCertEntry,
Certificate fingerprint (MD5):
C6:78:0F:58:32:04:DF:87:5C:8C:60:BC:58:75:6E:F7
amqa_ca, Dec 30, 2010, trustedCertEntry,
Certificate fingerprint (MD5):
5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB
```

5. Kopieren Sie den SiteScope-Client-Keystore aus dem Ordner **<SiteScope-Stammverzeichnis>\templates.certificates** in den Ordner **<SiteScope - Stammverzeichnis>\SiteScope\WEB-INF\classes\security**.

6. Aktualisieren Sie in der Datei **ssl.properties** die Eigenschaft **javax.net.ssl.keyStore** mit dem Keystore-Namen. Beispiel: `javax.net.ssl.keyStore=.ks`.

7. Ändern Sie das Kennwort für den SiteScope-Client-Keystore, sodass es mit dem Discovery-Kennwort für den Keystore identisch ist (der Standardwert ist `logomania`).

   ```
   keytool -storepasswd -new <Discovery_Keystore_Kennwort> -keystore
   <SiteScope-Stammverzeichnis>\WEB-INF\classes\security\.ks -storepass
   <Ihr_Keystore_Kennwort>
   ```

Beispiel:

```
keytool -storepasswd -new logomania -keystore C:\SiteScope\WEB-
INF\classes\security\.ks -storepass changeit
```

8. Ändern Sie das Kennwort für den privaten Schlüssel, sodass es mit dem Discovery-Kennwort für den Keystore identisch ist:

   ```
   keytool -keypasswd -alias sis -keypass <ihr_keystore_kennwort> -new <Discovery-
   Keystore-Kennwort> -keystore <SiteScope-Stammverzeichnis>\WEB-
   INF\classes\security\.ks -storepass <ihr_Keystore-Kennwort>
   ```

   Beispiel:

   ```
   keytool -keypasswd -alias sis -keypass changeit -new logomania -keystore
   C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania
   ```

9. Überprüfen Sie den Keystore mithilfe des neuen Kennworts:

   ```
   keytool -list -v -keystore <SiteScope-Stammverzeichnis>\WEB-
   INF\classes\security\.ks -storepass <ihr_Keystore-Kennwort>
   ```

   Beispiel:

   ```
   keytool -list -v -keystore C:\SiteScope\WEB-INF\classes\security\.ks -
   storepass logomania
   ```

10. Starten Sie den SiteScope-Server neu.

11. Wählen Sie in BSM **Admin > System Availability Management** und klicken Sie auf die Schaltfläche **Neuer SiteScope**, um die SiteScope-Instanz hinzuzufügen. Vergewissern Sie sich im Bereich **Profileinstellungen**, dass das Kontrollkästchen **Für BSM-Front-End HTTPS verwenden** aktiviert ist.

12. Überprüfen Sie, ob die Topologie in der Ansicht **BSM > Admin > RTSM-Verwaltung > IT Universe Manager > System Monitors** angezeigt wird.

Fehlerbehebung

- Überprüfen Sie die Datei **bac-integration.log** im Ordner **<SiteScope-Stammverzeichnis>\logs\bac_integration** auf die folgenden Fehler:

```
2010-12-30 11:03:06,399 [TopologyReporterSender]
(TopologyReporterSender.java:364)
 ERROR - failed to run main topology agent. topologyCommand=TopologyCommand
{commandType=RUN_SCRIPT, …
java.lang.IllegalArgumentException: cannot find script with name=create_
monitor.py
at
com.mercury.sitescope.integrations.bac.topology.dependencies.DependenciesCraw
ler.
findDependencies(DependenciesCrawler.java:60)
at com.mercury.sitescope.integrations.bac.topology.dependencies.
ScriptDependenciesFinder.find(ScriptDependenciesFinder.java:80)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
getDependencies(TopologyReporterSender.java:552)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
send(TopologyReporterSender.java:347)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
run(TopologyReporterSender.java:304)
at java.lang.Thread.run(Thread.java:619)
```

- Überprüfen Sie, ob die Kennwörter für das Zertifikat und den Keystore identisch sind.

Anhang D: Zugreifen auf SiteScope-Reports und die klassische Benutzeroberfläche mit HTTPS

Sie können den SiteScope-Webserver so einrichten, dass eine SSL-Verbindung mit Zugriff über das HTTPS-Protokoll verwendet wird. Im folgenden Abschnitt werden die dazu notwendigen Schritte beschrieben.

Dieser Abschnitt umfasst die folgenden Themen:

Informationen zum Arbeiten mit Zertifikaten in SiteScope

SiteScope wird mit der Datei **Keytool.exe** bereitgestellt. Bei Keytool handelt es sich um ein Dienstprogramm für die Verwaltung von Schlüssel und Zertifikaten. Benutzer können damit ihre eigenen Paare aus privaten und öffentlichen Schlüsseln sowie die dazugehörigen Zertifikate für die Authentifizierung mithilfe digitaler Signaturen verwalten. Außerdem haben Benutzer die Möglichkeit, die öffentlichen Schlüssel anderer Parteien, mit denen sie kommunizieren, zwischenzuspeichern. Der entsprechende Cache befindet sich im Verzeichnis **<SiteScope-Installationspfad>\SiteScope\java\bin**.

Hinweis: Bei dem Verfahren für das Erstellen, Anfordern und Installieren eines digitalen Zertifikats müssen Sie auf jedes Detail achten. Notieren Sie die Parameter und Befehlszeilenargumente, die Sie in jedem Schritt des Verfahrens verwenden, da es sehr wichtig ist, dieselben Werte im gesamten Verfahren zu verwenden.

Sie finden weitere Informationen zu Keytool auf der Website von Sun Microsystems:

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

Verwenden eines Zertifikats von einer Zertifizierungsstelle

Befolgen Sie die folgenden Schritte, um ein digitales Zertifikat zu verwenden, das von einer Zertifizierungsstelle ausgegeben wurde. Um diese Option zu verwenden, benötigen Sie ein digitales

Zertifikat, das sich in die von Keytool verwendete Schlüsselspeicherdatei importieren lässt. Falls Ihr Unternehmen derzeit nicht über ein digitales Zertifikat für diesen Zweck verfügt, müssen Sie die Ausgabe eines Zertifikats bei einer Zertifizierungsstelle anfordern.

So verwenden Sie ein Zertifikat von einer Zertifizierungsstelle:

1. Entfernen Sie die Datei **serverKeystore**, die sich im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** befindet. Sie können sie löschen oder einfach in ein anderes Verzeichnis verschieben.

   Hinweis: Die Datei muss entfernt werden, bevor Sie die unten aufgeführten Schritte durchführen.

2. Anschließend müssen Sie ein Schlüsselpaar erstellen. Führen Sie dazu den unten aufgeführten Befehl aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** aus.

   Hinweis: Bei den kursiv dargestellten Werten handelt es sich um Variablen, die Sie mit spezifischen Informationen zu Ihrem Unternehmen füllen.

   Dieser und alle anderen Befehle müssen in einer Zeile eingegeben werden. Die Zeile ist hier aus Platzgründen aufgeteilt.

   ```
   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
   O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias
   yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass
   passphrase -keyalg "RSA" -validity valdays
   ```

   Mit diesem Befehl wird eine Datei namens **serverKeystore** im Verzeichnis **SiteScope\groups** erstellt. SiteScope verwendet diese KeyStore-Datei, um die in Ihren sicheren Sitzungen verwendeten Zertifikate zu speichern. Stellen Sie sicher, dass Sie eine Sicherungskopie dieser Datei an einem anderen Speicherort aufbewahren.

   Der Wert einer **-dname**-Option muss die folgende Reihenfolge aufweisen, wobei die kursiv geschriebenen Werte durch Werte Ihrer Wahl ersetzt werden. Die Schlüsselwörter sind Abkürzungen für folgende Werte:

   CN = commonName – Allgemeiner Name einer Person (Beispiel: "Peter Mustermann")

   OU = organizationUnit – Kleine Organisationseinheit (Beispiel: "NetAdmin")

   O = organizationName – Name eines Großunternehmens (Beispiel: "ACMe-Systems GmbH")

L = localityName - Name eines Ortes (einer Stadt) (Beispiel: "Dortmund")

S = stateName – Name eines Bundeslands oder Kantons (Beispiel: "Nordrhein-Westfalen")

C = country – Länderkennzahl aus zwei Buchstaben (Beispiel: "DE")

- Bei den Unterkomponenten innerhalb der **-dname**-Variable (Zeichenfolge mit definiertem Namen) muss die Groß- oder Kleinschreibung sowie die Reihenfolge berücksichtigt werden, auch wenn Sie nicht alle Unterkomponenten verwenden müssen. Die **-dname**-Variable sollte Ihr Unternehmen darstellen. **CN** ist der Domänenname des Webservers, auf dem SiteScope installiert ist.
- Der Wert von **-storepass** ist ein Kennwort, das zum Schutz der KeyStore-Datei verwendet wird. Dieses Kennwort muss mindestens 6 Zeichen lang sein. Sie benötigen dieses Kennwort, um Zertifikatdaten aus der KeyStore-Datei zu importieren und zu entfernen.
- Bei der **-alias**-Variable handelt es sich um einen Alias oder Spitznamen, über den Sie einen Eintrag im Keystore identifizieren können.

3. Erstellen Sie eine Zertifikatanforderungsdatei. Führen Sie den folgenden Befehl ebenfalls aus dem Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** aus.

   ```
   keytool -certreq -alias yourAlias -file ..\..\groups\filename.csr -keypass
   keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg
   "RSA"
   ```

   Mit diesem Befehl wird eine .csr-Datei erstellt, die als Anforderungsdatei verwendet werden soll. Sie müssen diese Datei zusammen mit der Zertifkatanforderung an eine Zertifizierungsstelle (CA) senden. Wenn Sie Ihr Zertifikat von einer Zertifizierungsstelle erhalten haben (die Antwort sollte eine Datei mit dem Namen **cert.cer** enthalten) müssen Sie das Zertifikat in die KeyStore-Datei importieren, die Sie anhand der vorhergehenden Schritte erstellt haben. Die Datei sollte den Namen **serverKeystore** haben. Verwenden Sie die folgenden Schritte zum Importieren des Zertifikats.

4. Führen Sie zum Importieren der Zertifikatdaten in die KeyStore-Datei den folgenden Befehl aus dem Verzeichnis **SiteScope\java\bin** aus:

   ```
   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore
   ..\..\groups\serverKeystore
   ```

5. Um SiteScope so zu ändern, dass eine gesicherte Verbindung verwendet wird, müssen Sie die

folgenden Parameter in der Datei **<SiteScope-Stamm>\groups\master.config** hinzufügen oder ändern

```
_httpSecurePort=8899
```

Der Wert für den Parameter **_httpSecurePort** kann auf eine beliebige verfügbare Portnummer festgelegt werden. Es wird empfohlen, eine andere Portnummer als 8888 zu verwenden, die den Standardport für den Zugriff auf SiteScope mit HTTP (nicht gesichert) darstellt.

Um nur mit HTTPS auf SiteScope zuzugreifen, müssen Sie die folgenden Parameter in der Datei **master.config** wie weiter unten gezeigt ändern, sodass die entsprechenden Werte für die kursiv angezeigten Elemente ersetzt werden:

_httpPort=

_httpSecurePort=8899

_httpSecureKeyPassword=passphrase

_httpSecureKeystorePassword=keypass

> **Hinweis:** Bei allen Parametern in der Datei **master.config** muss die Groß-/Kleinschreibung und die Syntax beachtet werden. Stellen Sie sicher, keine extra Leerzeichen oder Zeilen in die Datei einzufügen.

6. Speichern Sie die Änderungen in der Datei **master.config**.
7. Beenden Sie den SiteScope-Dienst und starten Sie ihn erneut, damit die Änderungen wirksam werden.

Sie sollten nun mit HTTP auf SiteScope zugreifen können, beispielsweise innerhalb einer Firewall, indem Sie die folgende Standardadresse verwenden:

```
http://Server-IP-Adresse:8888
```

Sie sollten auf SiteScope zugreifen können, indem Sie HTTPS unter der folgenden Adresse verwenden und die Schritte aus dem oben genannten Beispiel beachten:

```
https://Server-IP-Adresse:8899
```

Verwenden eines selbstsignierten Zertifikats

Alternativ können Sie ein selbstsigniertes Zertifikat generieren. Verwenden Sie dazu die **-selfcert**-Option, damit das Keytool-Dienstprogramm ein selbstsigniertes Zertifikat generiert.

So verwenden Sie ein selbstsigniertes Zertifikat:

1. Entfernen Sie die Datei **serverKeystore**, die sich im Verzeichnis **<SiteScope-Stammverzeichnis>\groups** befindet. Sie können sie löschen oder einfach in ein anderes Verzeichnis verschieben.

   Hinweis: Die Datei muss entfernt werden, bevor Sie die unten aufgeführten Schritte durchführen.

2. Führen Sie als nächstes den folgenden Befehl im Verzeichnis **<SiteScope-Stammverzeichnis>\java\bin** aus.

   Hinweis: Bei den kursiv dargestellten Werten handelt es sich um Variablen, die Sie mit spezifischen Informationen zu Ihrem Unternehmen füllen.

   Dieser und alle anderen Befehle müssen in einer Zeile eingegeben werden. Die Zeile ist hier aus Platzgründen aufgeteilt.

   ```
   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
   O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias
   yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass
   passphrase -keyalg "RSA" -validity valdays
   ```

3. Führen Sie als nächstes den folgenden Befehl ebenfalls im Verzeichnis **SiteScope\java\bin** aus.

   ```
   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -
   dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName,
   L=yourLocation, S=yourState, C=yourCountryCode" -keystore
   ..\..\groups\serverKeystore
   ```

4. Um SiteScope so zu ändern, dass eine gesicherte Verbindung verwendet wird, müssen Sie die folgenden Parameter in der Datei **<SiteScope-Stamm>\groups\master.config** hinzufügen oder ändern

   ```
   _httpSecurePort=8899
   ```

Der Wert für den Parameter **_httpSecurePort** kann auf eine beliebige verfügbare Portnummer festgelegt werden. Es wird empfohlen, eine andere Portnummer als 8888 zu verwenden, die den Standardport für den Zugriff auf SiteScope mit HTTP (nicht gesichert) darstellt.

Um nur mit HTTPS auf SiteScope zuzugreifen, müssen Sie die folgenden Parameter in der Datei **master.config** wie weiter unten gezeigt ändern, sodass die entsprechenden Werte für die kursiv angezeigten Elemente ersetzt werden:

_httpPort=

_httpSecurePort=8899

_httpSecureKeyPassword=passphrase

_httpSecureKeystorePassword=keypass

Hinweis: Bei allen Parametern in der Datei **master.config** muss die Groß-/Kleinschreibung und die Syntax beachtet werden. Stellen Sie sicher, keine extra Leerzeichen oder Zeilen in die Datei einzufügen.

5. Speichern Sie die Änderungen in der Datei **master.config**.
6. Beenden Sie den SiteScope-Dienst und starten Sie ihn erneut, damit die Änderungen wirksam werden.

Sie sollten nun, beispielsweise innerhalb einer Firewall, mit HTTP auf SiteScope zugreifen können, indem Sie die folgende Standardadresse verwenden:

`http://Server-IP-Adresse:8888`

Sie sollten auf SiteScope zugreifen können, indem Sie HTTPS unter der folgenden Adresse verwenden und die Schritte aus dem oben genannten Beispiel beachten:

`https://Server-IP-Adresse:8899`

Senden von Feedback zur Dokumentation

Wenn Sie Anmerkungen zu diesem Dokument haben, können Sie sich per E-Mail an das Dokumentationsteam wenden. Wenn auf diesem System ein E-Mail-Client konfiguriert ist, klicken Sie auf den Link oben. Dann wird ein E-Mail-Fenster mit folgenden Informationen in der Betreffzeile geöffnet:

Feedback zu Handbuch zur Bereitstellung (SiteScope 11.30)

Geben Sie Ihr Feedback einfach in die E-Mail ein und klicken Sie auf **Senden**.

Ist kein E-Mail-Client verfügbar, kopieren Sie die oben genannten Informationen in eine neue Nachricht in einem Webmail-Client und senden Sie Ihr Feedback an SW-doc@hp.com.

Wir freuen uns über Ihr Feedback!