Einleitung

SAP HANA hat sich von einer reinen Datenbank zu einer mächtigen Applikation entwickelt, auf der u. a. auch umfangreiche Eigenentwicklungen möglich sind. Daher sind die Anforderungen an die Sicherheit von SAP HANA stark gestiegen. Ich hoffe, dass dieses Buch für alle, die mit der Sicherheit von SAP HANA befasst sind, eine hilfreiche Unterstützung ist.

Nachdem ich im Juni 2018 mein Buch »Sicherheit und Prüfung von SAP-Systemen« (den Nachfolger der OPSAP-Reihe) beim Rheinwerk Verlag veröffentlicht hatte, kam dieser bezüglich einer Veröffentlichung zum Thema Sicherheit von SAP-HANA-Datenbanken auf mich zu. Da ich mich bereits seit 2013 mit diesem Thema befasse und mein Wissen dazu aufgrund laufender Projekte und Seminarleitungen ständig auf dem aktuellen Stand halte, habe ich (fast) sofort zugesagt. Somit schloss sich für mich das nächste Buchprojekt gleich an.

Eine Herausforderung war, entsprechende Systeme zum Testen und für die Recherchen zu finden. Die IBS Schreiber GmbH hat verschiedene SAP-HANA-Datenbanken zu Testzwecken installiert, die ich hierfür nutzen konnte. Des Weiteren hatte ich die Möglichkeit, Kundensysteme im Live-Betrieb zu sichten und Interviews mit den verantwortlichen Administratoren zu führen. Hierdurch konnte ich einen tiefen Einblick in das Tagesgeschäft gewinnen, insbesondere in die Anforderungen in Bezug auf die Systemsicherheit.

Die maßgebliche Zielgruppe dieses Buches sind die SAP-HANA-Administratoren. Zu allen Themen beschreibe ich jeweils deren Konfiguration und Umsetzung. Dabei gehe ich sowohl auf das SAP HANA Cockpit als auch auf das SAP HANA Studio ein. In der Praxis wird Letzteres häufig noch eingesetzt, auch wenn neue Funktionen von SAP HANA oft als Oberfläche nur noch im SAP HANA Cockpit verfügbar gemacht werden.

Aber auch alle, die sich mit der Sicherheit von SAP-Systemen befassen oder dafür verantwortlich sind, finden in diesem Buch hilfreiche Hinweise. Ich gehe insbesondere in Kapitel 12, »Checklisten zur Analyse der Sicherheit von SAP HANA«, zu jedem Punkt auf das jeweilige Risiko ein, das sich daraus ableitet. Daher richtet sich dieses Buch sowohl an alle, die für die Sicherheit der SAP-Systeme verantwortlich sind, als auch an diejenigen, die durch Prüfungen die Sicherheit analysieren und bewerten.

Inhalt des Buches

In **Kapitel 1**, »Einführung in SAP HANA«, stelle ich Ihnen den Aufbau von SAP HANA vor. Dies umfasst auch die Tools, die zur Verwaltung und Analyse von SAP HANA genutzt werden können: das SAP HANA Cockpit, den SAP HANA Database Explorer, das SAP HANA Studio, das Programm hdbsql und das DBA Cockpit des SAP NetWeaver. Des Weiteren gehe ich auf die Entwicklungsumgebung des SAP HANA XSA (SAP HANA Extended Application Services, Advanced Model) ein. Auch die Besonderheiten beim Einsatz von SAP S/4HANA oder SAP ERP zeige ich auf. Im letzten Abschnitt stelle ich Ihnen die Leitfäden zu SAP HANA vor, die Sie für weitere Informationen zu den jeweiligen SAP-HANA-Release-Ständen nutzen können.

Kapitel 2, »Netzwerk- und Betriebssystemsicherheit«, zeigt die Sicherheit der Betriebssystemebene UNIX für SAP HANA auf. Da hier viele sicherheitsrelevante Daten gespeichert werden (u. a. die persistenten Daten, die Systemparameter und die Root-Keys für die Verschlüsselungen), ist es in die Sicherheitsbetrachtung mit einzubeziehen. Hier erfahren Sie, wie Sie die Standardbenutzer absichern, die Dateien und Verzeichnisse schützen und wo die Log-Dateien von UNIX gespeichert werden. Außerdem zeige ich Ihnen auf, wie Sie vom SAP NetWeaver aus auf die Betriebssystemebene zugreifen und diese Zugriffe absichern können.

In **Kapitel 3**, »Systemsicherheit in SAP HANA«, werden dann grundsätzliche Aspekte der Systemsicherheit behandelt. Dies beginnt mit der Lizenzierung von SAP HANA und der Verwaltung der Systemparameter. Ein wesentlicher Sicherheitsaspekt ist natürlich die Verschlüsselung der Daten und der Kommunikation, auf die ich hier eingehe. Dazu gehören auch die Schnittstellen, die Remote Sources, und deren Absicherung. Im letzten Abschnitt stelle ich Ihnen zwei Skripte aus der Statement Library vor, die für Sicherheitsanalysen genutzt werden können.

Seit SAP HANA Release 2.0 SPS1 werden nur noch Multi-Tenant-Datenbanken unterstützt. Auf deren Sicherheitsaspekte gehe ich in **Kapitel 4**, »Sicherheit in Multi-Tenant-Datenbanken«, ein. Hier erfahren Sie, wie Sie tenant-übergreifende Zugriffe einrichten bzw. absichern können. Um die tenant-spezifischen Daten auf der Betriebssystemebene abzusichern, kann das Isolation Level »high« eingerichtet werden. Wie dies installiert wird, zeige ich hier ebenfalls auf.

Die Absicherung des Anmeldevorganges stellt eines der wesentlichen Elemente für die Sicherheit eines jeden IT-Systems dar. In SAP HANA können Sie verschiedene Authentifizierungsmethoden nutzen, die ich Ihnen in **Kapitel 5**, »Authentifizierung in SAP HANA«, vorstelle. Des Weiteren können Kennwortrichtlinien eingerichtet werden, sowohl tenant-weit gültig als auch benutzergruppenspezifisch.

Ein zentrales Thema der SAP-Sicherheit ist die Benutzerverwaltung, die in **Kapitel 6**, »Benutzerverwaltung in SAP HANA«, behandelt wird. Dort gehe ich in den ersten

Abschnitten auf die Benutzerstammsätze in SAP HANA und SAP HANA XSA ein. Ein weiterer Schwerpunkt liegt auf der Absicherung der Standardbenutzer. Außerdem erfahren Sie hier, wie Sie Remote-Benutzer für tenant-übergreifende Zugriffe nutzen und absichern können. Im letzten Abschnitt gehe ich auf die Nutzung der Benutzergruppen ein.

Die Beschreibung und Analyse des SAP HANA Berechtigungskonzeptes habe ich aufgrund der Komplexität auf drei Kapitel aufgeteilt. In **Kapitel 7**, »Das Berechtigungskonzept von SAP HANA«, beschreibe ich das Konzept der SAP-HANA-Berechtigungen und stelle die verschiedenen Privileges vor. Auch auf die Funktionalitäten der Weitergabe von Berechtigungen, der Maskierung von Daten und der Möglichkeiten (und Einschränkungen) des Kopierens von Berechtigungen gehe ich ein. Eine weitere sehr wesentliche Funktion ist der Berechtigungs-Trace, der in SAP HANA natürlich auch verfügbar ist. Im letzten Abschnitt erläutere ich die Berechtigungen in SAP HANA XSA.

Kapitel 8 befasst sich mit dem Rollenkonzept von SAP HANA. Im ersten Abschnitt finden Sie u. a. einen Vorschlag für eine Namenskonvention der Rollen. In den weiteren Abschnitten stelle ich Ihnen die drei verschiedenen Arten von Rollen vor, die Runtime-Katalogrollen, die Design-Time-Repository-Rollen (XSC) und die Design-Time-HANA-DI-Rollen (XSA). Der letzte Abschnitt beschreibt einige SAP-HANA-Standard-Rollen.

In **Kapitel 9**, »Analyse des SAP-HANA-Berechtigungskonzepts«, beschreibe ich, wie SAP-HANA-Berechtigungen analysiert werden können. Dies ist mit verschiedenen Views oder auch mit einem Skript aus der Statement Library möglich. Im letzten Abschnitt liste ich wesentliche Fragestellungen für Berechtigungsanalysen auf.

Kapitel 10 befasst sich mit dem SAP-S/4HANA-Berechtigungskonzept. Hier gehe ich im ersten Abschnitt auf die wesentlichen Aspekte beim Umstieg von SAP ERP auf SAP S/4HANA ein. Danach zeige ich speziell die Berechtigungen beim Einsatz von SAP-Fiori-Apps auf.

Im Gegensatz zu SAP ERP bzw. SAP S/4HANA, wo wesentliche Protokollierungen bereits fest implementiert sind, muss in SAP HANA die Protokollierung system- und unternehmensspezifisch grundlegend konfiguriert werden. Dies beschreibe ich in **Kapitel 11**, »Auditing in SAP HANA«. Die ersten Abschnitte erläutern die Konfiguration und die Auswertungsmöglichkeiten des SAP HANA Auditings. Beim Einsatz von SAP HANA XSA kommen andere Protokolle zum Einsatz, worauf ich ebenfalls eingehe. Im letzten Abschnitt erhalten Sie Best-Practice-Empfehlungen zur Einrichtung der Protokollierung in SAP HANA.

Kapitel 12 ist eine umfassende Checkliste für die Analyse der Sicherheit von SAP HANA. Zu jedem Punkt sind die Risiken sowie die praktische Vorgehensweise zur Analyse beschrieben. Dies erlaubt es auch Personen, die nicht täglich mit SAP HANA arbeiten, die jeweiligen Analyseschritte sofort auszuführen.

Danksagung

Ich bedanke mich bei allen, die mir im Umfeld der Fertigstellung dieses Buches geholfen haben:

- beim Rheinwerk Verlag, der mich durch seine Anfrage zum Schreiben dieses Buches angeregt hat
- bei Maike Lübbers für das sehr gute Lektorat
- bei der IBS Schreiber GmbH für die Nutzung der SAP-HANA-Systeme für Recherchen und Screenshots
- bei allen Kunden, deren Systeme ich im Rahmen der Recherchen für dieses Buch analysieren durfte
- bei meiner Frau Kristin, die das Buch Korrektur gelesen hat

Und zu guter Letzt möchte ich wieder an alle Leser appellieren, mir jegliche positive und negative Kritik sowie Anregungen für weitere Themen zukommen zu lassen. Schreiben Sie mir gern an *thomas.tiede@ibs-schreiber.de*.

Thomas Tiede
Hamburg im Mai 2019