Evaluation of Mandatory Access Control for Database Management Systems on the Linux Platform

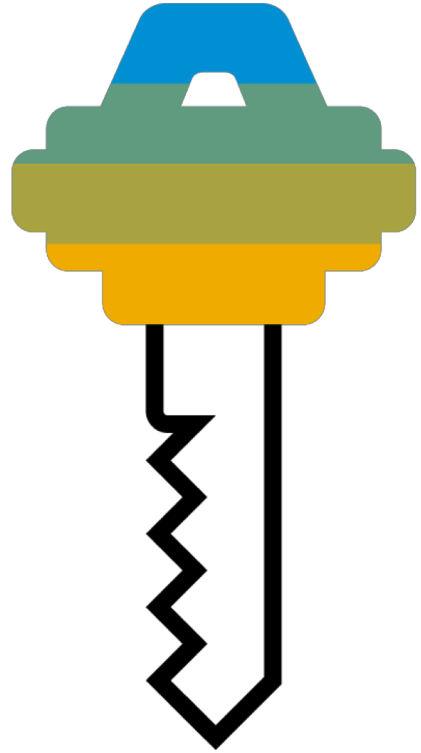
Felix Lange, Kim-Thomas Rehmann und Helge Deller, SAP SE
October 19th , 2018

PUBLIC

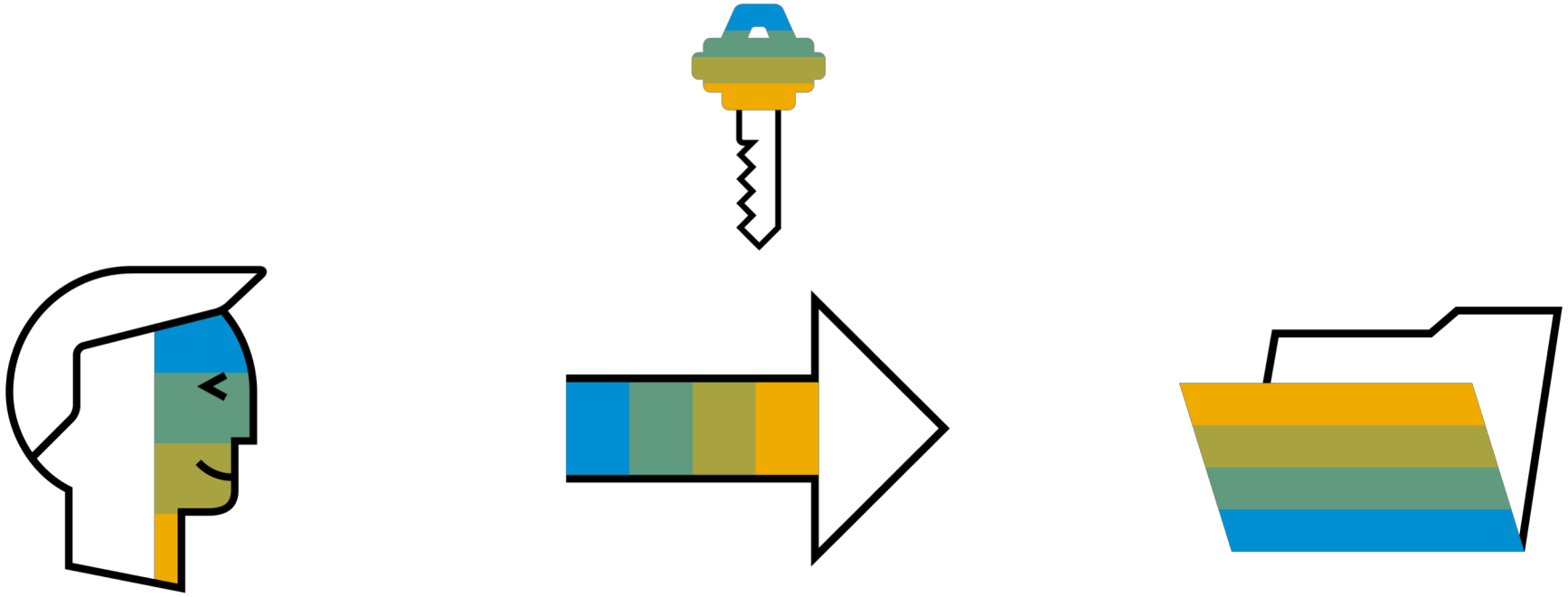
Agenda

- Access Control Paradigmen und das SAP HANA DBMS
- Evaluierung des HANA DBMS mit MAC Lösungen
- Ergebnisse der Evaluierung und Zusammenfassung

Hintergründe
Access Control Paradigmen



AC Paradigmen – Discretionary Access Control (DAC)



Metadaten &
Dateisystem

AC Paradigmen – Mandatory Access Control (MAC)

AC Paradigmen – Vorteile von MAC

Sicherheit

- Granulare und zielgerichtete Rechtevergabe
- Kontrolle über Informationsfluss
- Manipulationssicheres Berechtigungskonzept

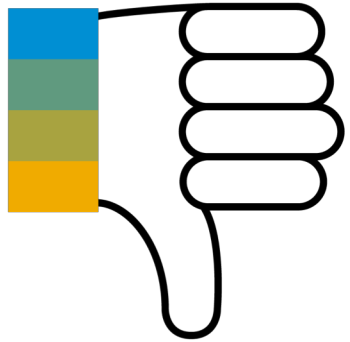
Kontext

- Berechtigungen an Programme vergeben
- Rollenbezogene Ansätze integriert
- Transparentere („sprechende“) Berechtigungen

AC Paradigmen – Nachteile von MAC

Aufwand

- Hoher Entwicklungsaufwand
- Hohes Fehlerpotential
- Komplizierte Wartung
- Sicherheitspolitiken sehr Einsatzbezogen



Kontext

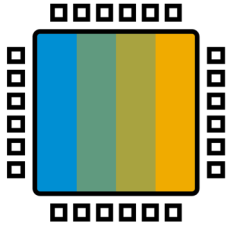
- Fokus liegt auf Schutz der Systemressourcen, nicht der Anwendungsobjekte
- Deren Einbindung ist möglich, aber komplex

Hintergründe
SAP HANA 2

Hintergründe – SAP HANA 2

Architektur

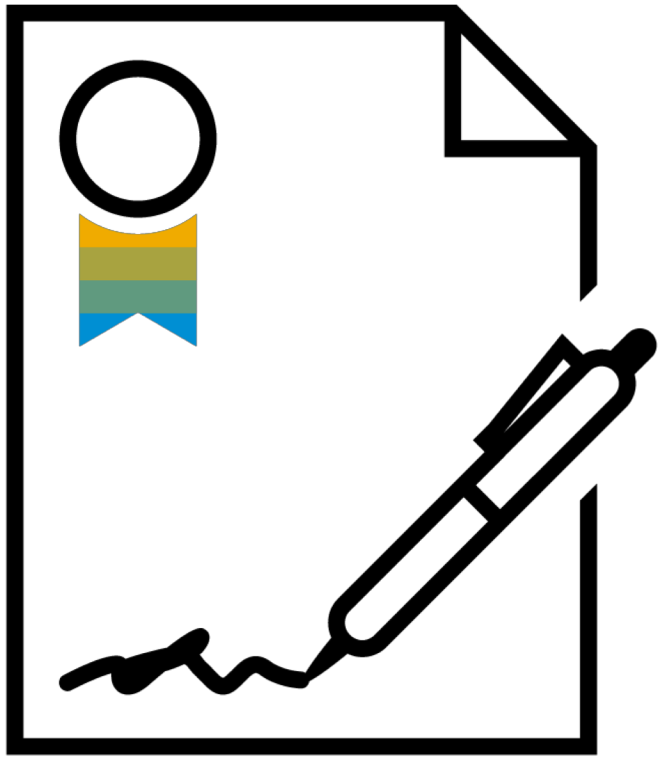
- In-Memory Datenbank Management System
- Ausgeführt auf der Linux Plattform
- Enthält u.a. mehrere Daten-engines und die HANA DB



Geschäftsziele

- Schnelle, verlässliche und skalierbare Datenbank
- Besonderer Fokus auf analytischen Aufgaben (SOLTP, TPC)
- Basis neuer SAP Anwendungen (ERP, CRM, etc.)

Hintergründe
Geschäftskontext



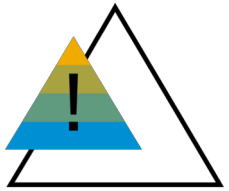
Hintergründe – Geschäftskontext

Gründe für MAC

- Offizielle Anforderungen einzelner Geschäftsfelder
- Best Practices einzelner Wirtschaftssektoren
- Verbesserte Sicherheit gegenüber DAC durch genauere Zugriffskontrolle

SAPs Status

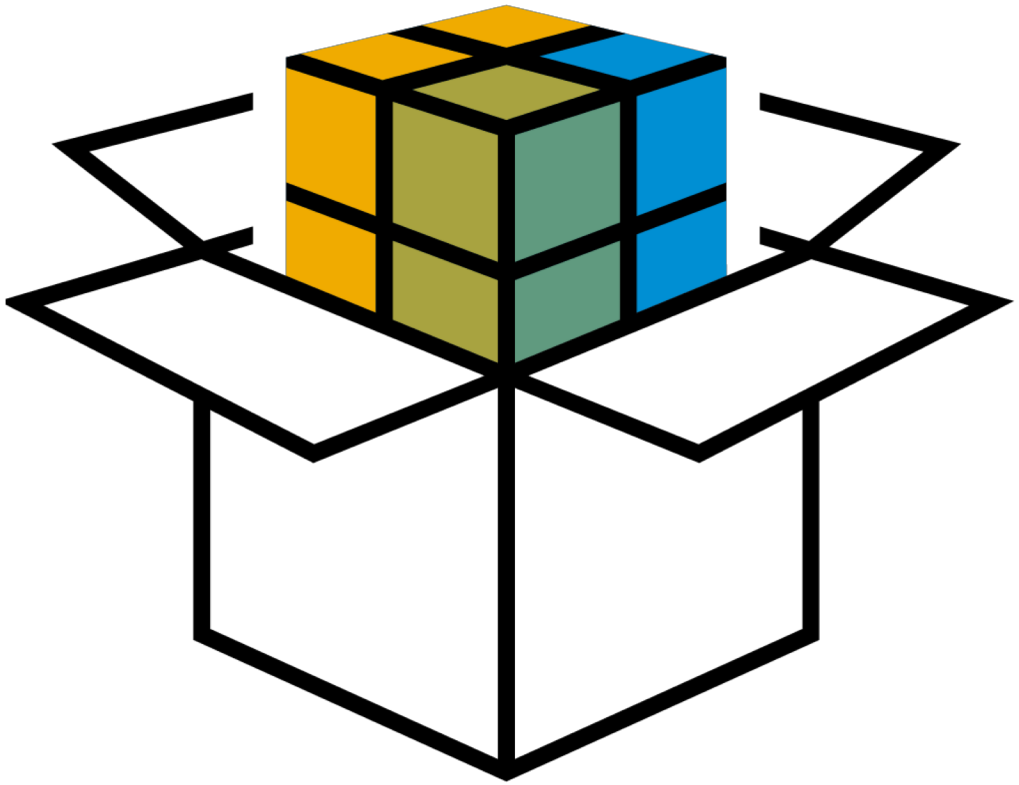
- Betriebssystemanforderungen für SAP HANA untersagen die Aktivierung von SELinux & AppArmor
- SAP Blogs dokumentieren frühere Versuche
- Externe Blogger kritisieren SAPs Entscheidung stark



“Können wir SAP HANA mit MAC ermöglichen?”

Evaluierungsprozess

Betrachtete MAC Implementierungen

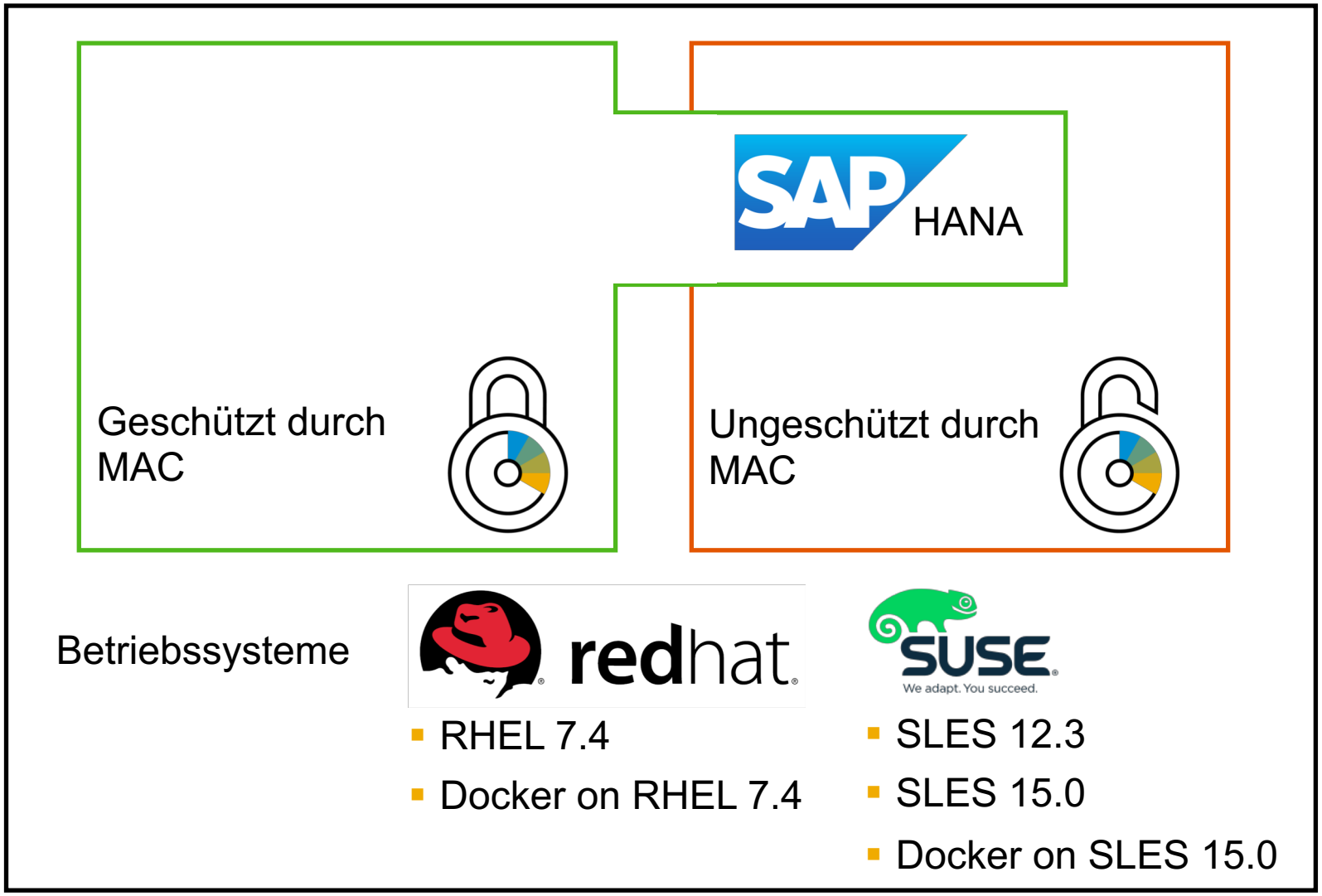


Evaluierung von HANA mit MAC – Implementierungen im Fokus

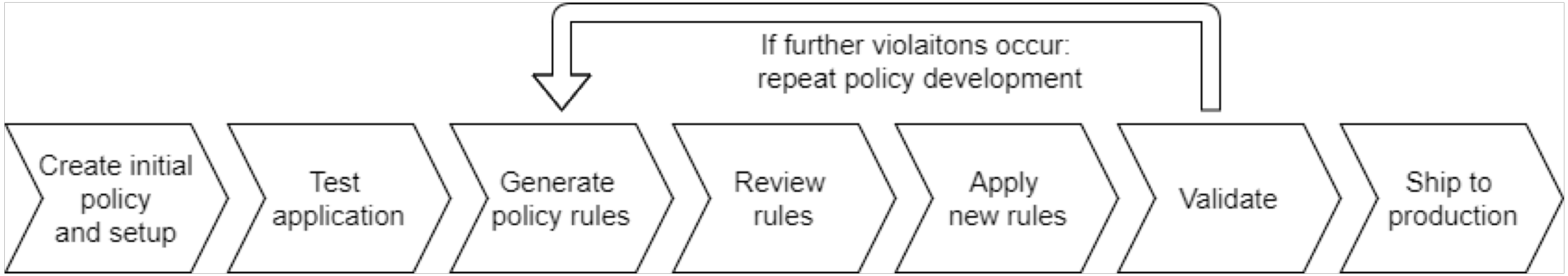
- AppArmor
  - Geringerer Funktionsumfang
  - Verfügbar auf SLES
  - Pfadbasiert
  - Anwendungsbezogene Profile
  - Einfache Handhabung

- SELinux
  - Größerer Funktionsumfang
  - Verfügbar auf SLES und RHEL
  - Basiert auf erweiterten Dateiattributen
  - Betriebssystemweite Sicherheitspolitik
  - Komplexere Handhabung

Evaluierung von HANA mit MAC – Implementierungsziel



Evaluierung von HANA mit MAC – Implementierungsablauf einer Policy

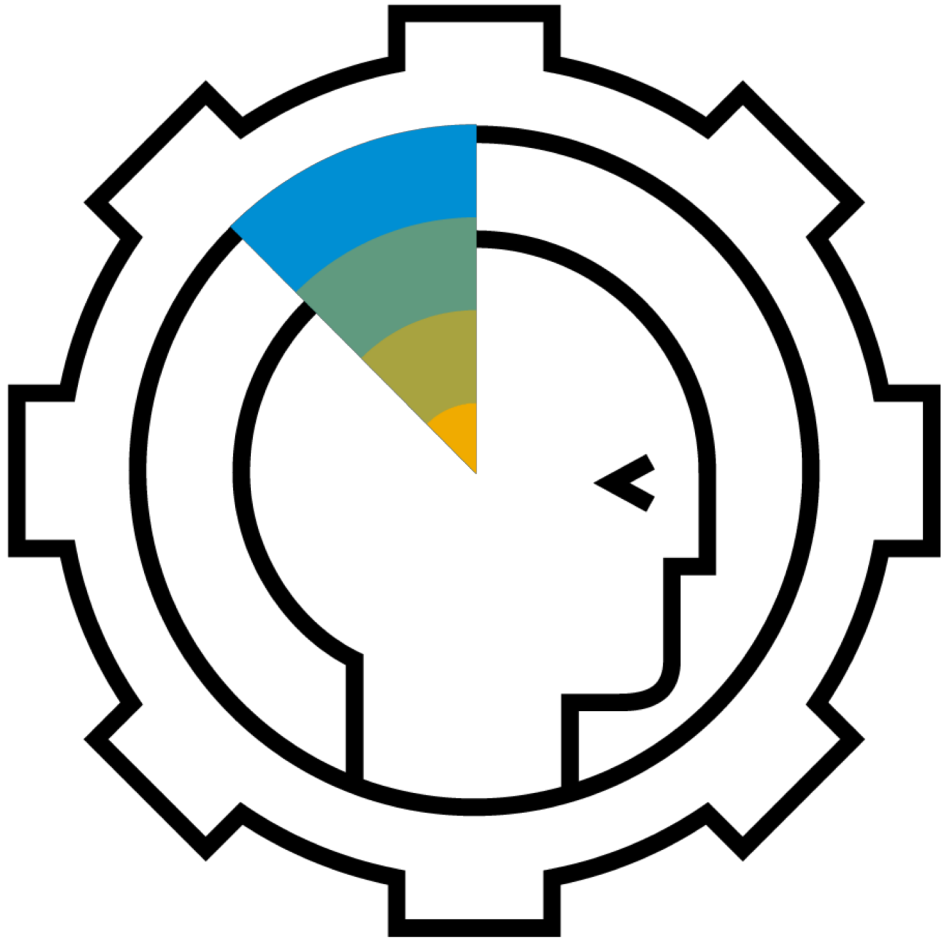


Evaluierung von HANA mit MAC – Implementierungsmatrix

OS Plattform	AppArmor	SELinux
RHEL 7.4	Nicht unterstützt	Ja
RHEL 7.4 + Docker	Nicht unterstützt	Zur Verfügung gestellt
SLES 12.3	Ja	Ja
SLES 15.0	Ja	Ja
SLES 15.0 + Docker	Teilweise bereits verfügbar	Teilweise bereits verfügbar, Eigene Entwicklungen, Kein MCS support

Evaluationsansatz

Vorgehen in der Analyse



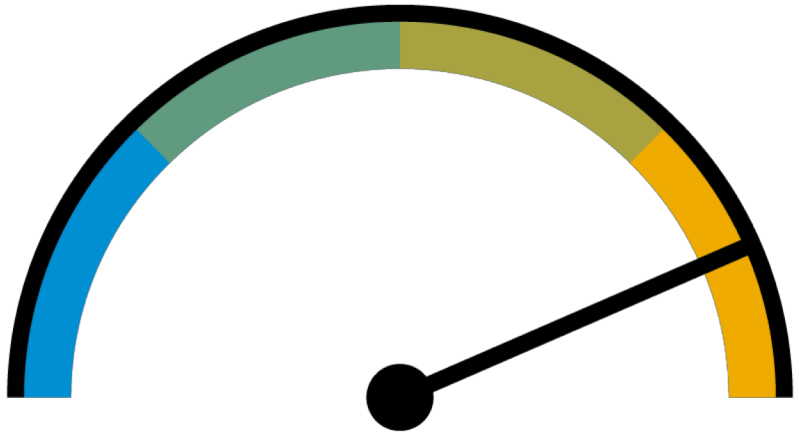
Evaluierung von HANA mit MAC – Vorgehen in der Analyse

- Leistungsanalyse
  - Basierend auf einzelnen Tests, die Geschäftsumfeld simulieren (SOLTP, TPC, etc.)
  - Tests je mehrfach ausgeführt
    - 100x für SELinux
    - 50x für AppArmor
  - Analyseergebnisse
    - Als Boxplots, Histogramme und Durchschnitte
    - Signifikanteste Ergebnisse einer weitergehenden Analyse unterzogen

- Sicherheitsanalyse
  - Sicherheitspolitiken manuell analysiert
  - Analyse verwendeter Drittsoftware (Abhängigkeiten)
  - Analyse der MAC Implementierungen (Hinsichtlich ihrer Fähigkeiten)

Evaluationsresultate

Leistung



Evaluationsresultate - Leistung

Folieninhalt nicht öffentlich freigegeben

Evaluationsresultate
Sicherheit

Evaluationsresultate - Sicherheit

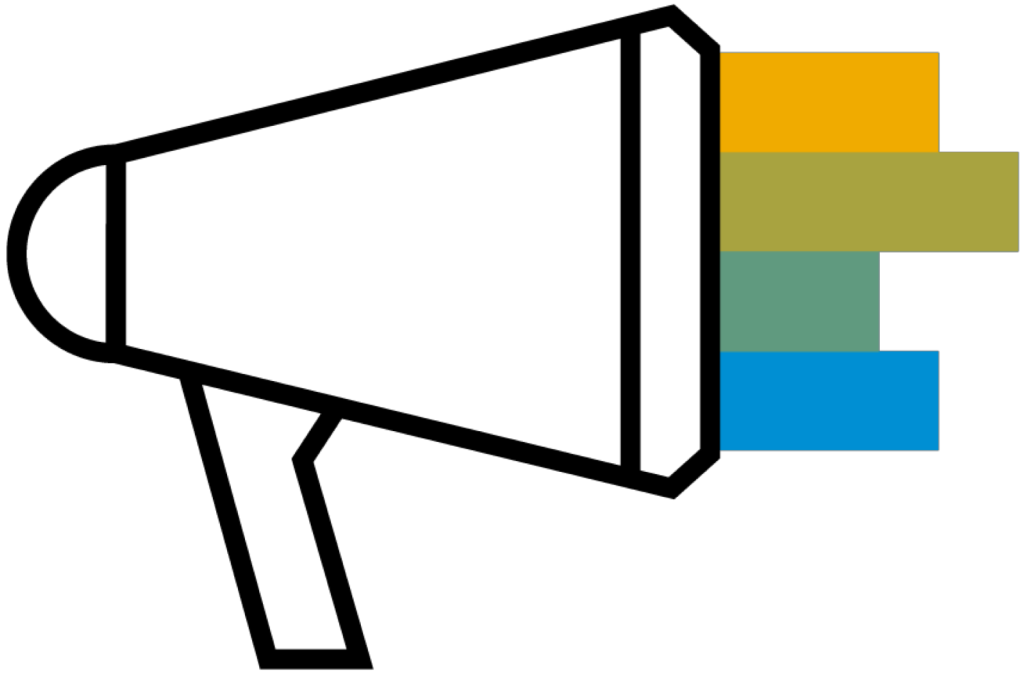
SELinux

- Sicherheitsvorteil bei nativer Anwendung
- Sicherheitsvorteil in Verbindung mit Docker von Umgebung abhängig
  - RHEL: wird vom Hersteller geliefert und als sicher angenommen
  - SLES: MCS nicht verfügbar

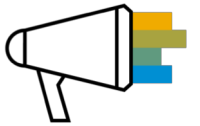
AppArmor

- Sicherheitsvorteil bei nativer Anwendung
- Sicherheitsvorteil in Verbindung mit Docker von Sicherheitspolitik abhängig
  - Docker Default: nahezu kein Vorteil
  - Vollständig eigenes Profil: Erhöht Sicherheit, ist aber hochgradig spezifisch
  - Mischen verschiedener Profile: Schwächt Containersicherheit

Evaluationsresultate
Zusammenfassung



Evaluationsresultate – Zusammenfassung



Ergebnis des Projektes

- Verwendung von HANA mit MAC ist möglich
- ABER
  - Hoher Entwicklungs- und Wartungsaufwand
  - Tatsächlich sichere Sicherheitspolitiken sind Einsatzspezifisch
  - Daher (aktuell) keine universelle Lösung
- Resultierende Produktentscheidung
  - Das Projekt war ein interner Prototyp
  - Aktuell wird daher HANA mit MAC weiterhin nicht unterstützt

Zukünftige Schritte

- Untersuchung möglicher Supportszenarien
- Untersuchung anderer Anwendungsfälle für MAC mit SAP Software

Vielen Dank.

Kontaktdaten:

Felix Lange
IT Security Analyst
SAP Customer Experience

Disclaimer

Die Informationen in dieser Präsentation sind vertraulich und urheberrechtlich geschützt und dürfen nicht ohne Genehmigung von SAP offengelegt werden. Diese Präsentation unterliegt weder Ihrem Lizenzvertrag noch einer anderen Service- oder Subskriptionsvereinbarung mit SAP. SAP ist in keiner Weise verpflichtet, in dieser Präsentation oder einem dazugehörigen Dokument dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen.

Diese Präsentation oder jedes dazugehörige Dokument über die Strategie von SAP und mögliche zukünftige Entwicklungen, Ausrichtungen und Funktionen von Produkten und/oder Plattformen kann von SAP jederzeit aus beliebigen Gründen ohne vorherige Ankündigung geändert werden. Die Informationen in dieser Präsentation stellen keinerlei Zusage, Versprechen oder rechtliche Verpflichtung zur Auslieferung von Materialien, Code oder Funktionen dar. Diese Präsentation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt insbesondere, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung geltenden Rechts. Diese Präsentation dient zu Informationszwecken und darf nicht in einen Vertrag eingebunden werden. SAP übernimmt keine Verantwortung für Fehler oder Unvollständigkeiten in dieser Präsentation, es sei denn, solche Schäden wurden von SAP vorsätzlich oder grob fahrlässig verursacht. Sämtliche vorausschauenden Aussagen unterliegen verschiedenen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können.

Die vorausschauenden Aussagen geben die Sicht zu dem Zeitpunkt wieder, zu dem sie getätigt wurden. Dem Leser wird empfohlen, diesen Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.