IT資格道場

AZ-120 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

AZ-120 出題範囲(Microsoft Learn 公式 Study guide・Skills measured as of April 17, 2026)準拠
2026年11月版

SAMPLE

© IT資格道場｜無料サンプル｜転載・再配布・AI学習利用禁止

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

SAMPLE

目次

この試験の範囲 [overview]

- 想定読者
- 試験の基本情報
- このテキストの構成と読み方
- 出題範囲(Skills measured)と配点

第1章 Migrate SAP workloads to Azure
[1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.1.7/1.1.8/1.1.9/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6/1.3.1/1.3.2/1.3.3/1.3

- SAP ワークロードのターゲット サイズを見積もる [1.1.1]
- Azure でサポートされる SAP の構成を知る [1.1.2]
- SAP の層ごとの計算、ストレージ、ネットワークの要件 [1.1.3]
- クォータと提供状況を確かめる [1.1.4]
- OS、SAP、DB のライセンス [1.1.5]
- 費用の要素と見積もりの道具 [1.1.6]
- Azure のサポート プランと SAP のサポート [1.1.7]
- 移行方式を選ぶ [1.1.8]
- 移行の道具と段取り [1.1.9]
- Azure RBAC とロールの割り当て [1.2.1]
- Azure Policy でガバナンスを効かせる [1.2.2]
- SAP のシングル サインオン：NetWeaver、Fiori、SAP GUI [1.2.3]
- SAP の SaaS と Microsoft Entra ID [1.2.4]
- 管理グループとリソースの階層設計 [1.2.5]
- SAP 向けのランディング ゾーン [1.2.6]
- RISE with SAP の責任分担と接続方式 [1.3.1]
- RISE との VNet ピアリングの実装、名前解決、オンプレミス [1.3.2]
- RISE の SAP と顧客の Azure サービスをつなぐ [1.3.3]
- SAP データを Azure のデータ サービスへ [1.3.4]
- RISE と Microsoft Entra ID、Microsoft Sentinel、顧客のセキュリティ [1.3.5]

サンプルはここまでです

SAMPLE

この試験の範囲 [overview]

このテキストは、**Microsoft Certified: Azure for SAP Workloads Specialty(試験コード AZ-120)** の合格を目的にしています。

- 試験の正式名称：**Planning and Administering Azure for SAP Workloads**
- 直訳：「SAP ワークロードのための Azure の計画と管理」
- 問われること：SAP を Azure に載せる設計と、載せた後に回し続ける運用の両方

SAP ワークロードとは、SAP HANA や SAP NetWeaver、SAP S/4HANA のように、企業の基幹業務を担う SAP のシステムのこと。止まると会社の業務が止まるため、Azure の中でも **可用性・性能・サポートの条件が厳しい** 領域になります。

想定読者

公式の学習ガイドは、受験者に **Azure Administrator Associate(AZ-104)を強く推奨** しています。あわせて、次の経験を求めています。

- SAP HANA
- SAP Business Suite
- SAP NetWeaver

ここで問われるのは SAP の導入手順の暗記ではなく、**この要件なら Azure のどのサービスを、どの構成で選ぶか** という判断。VNet、NSG、ストレージ アカウント、Microsoft Entra ID、RBAC が初見だと、読み進めるのに時間がかかります。不安なら、先に AZ-104 の範囲を一周してください。

試験の基本情報

項目	内容
試験名	Planning and Administering Azure for SAP Workloads(AZ-120)
認定	Microsoft Certified: Azure for SAP Workloads Specialty(スペシャリティ)
出題範囲の版	**Skills measured as of April 17, 2026**(このテキストはこの版に準拠)
試験時間	**100 分**
合格ライン	**1,000 点満点中 700 点以上**
受験方法	ピアソン VUE。監督付き(proctored)。対話的な構成要素が含まれる場合があります
言語	英語・日本語・簡体中国語・フランス語・ドイツ語・スペイン語・ポルトガル語(ブラジル)
認定の更新	12 か月

SAMPLE

試験ごとの問題数と形式は、Microsoft が公表していません。受験前に、公式の試験ページと学習ガイドで最新の記載を確かめてください。

このテキストの構成と読み方

章と節の並びは、公式の到達目標の並びと同じ。見出し末尾の `[1.1.1]` のような番号が、到達目標のコードです。問題集の各問も同じコードを持つので、**間違えた問題のコードを見て、同じコードの節に戻る** 使い方ができます。

読む順序は、頭からで構いません。第 1 章の最初の節で SAP の構成と Azure の対応を押さえておくと、第 2 章以降の設計判断が一本の線でつながります。

出題範囲(Skills measured)と配点

2026 年 4 月 17 日版の Skills measured は 4 分野。配点は **幅** で公表されています。

分野	配点	一言でいうと
① Migrate SAP workloads to Azure	**25〜30%**	移す：サイズ見積もり・サポート条件・移行方式・ガバナンス・RISE with SAP
② Design and implement an infrastructure to support SAP workloads on Azure	**25〜30%**	組む：VM・ネットワーク・ストレージの設計と自動展開
③ Design and implement high availability and disaster recovery (HADR)	**20〜25%**	止めない：クラスター・可用性ゾーン・バックアップ・DR
④ Maintain SAP workloads on Azure	**20〜25%**	保つ：性能と費用の最適化・監視・SAP 向けの管理サービス

- ①と②で半分以上。**どちらも「SAP が Azure でサポートされる構成か」が判断の土台**
- ③は Pacemaker、STONITH、フェンス エージェント、Azure Site Recovery のように、**名前を知らなければ解けない論点** が集中
- ④は費用の最適化と監視が中心。Azure Advisor、Azure Monitor、予約割引が SAP の構成にどう当たるかを問う

SAMPLE

第1章 Migrate SAP workloads to Azure [1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.1.7/1.1.8/1.1.9/1.2.1/1.2.2/1.2.3/1.

SAP を Azure へ移す仕事は、移す前の設計で決まる部分が大きくなります。この章は移行の前提づくりから順に進みます。サイズの見積もり、サポートされる構成、クォータ、ライセンス、費用、サポート契約、移行方式と道具。次にガバナンスと ID、最後に RISE with SAP との接続です。

SAP ワークロードのターゲット サイズを見積もる [1.1.1]

SAPS は、SAP Application Performance Standard というベンチマークで測る処理性能の単位です。CPU の速さそのものではなく、業務トランザクションをどれだけさばけるかを表します。認定された Azure VM ごとの SAPS 値は、SAP Note 1928533 に載っています。[^c1-1]

見積もりは 2 つの部分に分けて行います。DBMS が必要とする SAPS と、SAP アプリケーション サーバーが必要とする SAPS です。分ける理由は、スケールの仕方が違うからです。アプリ層は台数を増やして広げられますが、DB 層は多くの構成でスケールアウトしません。そのため、まず DBMS を載せる VM の SAPS から決めます。[^c1-1]

見積もりの出発点は、システムが既存か新規かで変わります。既存システムは、いまのハードウェアの SAP 標準ベンチマークの値から SAPS を推定します。新規システムは SAP とのサイジング演習で SAPS を決めます。新規の場合は、業務ドキュメントの量から計算する SAP Quicksizer のプロジェクトを技術設計書に含め、出力を Azure の計算、ストレージ、ネットワークに対応付けます。[^c1-2]

Quicksizer の代わりになる方法もあります。DBMS のワークロード レポートや SAP EarlyWatch Reports のように、いまのソース システムの負荷を元にした詳細なサイジングです。既存システムでは、DBMS サーバーの I/O スループットと IOPS も測っておきます。測れない場合は概念実証（PoC）が必要になります。サイジングの結果をまとめる項目は、VM の数、DBMS・(A)SCS・アプリケーション サーバーの層ごとの VM ファミリと VM の SKU、I/O スループットか計算したストレージ容量の要件の 3 つ。[^c1-50][^c1-1]

HANA は事情が少し違います。HANA の VM は、SAP HANA ハードウェア ディレクトリに載った認定 VM から選びます。メモリ量が HANA のサイジングの主役になり、必要メモリを満たす認定 VM のうち、SAPS と I/O も足りるものを選びます。HANA の認定は、メジャー バージョンやマイナー バージョンごとではありません。ディレクトリに載った VM は、HANA 1.0 と 2.0 の両方に使えると見なします。実際に使える HANA のリリースとパッチ レベルは、SAP Note 2235581 で調べます。[^c1-3]

VM 一覧には罠が 1 つあります。Note 1928533 には表が 2 つあり、2 つ目の表は Azure Standard Storage だけに対応する VM の SAPS です。この表の VM に DBMS を置く構成はサポートされません。[^c1-3]

場面で考えます。新規の S/4HANA を Azure に建てる計画で、Quicksizer の結果から DB 層に大きなメモリが要るとわかりました。この場合、DB 用の VM は HANA 認定 VM から選び、アプリ層は必要な SAPS を満たす台数を NetWeaver 認定 VM で並べます。アプリ層は台数で足せるのに対し、DB 層は後から大きな VM へ載せ替える作業が重いので、DB 側を先に固めずに進めることはできません。

移行元が多数ある場合は、Azure Migrate の SAP アセスメントが使えます。SAP システムの SID、サーバーごとの SAPS、サーバー一覧をテンプレート ファイルに入れて取り込む、インポート方式です。結果は、SAP の参照アーキテクチャに沿った VM とディスクの種類の推奨と、コストの見積もりのレポート。使うには Azure Migrate プロジェクトを

SAMPLE

アジアまたは米国のジオグラフィに作る必要があります。ターゲットのリージョンは自由に選べ、コストの推奨は指定したリージョンの料金で出ます。通貨、OS ライセンス、OS もアセスメントで指定します。この機能はプレビューとして扱われています。[^c1-4]

Azure でサポートされる SAP の構成を知る [1.1.2]

SAP ワークロードに使える Azure IaaS は、x86-64 のハードウェアだけです。Sparc や Power の CPU を使うサービスはありません。IBM メインフレーム、AS400、HP-UX、Solaris、AIX の上で動く SAP は、DBMS を含めて次のいずれかの OS へ移します。Windows Server、SUSE Linux、Red Hat Linux、Oracle Linux の 64 ビット版です。これ以外の OS や Linux ディストリビューションは、SAP ソフトウェアと組み合わせるとサポートされません。[^c1-5]

構成の基本形は 2 層と 3 層です。2 層は DBMS と SAP アプリケーション層が同じ VM を使い、3 層は別々の VM に分けます。どちらも、追加の高可用性は付きません。可用性は、使っている Azure の各コンポーネントの SLA の範囲にとどまります。2 層で HANA を使う構成は、高可用性のフェールオーバー クラスターを必要としない非運用のシステムだけがサポートされます。2 層では DBMS と SAP が 1 台のリソースを取り合うので、DBMS が使えるメモリを制限し、SAP の拡張メモリ（Extended Memory）も制限します。[^c1-6]

ホスト先にも制約があります。Azure VMware Solution は、一般に SAP が SAP ワークロードのホスト先としてサポートしていません。HANA Large Instances は sunset（終了に向かう）モードで、新規の顧客は受け付けません。既存の顧客への提供だけが続き、代わりに使うのは HANA 認定の Azure VM です。[^c1-6]

アカウントにも制約があります。Windows 上の SAP NetWeaver と S/4HANA は、Microsoft Entra ID のアカウントでは動きません。オンプレミスの Active Directory か、Microsoft Entra Domain Services を使います。ただし、SAP への SSO に Entra ID を使うことは影響を受けません。[^c1-6]

高可用性の枠は、Microsoft がサポートする構成が決めています。Microsoft は SAP ワークロードのシナリオに書かれた HA 構成とソフトウェアだけをサポートします。書かれていないサードパーティの HA フレームワークは、そのベンダーが窓口になります。Microsoft が直接サポートする HA フレームワークは、Pacemaker（Linux）と Windows Server フェールオーバー クラスタリングです。SIOS DataKeeper を使う構成は Microsoft が手順を文書化していますが、SIOS とのサポート契約は別に結ばなければなりません。Oracle Linux は Pacemaker をサポートしないので、HA にはサードパーティ製品が必要になります。[^c1-6]

DB 層の HA には対応表があります。

- HANA: Pacemaker を使う HANA System Replication（SUSE と Red Hat）、および Azure NetApp Files を使うスケールアウトの standby 構成
- SQL Server: Always On（運用の既定の推奨）、フェールオーバー クラスター インスタンス
- Oracle: Windows と Oracle Linux 上の Oracle Data Guard
- Db2: SUSE と Red Hat 上の IBM Db2 HADR

1 台の VM に複数の DBMS インスタンスを置く構成は、Windows 上の SQL Server、IBM Db2、Oracle、SAP HANA（MCOS）で使えますが、上の HA 構成ではサポートされません。1 つのインスタンスの中に複数のデータベースを入れる構成（HANA の MDC など）は、1 つのクラスター リソースで済むならサポートされます。[^c1-6]

サポートされない構成は、アプリ層と DB 層の間に遅延を増やす配置が中心です。

SAMPLE

- 片方の層をオンプレミスに、もう片方を Azure に置く
- アプリ層と DB 層を別の Azure リージョンに置く
- アプリ層と DB 層の間にネットワーク仮想アプライアンス（NVA）を置く
- 2 層を別のクラウド ベンダーに置く

このほかに、共有ディスク クラスターにデータベース ファイルを置く構成はサポートされません。例外は maxDB だけです。Azure Site Recovery で DBMS 層の VM を複製する構成は、テストされていないためサポート対象外です。DR には DBMS ネイティブの非同期複製を使います。[^c1-6]

SAP HANA ハードウェア ディレクトリで、文字「S」で始まるユニットは HANA Large Instances のユニットです。[^c1-47]

HANA には、NetWeaver の一般の場合と違う最小の OS リリースが当てはまることがあります。サポートされる OS は、ディレクトリのユニットの詳細で、ユニットごとに確かめます。M シリーズと Mv2 シリーズの VM にも、ほかの VM の種類と違う最小の OS リリースが当てはまります（SAP Note 1928533）。[^c1-48]

SAP と Microsoft の両方から完全なサポートを受けるには、SAP と Azure の両方でサポートされるリリースの組み合わせを使います。SAP NetWeaver や S/4HANA がサポートする OS のリリースが、どれも Azure の VM でサポートされるとは限りません。[^c1-49]

DR のリージョンの DB には、本番より小さい VM を使えます。DR 側の VM は、本番の負荷をすべて受けるわけではないからです。ただし小さい VM は、ネットワークとストレージのスループットが小さく、付けられるディスクの数も少なくなります。同じ可用性セットに VM が集まっている時や、M シリーズと Mv2 シリーズの間のサイズ変更では、VM ファミリをまたぐサイズ変更が問題になることがあります。DR 側の DB に要るのは、本番からの変更を遅れなく受け取って適用できるだけの CPU とメモリ。[^c1-47]

SAP の層ごとの計算、ストレージ、ネットワークの要件 [1.1.3]

SAP のランドスケープは、DB、ASCS/SCS（Central Services）、アプリケーション サーバーの 3 つの役割に分かれます。DB はディスクの IOPS、スループット、待機時間に敏感で、ASCS/SCS は小さいが止まると全体が止まる単一障害点になり、アプリ サーバーは台数で拡張します。要件はこの役割ごとに別々に決めます。

HANA の要件では、SAP が推奨する最小のスループットが次の 3 つです。[^c1-7]

- /hana/log：1 MB の I/O サイズで読み書き 250 MB/秒
- /hana/data の読み取り：16 MB と 64 MB の I/O サイズで 400 MB/秒以上
- /hana/data の書き込み：16 MB と 64 MB の I/O サイズで 250 MB/秒以上

/hana/data と /hana/log に使えるのは、HANA 認定のストレージだけです。Azure Premium SSD、Premium SSD v2、Ultra Disk、Azure NetApp Files の 4 つで、必須の条件です。/hana/data と /hana/log で別の種類を組み合わせる構成もサポートされます。たとえば /hana/data を Premium SSD に置き、低い待機時間が要る /hana/log を Ultra Disk に置けます。[^c1-7]

一方で、HANA System Replication（HSR）を組む場合の制約があります。各レプリカの /hana/data は同じストレージ種別、/hana/log も同じストレージ種別にします。片方の VM が Premium SSD v1、もう片方が Ultra Disk という構成はサポートされません。[^c1-7]

SAMPLE

ディスクを束ねる時の設定値は決まっています。LVM または mdadm でストライプを組む時のストライプ サイズは、/hana/data が 256 KB、/hana/log が 64 KB です。Azure のブロック ストレージは 3 つのコピーを保持するので、RAID の冗長構成は要りません。ストライプは IOPS とスループットを足し合わせる目的だけで使います。/hana/data、/hana/log、/hana/shared は、ルート用のボリューム グループに置かず、それぞれ別のボリューム グループに置きます。HANA 2.0 SPS03 以降は、HANA のデータ ボリュームのパーティション分割で、ボリューム マネージャーなしに複数ディスクへ I/O を分散できます。/hana/shared の推奨サイズは、スケールアップで Min(1 TB, 1 × RAM) です。[^c1-7]

場面で考えます。HANA の VM に 3 本の P30 ディスクを束ねて /hana/data を作ったところ、ディスク全体のスループットが VM の上限を超えていました。savepoint を書く時に HANA が I/O を強く出すと、VM の上限を使い切り、redo ログの書き込みに回る帯域を圧迫します。対策は、/hana/data の構成のスループットを VM の全体上限より低く保つことです。VM とディスクを 1 つの表で突き合わせて決めます。[^c1-7]

ストレージの冗長性は、Standard HDD/SSD、Premium、Premium SSD v2、Ultra Disk のいずれも、3 つのコピーを持つ LRS が既定です。DB のデータと REDO ログではLRS だけがサポートされます。SAP HANA の DBMS データ ボリュームとログ ボリュームに、Azure Files は使えません。[^c1-8]

ネットワークと VM の要件は次の通りです。[^c1-9]

- SAP ワークロードを動かすすべての VM で Azure の高速ネットワーク（accelerated networking）を有効にします。新規 VM では既定で有効ですが、状態を確かめます。
- HA クラスターには Standard ロードバランサーを使います。Basic ロードバランサーは SAP 構成に使うべきでなく、2025 年 9 月 30 日に廃止されました。
- VM の世代は第 2 世代が推奨。SAP の計画ガイドは、世代を変えるには必要な世代の VM を新しくデプロイし、ソフトウェアを入れ直すとしています。Azure には、第 1 世代の VM を Trusted launch に更新して第 2 世代にする手段もあります（2.1.1 で説明）。
- 可用性ゾーンと可用性セットは、1 台の VM に同時には割り当てられません。SAP ワークロードで使える scale set は、障害ドメイン数 1 の flexible scale set だけです。
- アプリ層と DB 層の通信経路に NVA は置けません。NSG と ASG のルールは、直接の経路を許す限り対象外です。
- アプリ層と DB 層を別の仮想ネットワークに分ける構成はサポートされません。やむを得ない場合は 2 つの仮想ネットワークをピアリングします。

資料に載るクォータは、理論上の最大値です。ディスクの IOPS の上限は、8 KB のような小さい I/O では届いても、1 MB のような大きい I/O では届かないことがあります。DB の I/O の設計は、VM のサイズの一覧の上限をそのまま当てにせず、I/O のサイズを含めて見積もります。[^c1-50]

クォータと提供状況を確かめる [1.1.4]

クォータは、Azure サブスクリプションに割り当てられたリソース数の枠で、設定も適用もサブスクリプションのスコープで行われます。調整可能なクォータは、Azure Home の My quotas ページから増枠を申請できます。調整不可のクォータは上限が固定で、変更にはサポート リクエストが必要です。増枠の申請に費用はかかりません。課金は、リソースを実際に使った量で決まります。[^c1-10]

SAMPLE

vCPU のクォータは 2 階層です。サブスクリプションとリージョンごとの Total Regional vCPUs と、VM サイズ ファミリごとのコア数です。どちらか一方でも超えると、VM はデプロイできません。コア数は、割り当て済みと、割り当て解除済み（停止してコンピューティングを解放した状態）の VM の合計で数えます。[^c1-11]

クォータとキャパシティは別物です。クォータは配置してよい枠で、キャパシティはリージョンとゾーンに実際にある資源です。クォータに余裕があっても、キャパシティが足りなければデプロイが通らないことがあります。増枠が承認されても、キャパシティの確保は保証されません。[^c1-10]

SAP では、デプロイの前に確かめる手順が決まっています。Azure Center for SAP solutions のデプロイの前提は、サブスクリプションのクォータが足りていることです。足りなければ先にサポート リクエストを作ります。プロジェクト計画のチェックリストにも、サブスクリプションの数とコア クォータを決め、必要なら増枠のサポート リクエストを開く、という項目があります。[^c1-12]

VM の種類がそのリージョンで使えるかは、Products available by region（リージョン別の提供製品のページ）で確かめます。ゾーン構成の HANA を計画する時は、使う VM サイズが対象の可用性ゾーンにあるかも先に確かめます。VM の SKU によっては、3 つのゾーンのうち 2 つにしか無く、残りの 1 つのゾーンには置けません。

OS、SAP、DB のライセンス [1.1.5]

Linux の OS ライセンスには 2 つの方式があります。BYOS（Bring Your Own Subscription）は、RHEL または SLES のサブスクリプションを自分で持ち込む方式で、Azure には VM のインフラ料金だけ払います。PAYG（従量課金）は、OS のサブスクリプション料を使った分だけ Azure に払う方式で、VM にはインフラ料金とソフトウェア料金の両方がかかります。[^c1-13]

方式は Azure Hybrid Benefit で切り替えられ、VM の再デプロイもダウンタイムも要りません。Azure Hybrid Benefit は、BYOS の Marketplace イメージや、オンプレミスや他のクラウドから持ち込んだ RHEL や SLES のイメージにも使えます。RHEL の BYOS のオファーは非公開の掲載で、使うには Red Hat Cloud Access プログラムへの参加が必要です。PAYG から BYOS への変換ができるのは、Red Hat または SUSE が公開したイメージだけです。[^c1-13]

VM に設定する license type の値は、SAP の試験で名前ごと問われます。

ディストリビューション	PAYG 側の license type	BYOS 側の license type
RHEL	RHEL_BASE、RHEL_EUS、RHEL_SAPAPPS、RHEL_SAPHA、RHEL_BASESAPAPPS、RHEL_BASESAPHA	RHEL_BYOS
SLES	SLES、SLES_SAP、SLES_HPC	SLES_BYOS

RHEL を BYOS から PAYG へ戻す場合は、VM に AHBForRHEL 拡張機能を入れてから license type を変えます。SUSE は拡張機能が要りません。SUSE では製品そのものは変えられず、課金の種類だけが切り替わります。license type が空のままなら、VM は元のイメージの課金方式を使い続けます。[^c1-13]

RHEL 側は、RHEL-SAP-HANA の提供が Red Hat により終了しています。既存の VM は動き続けますが、HANA のリポジトリを含む RHEL-SAP-HA イメージへの移行が推奨されます。また、ライセンスの方式によっては、記載された HA 構成を完全にサポートの対象にするために、OS プロバイダーとのサポート契約も必要です。[^c1-14]

SAMPLE

Azure Compute Gallery では、OS ベンダーによって BYOL のイメージを使えます。それ以外の OS イメージは、サポートが Azure の料金に含まれます。Compute Gallery のイメージを使う時は、OS ベンダーとのサポート契約を反映したイメージを選びます。[^c1-49]Azure Center for SAP solutions 自体に追加のライセンス費用はなく、デプロイしたコンピュート、ストレージ、ネットワーク、OS イメージのライセンス（Red Hat、SUSE）の分だけを払います。[^c1-15]

SAP のライセンスと DB のライセンスは、Azure ではなく SAP と DB ベンダーとの契約です。外部サービスから SAP のデータにアクセスする場合の影響は、SAP のライセンスの詳細を SAP に確かめます。Oracle で SAP を動かす場合の条件も、ライセンスと一体で問われます。ゲスト OS は Windows と Oracle Linux だけで、Oracle RAC はサポートされません。最小のリリースは Oracle 11g R2 パッチ セット 3（11.2.0.4）です。Oracle Linux のサポートは Oracle DBMS のクライアントにも及ぶので、ABAP や Java のダイアログ インスタンスのような SAP のコンポーネントも Oracle Linux で動かします。Oracle ASM は、一部のケースでサポートされます。[^c1-48][^c1-5]

SQL Server のライセンスについては、Software Assurance 付きのライセンスを Azure SQL Database と Azure SQL Managed Instance に割り当てる Azure Hybrid Benefit があります。SQL Server Enterprise の 1 コアは General Purpose の 4 vCore に、Standard の 1 コアは 1 vCore に相当します。Azure SQL Database でこの特典を使えるのは、vCore 購入モデルのプロビジョニング済みコンピューティングだけです。SQL Server の移行用の猶予期間は 180 日です。[^c1-16]

PAYG から BYOS への変換が終わったら、RHEL の VM は Red Hat に、SLES の VM は SUSE に直接登録します。更新と使用状況のコンプライアンスのためです。PAYG の VM は、既定で Red Hat Update Infrastructure（RHUI）か SUSE Cloud Update Infrastructure（CUI）につながっています。BYOS のイメージはプライベート プランに基づくため、今は CSP（クラウド ソリューション プロバイダー）のサブスクリプションでは使えません。[^c1-51][^c1-52]

RHEL の SAP 向けイメージの料金は、ベースのコンピューティング料金にプレミアムが上乗せされる形。RHEL for SAP with High Availability and Update Services は RHEL、SAP、HA の 3 つのプレミアム、RHEL for SAP は RHEL と SAP の 2 つのプレミアムが加わります。[^c1-52]

Windows Server にも Azure Hybrid Benefit があります。資格は、有効な Software Assurance か対象のサブスクリプション ライセンスが付いた、オンプレミスの Windows Server のコア ライセンスです。1 台の VM には最低 8 コア分のライセンスが要り、4 コアの VM でも 8 コア分を数えます。プロセッサ ライセンス 1 つは、16 コア ライセンスに相当。SQL Server や Marketplace のソフトウェアが入った Windows Server の VM でも、全リージョンで使えます。[^c1-53]

Azure の VM で SQL Server を動かす時のライセンス モデルは、従量課金、Azure Hybrid Benefit、High Availability/Disaster Recovery（HA/DR）の 3 つ。従量課金では、VM の秒単位の料金に SQL Server のライセンスが含まれます。HA/DR は、Azure に置く無償の HA/DR レプリカに使うモデルです。[^c1-54]

費用の要素と見積もりの道具 [1.1.6]

SAP の費用には、VM、ディスク、Azure NetApp Files（ANF）、ネットワークの転送、バックアップなどの要素があります。VM は料金モデルを選べ、従量課金、1 年または 3 年の予約（Reserved Instances）か Savings Plan、スポットの中から決めます。同じ VM タイプでも、リージョンによって価格が違います。見積もりには Azure 料金計算ツール（Pricing Calculator）を使い、リージョンも一緒に比べます。従量課金のライセンスの費用と、Azure Hybrid Benefit を使った場合の削減額を見積もるのも、この料金計算ツール。[^c1-54][^c1-17]

SAMPLE

ネットワークの転送料金は見落としやすい項目です。ピアリングした 2 つの仮想ネットワークの間を流れるトラフィックには、転送料金がかかります。アプリ層と DB 層を別の仮想ネットワークに分けると、層の間の通信が毎回課金されるので、大きな費用になりえます。[^c1-17]

システム単位のコストは、Azure Center for SAP solutions（ACSS）のコスト分析で見られます。Virtual Instance for SAP solutions（VIS）のリソースから、システムごとの稼働コストを確認できます。VM、ディスク、ロードバランサーに costanalysis-parent というタグが付くので、そのタグを元に集計されます。表示にはサブスクリプションの Cost Management Reader ロール、または同等の権限が必要で、コストと使用状況のデータの反映には通常 8 から 24 時間かかります。[^c1-18]

コスト分析に入らないリソースもあります。仮想ネットワーク、ストレージ アカウント、ANF、Key Vault、Azure Monitor for SAP solutions、Azure Backup のリソースです。システム単位の数字は、全体の費用の一部だとわかった上で読みます。[^c1-18]

そのほかの注意は次の通りです。HANA Large Instances は新規の顧客を受け付けないため、新規の見積もりは HANA 認定の Azure VM を前提にします。Azure Dedicated Host は SAP ワークロードでサポートされ、インフラのパッチ適用の周期を自分で制御したい顧客が使います。Azure Migrate の SAP アセスメントは、通貨、OS ライセンス、OS を指定して、指定したリージョンの料金でコストを推奨します。[^c1-17]

運用の形で費用の考え方が変わります。本番は常に動かすので、予約のように期間を約束して割引を受ける料金モデルが合います。開発や検証などの非本番は、使う時間帯が限られるので、必要な時間だけ動かす運用で費用を抑えられます。ただし、停止（割り当て解除）した VM のコア数も、クォータには数えられます。割り当て解除した VM でも、ディスクやネットワークなどのリソースの課金は止まりません。止まるのは、基盤のハードウェアを手放すコンピューティングの課金です。[^c1-69][^c1-19]

予約の割引が効く範囲は、OS で違います。SUSE Linux の予約は SUSE のソフトウェア プランの費用だけに効き、VM の使用料には効きません。Windows の VM と SQL Database では、予約の割引はソフトウェアの費用に効きません。Windows Server のライセンス費用を下げる手は、Azure Hybrid Benefit。予約は課金の割引で、リソースの動作には影響しません。[^c1-55][^c1-53]

Azure のサポート プランと SAP のサポート [1.1.7]

Azure のサブスクリプション管理（課金、クォータの調整、アカウントの移管）のサポートは無制限です。技術サポートには、サポート プランが必要です。[^c1-20]

プラン	24 時間 365 日の技術サポート	主な用途
Basic	なし（セルフヘルプのみ）	すべての Azure 顧客に付属
Developer	なし（営業時間内）	試用と非運用の環境
Standard	あり	Azure の運用ワークロード。重大度 A に 1 時間以内
Professional Direct	あり	事業に不可欠なワークロードの中小規模の企業

SAMPLE

プラン	24 時間 365 日の技術サポート	主な用途
Unified（Enterprise）	あり（エスカレーション管理付き）	大企業。業務システムの停止（重大度 1）に、Azure は 15 分以内、それ以外の製品は 1 時間以内

24 時間 365 日の技術サポートがあるのは Standard 以上のプランです。Unified（Enterprise）の対象は、Azure だけでなく Microsoft 365 や Dynamics 365 など、ほかの Microsoft の技術まで。[^c1-57]SAP の運用に必要な Microsoft とのサポート契約は、SAP Note 2015553 で確かめます。この Note は「SAP on Azure: Support Prerequisites」で、ストレージ、ネットワーク、監視、Microsoft とのサポート関係の前提を定義します。サードパーティのサービスをストレージ層に使う場合の SAP のサポートの制限も、この Note で調べます。[^c1-21]

サポート リクエストを作る側の権限にも決まりがあります。サブスクリプション レベルで、Owner、Contributor、Support Request Contributor、または Microsoft.Support/* を含むカスタム ロールが必要です。アカウント情報の変更や、サブスクリプションの所有権の移管とキャンセルは、サブスクリプションの課金管理者でなければできません。[^c1-20]

プロジェクト計画では、Microsoft とのサポートのエスカレーション経路と連絡先を決めておきます。SAP と Microsoft の窓口の分け方は、SAP を Azure 上で自分のサブスクリプションに持つ場合と RISE で SAP に任せる場合で変わります。RISE では、Azure サポートの対象は顧客自身のサブスクリプションのリソースだけです。SAP のサブスクリプションの中のリソースは、SAP に問い合わせます。[^c1-22]

Unified の重大度 1（業務システムの停止）の応答の目標は、Azure は 15 分以内、Azure 以外の製品は 1 時間以内です。[^c1-57]

サポート リクエストの権限にも決まりがあります。担当のサポート エンジニアが調べられるのは、起票時に指定したサブスクリプションのリソースだけです。Microsoft Entra の問題のように、サブスクリプション無しで起票するには Admin である必要があります。サブスクリプションの所有権の移管や解約、アカウント情報の変更には、そのサブスクリプションの課金管理者（account billing administrator）の権限が必要。選べる最大の重大度と応答の時間は、サポート プランと、所在の国や地域（その営業時間を含む）で決まります。[^c1-56]

移行方式を選ぶ [1.1.8]

移行の方式は、OS と DB が変わるかどうかで分けます。変わらないものは同種（homogeneous）、変わるものは異種（heterogeneous）です。異種の移行では、データをエクスポートしてインポートする作業が入るので、両方の段階をテストして最適化します。[^c1-2]

出題範囲は、リフト アンド シフト、リフト シフト マイグレート、リフト シフト マイグレート to HANA の 3 つから選ぶ力を求めています。設計の分かれ目は、OS と DB をそのまま移すか、移す時に DB を替えるか、DB を SAP HANA に替えるか、の 3 通り。

リフト アンド シフトには、道具と限界があります。VM ベースのワークロードの一部は、Azure Migrate や Azure Site Recovery（ASR）でそのまま移せます。ただし、OS とワークロードがサポートされているかを先に確かめます。多くの忙しい SAP システムは、移行ツールが許容する変更率を満たせません。DB のワークロードは整合性を保証できないため、対象外になることが多くなります。Azure Site Recovery と Azure Migrate は、大規模な SAP の移行では検証されていません。[^c1-1]

SAMPLE

実績のある移行方式は、DBMS のレプリケーション（HANA System Replication など）か、SAP の移行ツールを使う方法です。基本的な VM の移行より、Azure 上に新しくデプロイして移行するほうが容易です。その場合、DBMS ネイティブのレプリケーション、バックアップと復元、SAP の移行ツールのどれかを使います。新しく展開する作業には、Azure Center for SAP solutions や SAP Deployment Automation Framework のような自動化の仕組みも使え、自動のタスクを素早く実行できます。[^c1-50][^c1-1]

場面で考えます。巨大で更新の多い本番の SAP DB を、停止時間を短くして Azure へ移したいとします。VM ごとの複製では変更率に追いつけず、整合性も保証されません。そこで DB のネイティブ複製（HANA なら HANA System Replication）で Azure 側に複製を作り、切り替えの時に役割を入れ替えます。複製は先に始めておけるので、停止するのは切り替えの短い時間だけです。

移行の作業を速くする工夫もあります。移行中は、VM のサイズや Premium SSD v1 のパフォーマンス ティア、Premium SSD v2 の IOPS とスループットを一時的に上げると、展開が速くなります。マネージド ディスクのサイズは縮小できないので、大きくしすぎた分は戻せません。Azure ストレージへのデータ コピーは、多くの場合、インターネット経由が安全で最速の経路です。ExpressRoute や VPN はボトルネックになることがあります。接続の種類によらず、単一ストリームの転送性能は低いことが多いので、複数の TCP ストリームに対応したツールで転送を速めます。[^c1-50][^c1-1]

移行の道具と段取り [1.1.9]

SAP が提供する移行の道具は次の通りです。Migration Monitor と SWPM（Software Provisioning Manager）、SAP DMO（Database Migration Option of SUM）、DMO with System Move です。いずれも停止時間を短くするための手法です。最新リリースの DMO with System Move は、インターネット越しのデータ転送に AzCopy を使え、最速のネットワーク経路をそのまま使えます。[^c1-2]

道具の選び方には基準があります。移行元と移行先の SAP リリース、DBMS、それにリリースのアップグレードや Unicode 変換、S/4HANA 変換を同時に行うかどうかです。システム コピーは、同種と異種で手順が違い、異種のシステム コピーはエクスポートとインポートを伴います。SAP DMO は、移行に SAP のリリース アップグレードや SAP HANA への移行を組み合わせる時に使います。ただし、移行元の DBMS と移行先の DBMS のすべての組み合わせがサポートされるわけではありません。組み合わせは、DMO のリリースごとの SAP Note で確かめます。[^c1-49][^c1-2]

DB のネイティブな仕組みによる移行の例は、HANA System Replication のような DBMS ネイティブのレプリケーションと、DBMS のバックアップと復元です。移行元の DB と同じ種類のまま Azure へ移す同種の移行で使い、Azure 側の複製を先に同期させておけば、停止時間が短くなります。小さな DB は、バックアップと復元で移せます。停止時間を短くしたい DB は、バックアップと復元で Azure 側の DB に初期データを入れ（seed）、SQL Server Always On、HANA System Replication、ログ配布のどれかで移行元と同期させます。[^c1-49][^c1-1]

Azure 側の道具の役割は分かれています。Azure Migrate は無料のサービスで、ワークロードの把握、IaaS と PaaS のターゲットの評価、移行計画、移行の実行を扱います。SAP アセスメントは、システムの SID とサーバーごとの SAPS をテンプレートに入れて取り込み、サイジングとコストを出す機能です。AzCopy は、データを Azure ストレージへコピーするコマンド ライン ツール。ネットワークが細くて転送に時間がかかる大容量のデータには、Azure Data Box のような物理媒体で送る方法もあります。Data Box は、ネットワーク接続が無いか限られる場面で 40 TB を超えるデータを送るのに向きます。初期の一括転送を Data Box で行い（seed）、その後の増分をネットワーク経由で送る使い方もあります。[^c1-70][^c1-23]

SAMPLE

段取りは、試行移行、停止時間の見積もり、切り替えの順に組みます。試行移行では、移行の前後で主要な業務プロセスの実行時間と正確性を比べ、本番移行の前に最適化します。検証テストの結果は、移行元の元のシステムでも結果が取れている時だけ受け入れます。[^c1-49]異種の移行では、試行でエクスポートとインポートの段階をテストして最適化します。[^c1-1]

パイロット展開の段取りも、チェックリストに沿って組みます。パイロットの間に、HADR とセキュリティの設計を完全な形で検証します。パイロットで使う移行のネットワーク経路は、将来の本番の移行で使う経路と同じにします。Azure で動いている既存のワークロード（SAP も SAP 以外も）には、影響を出しません。パイロットでは、本番システムを Azure へ移す手順そのものもテストします。大規模な SAP 環境の移行では、公開されているベストプラクティスを確かめます。[^c1-49]

本番システムを同じ時期にまとめて移さない場合は、同じホスティング先に置く必要がある本番システムごとにグループを作ります。データ移行は、つながる SAP 以外のアプリケーションとインターフェースも含めてテストします。本番の移行の後に行う機能と業務のテストの内容は、事前に業務の責任者と合意しておきます。[^c1-49]

データ転送の経路は、多くの場合インターネット経由が最速です。例外は DB の複製に私設の接続が要る場合で、ExpressRoute の回線に十分な帯域があれば ExpressRoute が最速。計画の段階では、大量のデータを Azure へ送る専用の移行ネットワークも検討します。移行の通信が利用者やアプリの経路に与える影響は、前もって見込んで抑えます。HANA System Replication の同期が共用の ExpressRoute の帯域を圧迫する場面は、この見込みが足りない例です。[^c1-49][^c1-50]

Azure RBAC とロールの割り当て [1.2.1]

Azure RBAC は、Azure Resource Manager 上の認可の仕組みです。Azure リソースへのアクセスを細かく管理します。ロールの割り当ては 3 つの要素でできています。セキュリティ プリンシパル（ユーザー、グループ、サービス プリンシパル、マネージド ID）、ロール定義、スコープです。[^c1-24]

スコープは、管理グループ、サブスクリプション、リソース グループ、リソースの 4 階層で、親から子へ継承されます。複数のサブスクリプションを管理グループの下に置けば、管理グループへの 1 回のロール割り当てが、すべてのサブスクリプションに継承されます。複数のロールが重なった時は加算で、有効な権限は、割り当てられたロールの権限を合算したものになります。ただし、拒否割り当て（deny assignment）が当たる操作は、ロールの割り当てに関係なくブロックされます。[^c1-24]

組み込みロールの基本は次の通りです。Owner は、リソースの管理とアクセス権の割り当てまでできます。Contributor は、リソースの作成と管理はできますが、アクセス権の割り当てはできません。Reader は、見るだけです。Virtual Machine Contributor は、VM とそのディスクを作って管理できますが、VM が接続している仮想ネットワークとストレージ アカウントの管理権限は含みません。SAP の運用では、基盤を作る担当に Contributor 系を、監査や参照だけの担当に Reader を割り当て、アクセス権の付与は少人数の Owner か User Access Administrator に絞ります。User Access Administrator は、Azure リソースへの利用者のアクセスを管理するロールで、リソースそのものを管理する権限は含みません。[^c1-58]

Azure Center for SAP solutions（ACSS）には、専用のロールがあります。[^c1-25]

SAMPLE

ロール	できること
Azure Center for SAP solutions administrator	インフラのデプロイ、SAP のインストール、既存システムの VIS への登録、開始と停止、VIS の削除まで、すべての操作
Azure Center for SAP solutions service role	ユーザー割り当てマネージド ID に付けるロール
Azure Center for SAP solutions reader	すべての VIS リソースの閲覧

マネージド ID を使う場面では、追加のロールが要ります。既存のユーザー割り当てマネージド ID を使うには、Managed Identity Operator が追加で必要です。新しくユーザー割り当てマネージド ID を作る場合は、Managed Identity Contributor と Managed Identity Operator の両方が必要です。SAP ソフトウェアをインストールする時は、そのユーザー割り当てマネージド ID に、ACSS service role と Reader and Data Access を付けます。[^c1-25]

本番の SAP の誤操作を防ぐ手段は、リソース ロックとカスタム ロールです。ロックは、サブスクリプション、リソース グループ、リソースに付けられます。CanNotDelete は読み取りと変更ができて削除できないロック、ReadOnly は読み取りだけで変更も削除もできないロックです。ロックはすべてのユーザーとロールに効き、RBAC の権限を持っていても、ロックがある間は削除や変更ができません。親のスコープに付けたロックは子に継承され、継承の鎖の中では最も厳しいロックが効きます。ロックの作成と削除には Microsoft.Authorization/locks/* の権限が必要で、Owner と User Access Administrator が持っています。[^c1-26]

ロックには意外な副作用もあります。リソース グループに ReadOnly を付けると、その中の VM は開始も再起動もできなくなります。この操作が POST の要求だからです。また、ロックが効くのは、管理操作（コントロール プレーン）だけです。データの読み書き（データ プレーン）は止まりません。管理グループにはロックを付けられません。[^c1-26]

カスタム ロールは、組み込みロールで足りない時に、必要な操作だけを集めて作ります。たとえば Microsoft.Support/* の操作を含むカスタム ロールは、サポート リクエストの作成に使えます。[^c1-20]

ロールの割り当てだけを任せたい時は、Role Based Access Control Administrator を使います。Azure RBAC のロールを割り当ててアクセスを管理するロールで、Azure Policy などほかの方法でのアクセス管理は許しません。すべてのリソースの管理とロールの割り当てができる Owner より、狭い権限です。[^c1-58]

Azure Policy でガバナンスを効かせる [1.2.2]

Azure Policy は、組織の標準を強制し、大規模にコンプライアンスを評価する仕組みです。ビジネス ルールは JSON のポリシー定義に書き、複数の定義をまとめたものがイニシアティブ（ポリシー イニシアティブ）です。評価の結果はコンプライアンス ダッシュボードに集約されます。既存のリソースの一括修復も、新規リソースの自動修復もできます。[^c1-27]

割り当てのスコープは、管理グループ、サブスクリプション、リソース グループ、個別のリソースです。必要なら下位のスコープを除外できます。除外（notScopes）に入れたスコープは評価されず、コンプライアンスの数にも入りません。検証環境のような広いスコープを恒久的に外すなら除外、期限付きや個別の事情で外すなら免除（exemption）を使い、免除したリソースは追跡が続きます。[^c1-71]管理グループに割り当てたポリシーは、配下の管理グループ、サブスクリプション、リソースに継承され、配下のリソースやサブスクリプションの所有者は変更できません。評価は、リソースの作成と更新の時、新しく割り当てた時、割り当て済みのポリシーを更新した時と、24 時間ごとの標準評価サイクルで実行されます。リソース グループに割り当てたポリシーは、そのリソース グループと中のリソースに適用され、同じサブスクリプションのほかのリソース グループには適用されません。[^c1-72][^c1-27]

SAMPLE

非準拠のリソースに何をするかは、効果（effect）で決めます。効果は、ポリシー定義のポリシー ルールの中に 1 つだけ設定します。試験で押さえる 4 つは次の通りです。[^c1-28]

効果	動き
Deny	非準拠になる作成と更新を拒否する
Audit	拒否せず、非準拠をアクティビティ ログに警告として記録する
Modify	作成や更新の時に、タグなどのプロパティを追加、更新、削除する
DeployIfNotExists	条件に合うリソースがあって、関連リソースが無い時に、テンプレートをデプロイする

ほかに Append、AuditIfNotExists、Disabled、DenyAction、Manual があり、評価の順番は、Disabled が最初、次に Append と Modify、その次に Deny、さらに Audit です。Append や Modify が要求を書き換えると、後ろの Audit や Deny が起きなくなることがあります。Deny を Audit より先に評価するのは、望ましくないリソースの二重のログを避けるためです。AuditIfNotExists と DeployIfNotExists は、リソース プロバイダーが成功を返した後に評価されます。AuditIfNotExists が監査するのは、if の条件に合うリソースに関連する子リソースや拡張リソースが、指定した性質を持たない時。Deny、Modify、DeployIfNotExists のような強制の効果を割り当てる前に、Audit か AuditIfNotExists で、定義が環境のリソースに与える影響を確かめるのが推奨です。Deny を割り当てる前からあるリソースは、評価で非準拠とマークされるだけで、変更も削除もされません。DeployIfNotExists は、評価サイクルでは条件に合う既存のリソースを非準拠とマークするだけで、そのリソースには何もしません。既存の非準拠のリソースは、修復タスク（remediation task）で是正します。Append も既存のリソースを変えずに非準拠とマークするので、タグの管理には、既存のリソースも是正できる Modify が推奨です。[^c1-59][^c1-28]

複数の割り当てが同じリソースに効く時は、それぞれが独立して評価され、結果は累積して最も厳しい方になります。サブスクリプションに Deny、その下のリソース グループに Audit という組み合わせでは、サブスクリプションの Deny の条件に反する新規リソースは、リソース グループの Audit に関係なく拒否されます。スコープの違いですり抜ける隙間はありません。[^c1-28]

SAP の方針の例は次の通りです。許可するリージョンだけにデプロイさせる。タグを必須にして一貫して付ける。診断ログを Log Analytics ワークスペースに送ることを要求する。タグの一貫性は、Azure Policy で強制する設計が基本です。SAP ワークロードの計画では、サブスクリプションと管理グループに対して、全社で Azure Policy を使うことを検討します。[^c1-27]

規制の準拠は、組み込みのイニシアティブを割り当てて評価します。結果は Microsoft Defender for Cloud の規制コンプライアンスのダッシュボードでも確かめられます。Azure Arc を使えば、ポリシーによるガバナンスを他のクラウドやオンプレミスのデータセンターにまで広げられます。[^c1-27]

組み込みのポリシーでは、場所の制限に Allowed locations、VM のサイズの制限に Allowed virtual machine SKUs を、許可する値の一覧を指定して割り当てます。必須のタグを既定値つきで付けるには、Modify の組み込みポリシー Add a tag to resources を使います。[^c1-59][^c1-59]

割り当ての enforcementMode を DoNotEnforce にすると、リソースは評価されますが、効果は発動しません。強制する前に、既存のリソースへの影響を確かめる時に使います。[^c1-60]

SAMPLE

Append は、要求の既存の値を別の値で上書きすることになる時、deny と同じように要求を拒否します。既存の配列に値を足すには、配列の [] のエイリアスを使います。[] でないエイリアスで配列全体を設定すると、配列がすでにある要求では競合が起き、拒否されます。[^c1-61]

Modify と DeployIfNotExists の割り当ては、修復のためにマネージド ID を使います。1 つの割り当てに関連付けられるマネージド ID は 1 つで、その ID に複数のロールを付けられます。[^c1-62]

自作のイニシアティブを規制コンプライアンスとして扱うには、定義の category プロパティを Regulatory Compliance にします。[^c1-63]

SAP のシングル サインオン：NetWeaver、Fiori、SAP GUI [1.2.3]

SAP アプリケーションには、SSO か MFA を推奨し、従来のユーザー名とパスワードは推奨しません。クライアントの種類で、使える認証の方式が決まります。ブラウザーは SAML か OIDC、SAP GUI は X.509 か Kerberos チケット、モバイルは X.509 か SAML です。SAML と OIDC の方が推奨です。[^c1-29]

SAP NetWeaver を Microsoft Entra ID と SSO させる手順は、決まった順に進みます。必要なものは、Application Administrator、Cloud Application Administrator、Application Owner のいずれかのロールと、SAP NetWeaver V7.20 以降です。NetWeaver は SAML（SP-initiated SSO）と OAuth の両方をサポートし、チュートリアルは SAML です。SAML か OAuth のどちらかで構成します。[^c1-30]

SAML の設定の流れは次の通りです。

1. SMICM で、HTTP と HTTPS のサービスが有効で、ポートが割り当てられていることを確認する
2. SICF_SESSIONS で HTTP のセキュリティ セッションを有効にする
3. SICF のサービスを有効にする
4. SAML2 トランザクションで、SAP 側（サービス プロバイダー）のメタデータ XML を生成する
5. Entra のエンタープライズ アプリの Basic SAML Configuration に、そのメタデータ XML をアップロードする（識別子と応答 URL が自動で入る）
6. Entra のフェデレーション メタデータ XML をダウンロードし、SAP の SAML2 に取り込む

プロファイル パラメーターの例として、login/create_sso2_ticket = 2、login/accept_sso2_ticket = 1、http/security_session_timeout = 1800 などが示されています。値は組織の要件で調整します。プロバイダー名は既定で「SID + クライアント」の形ですが、Entra ID は「プロトコル://名前」の形を期待するので、https:// を付けた形を推奨します。[^c1-30]

SAP Fiori と HANA にも専用のチュートリアルがあります。SAP HANA は IDP-initiated SSO と just-in-time のユーザー プロビジョニングをサポートします。アプリケーションの識別子が固定値なので、テナントに入れられるのは 1 インスタンスだけです。[^c1-31]

SAP GUI の SSO には、SNC の X.509 証明書か Kerberos チケットを使います。SAP GUI が Entra ID と連携する場合も SNC を使います。RISE の環境を含めて整理すると、使い分けは次の通りです。[^c1-32]

SSO の方式	IdP	主な用途
SAML / OAuth	Microsoft Entra ID	SAP Fiori、Web GUI、Portal、HANA

SAMPLE

SSO の方式	IdP	主な用途
SNC	Microsoft Entra ID	SAP GUI
SPNEGO	Active Directory	Web GUI、SAP Enterprise Portal

社内に Windows ドメインがあり、SAP GUI の利用者は社内 PC だけで、ブラウザーの Fiori は社外からも使う場面を考えます。この場合、SAP GUI は Kerberos で AD のチケットを使い、Fiori は SAML で Entra ID に任せると、MFA を Fiori の入り口に集められます。

VM への OS のサインインは、SSO とは別の話です。Linux と Windows の VM に Microsoft Entra ID でサインインさせて、VM ごとのローカル アカウントへの依存を減らせます。Linux の VM で使うのは、AADSSHLoginForLinux の VM 拡張機能と、OpenSSH の証明書ベースの認証。利用者に SSH の鍵を配らず、VM に公開鍵も置かずに、Entra ID の資格情報でサインインできます。[^c1-65]Azure Bastion は、パブリック IP を持たない VM へ、ブラウザー経由で RDP や SSH を中継するサービス。SAP の VM を閉じたネットワークに置いたまま、運用担当が入る入口になります。Windows 上の SAP NetWeaver と S/4HANA が Entra ID のアカウントでは動かないことと、SSO の話は別物です。Windows 上の SAP NetWeaver と S/4HANA は従来の Active Directory に依存するので、Microsoft Entra ID のアカウントはサポートされず、AD のドメイン アカウントで動かします。[^c1-47][^c1-6]

SAP は 2022 年に Fiori のモバイル アプリの提供を終え、モバイルでもネイティブのブラウザーを使う形に変わりました。そのため、モバイルにも SAML か OIDC を推奨します。SAML は確立された業界標準、OIDC は新しい方式で、どちらもブラウザー ベースのクライアントに使えます。NetWeaver Business Client、Concur、BEx、BusinessObjects などのクライアントはこの説明の対象外で、一部はサポートが終わっています。こうしたクライアントには、可能な限り SAP Cloud Identity Services を使います。[^c1-29]

HANA の SSO では、既存の HANA のユーザーの External Identity に、Entra の SAML トークンの NameID と同じ値（たとえばメール アドレス）を入れます。Entra ID のアプリへの割り当てだけで、External Identity が空のままでは、ユーザーを対応付けられません。Any のチェックボックスはオンにしません。Any は IdP が NameID に SPProviderID を送る前提の設定で、Microsoft Entra ID はこれに対応していないからです。[^c1-31]

Windows の VM で Microsoft Entra ID のサインインを有効にすると、VM は Microsoft Entra 参加になり、オンプレミスの Active Directory などの別のドメインには参加できません。AD のアカウントで動く Windows 上の SAP NetWeaver のサーバーとは、両立しません。Entra ID で VM にサインインさせるには、VM と関連するネットワーク リソースを含むリソース グループに、Virtual Machine Administrator Login（管理者の権限）か Virtual Machine User Login（一般ユーザーの権限）のロールを割り当てます。[^c1-64][^c1-65]

SAP の SaaS と Microsoft Entra ID [1.2.4]

SAP Cloud Identity Services は、4 つの機能を含みます。Identity Authentication（IAS）、Identity Provisioning（IPS）、Identity Directory、Authorization Management です。IAS は SAP のクラウドとオンプレミスのアプリの認証、SSO、ユーザー管理を担います。IPS は、ID とその権限を SAP アプリへプロビジョニングするクラウド サービスです。[^c1-33]

SAP BTP のビジネス ユーザーの認証と認可を担うのは XSUAA（Extended Services for Cloud Foundry User Account and Authentication）です。マルチテナントの OAuth 認可サーバーです。BTP/XSUAA と IdP の信頼の構成

SAMPLE

には SAML 2.0 を使います。SAP の今の文書では、IAS との間に OpenID Connect 型の信頼も構成できます。アプリと BTP/XSUAA の間は OpenID Connect。[^c1-33]

Entra ID との組み合わせは 2 通りあります。BTP/XSUAA から Entra ID へ直接フェデレーションする方法と、IAS を間に入れて Entra ID を Corporate Identity Provider とする方法（SAML Proxying）です。推奨は IAS を介する方です。Entra ファーストの設計では、次の 6 つを推奨します。[^c1-33]

- IAS を介してフェデレーションする
- 認証は Entra ID、認可は IAS と BTP で持つ
- Entra のグループと BTP のロール コレクションを対応させる
- BTP のサブアカウントは、同じ種類の ID 要件のものだけをまとめる
- 本番の IAS テナントを使う
- SAML の署名証明書のロールオーバー手順を決めておく

SAML アサーションの大きさや、Cloud Foundry のロール コレクション名の長さと数には SAP 側の制限があります。超えると認可の問題が起きます（SAP Note 2732890）。[^c1-33]

SSO とプロビジョニングは別の仕事です。SSO は、サインインの時に誰かを確かめる認証の仕組み、プロビジョニングは、ユーザーやグループを事前に SAP 側に作って同期する仕組みです。Microsoft Entra から IAS へのユーザーとグループの同期は、ネイティブに対応した、無料で追加できる機能です。Entra ID から BTP へは、ネイティブのプロビジョニングがありません。IAS を経由します。[^c1-73]SuccessFactors については、SuccessFactors から Microsoft Entra へのインバウンド プロビジョニングが推奨です。アウトバウンドは CIS でターゲット システムを設定します。SuccessFactors、SAP BTP、SAP Fiori はいずれも SP-initiated SSO をサポートします。[^c1-29]

ギャラリーから SAP の SaaS アプリを追加するには、Application Administrator、Cloud Application Administrator、Application Owner のいずれかのロールが必要です。手順は Entra admin center の Enterprise apps から New application を選びます。SAP BTP の SSO をテストするには、BTP アカウントに自分のアプリをデプロイするか、アプリをサブスクライブする必要があります。SAP Identity Management（SAP IDM）は 2027 年までに廃止予定で、SAP は Microsoft Entra への移行を推奨しています。[^c1-32]

SuccessFactors にサインインさせるには、Entra のユーザーが SuccessFactors にプロビジョニングされている必要があります。SP 起点のログインを有効にしても、まだ登録されていない利用者は SSO できません。[^c1-66]

BTP の信頼構成で Create Shadow Users During Logon を有効にすると、BTP にまだ無い利用者は、初回のサインインでアカウントが自動で作られます。無効にすると、事前にプロビジョニングしたユーザーしかサインインできません。[^c1-33]

Microsoft の資料では、IAS の Corporate Identity Provider はメタデータ XML のインポートで設定し、BTP にも IAS のメタデータ XML を 1 回アップロードします。SAP の今の文書では、IAS の SAML 2.0 の Corporate Identity Provider にメタデータの URL も指定できます。Entra の SAML 署名証明書の初期の有効期間は既定で 3 年で、エンタープライズ アプリごとに固有。期限切れの通知は既定でアプリを構成した人に届くので、宛先をグループのメールボックスにしておきます。[^c1-33]

IAS とのフェデレーション用のエンタープライズ アプリでは、User assignment required を明示的にオフにします。SAML アプリでは既定でオンの設定です。Entra からは利用者がどの BTP アプリに入るかが見えず、認可を 2 か所で

SAMPLE

持つと食い違うからです。有効のまま利用者をアプリに割り当てないと、BTP で許可された利用者でも、Entra ID での認証は通りません。[^c1-73][^c1-33]

グループのクレームには、変わらず再利用されないグループ ID（オブジェクト ID）を識別子に使います。Entra の SAML のグループ クレームの上限 150 を超えないよう、アプリに割り当てたグループだけを返す。IAS の Corporate Identity Provider で Use Identity Authentication user store を有効にすると、Entra のグループの情報が BTP へ渡る SAML トークンに残らず、グループでの認可が失敗します。[^c1-33]

管理グループとリソースの階層設計 [1.2.5]

管理グループは、サブスクリプションの上のガバナンスのスコープです。適用した条件は、配下のサブスクリプションに継承されます。同じ管理グループ内のサブスクリプションは、同じ Microsoft Entra テナントを信頼している必要があります。各管理グループとサブスクリプションがサポートする親は 1 つだけで、管理グループは多数の子を持てます。[^c1-34]

数値は決まっています。1 つのディレクトリに管理グループは 10,000 個まで、階層はルートとサブスクリプションのレベルを除いて最大 6 レベルです。管理グループあたりのサブスクリプション数は無制限で、サブスクリプションあたりのリソース グループは 980 個までです。[^c1-35]

ルート管理グループは、各ディレクトリに 1 つあります。既定の表示名は Tenant root group、ID は Entra テナント ID と同じです。移動も削除もできません。新規のサブスクリプションは既定でここに入ります。既定ではルートへのアクセス権を持つ人はいません。Microsoft Entra の Global Administrator だけが昇格でき、昇格すると User Access Administrator ロールが付きます。表示名を変えるには Owner か Contributor が必要です。Microsoft Customer Agreement（MCA）のサブスクリプションの Cost Management 機能では、管理グループは現在サポートされていません。[^c1-34]

Cloud Adoption Framework は、リソースの編成を 4 つのスコープで考えます。管理グループ、サブスクリプション、リソース グループ、リソースです。サブスクリプションは、ポリシーと管理の境界であり、スケールの単位でもあります。SAP のような大規模で専門的なワークロードは、サブスクリプションの上限に当たらないよう、別のサブスクリプションにします。仮想ネットワークは、サブスクリプションをまたいで共有できません。つなぐ時は、ピアリングや ExpressRoute を使います。[^c1-74]SAP の設計では、ワークロード別、デプロイの段階（本番と非本番）別、事業部別にサブスクリプションを分けるかを決めます。[^c1-36]

本番と非本番で、ポリシーとロールを別々にしたい SAP の環境を考えます。本番用と非本番用で管理グループを分け、それぞれにサブスクリプションをぶら下げます。本番側の管理グループには Deny 中心の厳しいポリシーと少人数のロール割り当て、非本番側には緩めの設定。サブスクリプションの数が増えても、管理グループへの 1 回の割り当てで全体に効きます。

SAP のシステムごとのリソース グループの設計では、1 つの SAP システム（SID）の VM、ディスク、ロードバランサーを同じリソース グループにまとめるのが基本で、ロールやロックやコストをシステム単位で扱えます。

SAP 向けのランディング ゾーン [1.2.6]

ランディング ゾーンは、ワークロードを載せる前に用意する、Azure 環境の土台です。Cloud Adoption Framework のランディング ゾーンは、設計領域を A から I の文字で示します。具体的には、請求と Entra テナント、ID とアクセス管理、リソースの編成、ネットワークのトポロジと接続、セキュリティ、管理、ガバナンス、プラットフォームの自動化と

SAMPLE

DevOps などの領域。このうち、請求とテナント、IAM、リソースの編成、ネットワークは環境の設計領域で、セキュリティ、管理、ガバナンス、自動化と DevOps はコンプライアンスの設計領域です。ID とアクセス管理は、パブリック クラウドの主要なセキュリティ境界です。コンプライアンスの設計領域の目的は、次のとおりです。[^c1-75][^c1-37]

- ガバナンス: ポリシーの監査と強制の自動化
- 管理: 可視性、運用のコンプライアンス、保護と復旧の能力を持つ管理のベースライン
- セキュリティ: クラウド環境を守る統制とプロセスの実装
- プラットフォームの自動化と DevOps: ランディング ゾーンと関連リソースをデプロイするツールとテンプレートの整合

SAP 向けのランディング ゾーン アクセラレータは、SAP の基盤の設計を扱います。ネットワークのトポロジ、AD と DNS、ID の管理、Azure RBAC の構造、リソースの命名戦略、セキュリティの運用が、設計に含まれます。[^c1-2]

ネットワークは、ハブ アンド スポークか Virtual WAN の構成を評価し、SAP ワークロード用に独立した仮想ネットワークのスポークを設けます。小規模なら、1 つの仮想ネットワークの中でのマイクロセグメント化もあります。オンプレミスと接続する SAP には ExpressRoute のプライベート接続を推奨します。小規模や遠隔の拠点には VPN で、ExpressRoute のフェイルオーバー経路に VPN のサイト間接続を併用できます。[^c1-2]

セキュリティの最小構成には、Defender for Endpoint、Sentinel for SAP などの SIEM/SOAR、TDE などの DB の暗号化と Key Vault、第 2 世代 VM と Trusted Launch、Azure Backup の不変ストレージが入ります。ただし SAP HANA は、暗号化キーを Azure Key Vault やほかの HSM に置くことをサポートしません。既存の環境が管理グループを使っていなければ、ポリシー、アクセス、コンプライアンスを大規模に管理するために導入を検討します。[^c1-38]

どの Azure サービスで SAP を扱うかを選ぶ指針もあります。新しい S/4HANA をガイド付きでデプロイするなら Azure Center for SAP solutions です。環境を繰り返しデプロイするなら SAP Deployment Automation Framework です。インフラの設計を自分で決めたいなら SAP on Azure VM workloads を選びます。[^c1-39]

ネットワーク構成の評価の観点は、ほかにもあります。サブネットの VM がリスクになった時の切り離しでは、別のスポークならピアリングを切るだけで済み、NSG を変えてサブネットを隔離するより素早く切り離せます。ピアリングした仮想ネットワークの間のデータのやり取りには費用がかかり、これも評価の観点の 1 つ。オンプレミス、インターネット、Azure の仮想データセンターの間のトラフィックを、集中的に記録して監査できるかも確かめます。[^c1-49]

RISE with SAP の責任分担と接続方式 [1.3.1]

RISE with SAP の SAP 環境は、SAP が所有する Azure のサブスクリプションとテナントの中にあり、SAP が運用します。顧客の Azure 環境には、その SAP と連携するアプリが置かれます。SAP は RISE のアーキテクチャ全体を自分のサブスクリプションとテナントで作って管理し、使う技術要素の決定、検証、デプロイも担います。デプロイされた RISE の構成とカスタマイズは、顧客が SAP と相談して、自社の要件に合わせる形。[^c1-76]Microsoft が文書化するのは RISE と統合する部分で、SAP が使う詳細なアーキテクチャは SAP の知的財産のため対象外です。[^c1-40]

Azure のサポートの対象は、顧客自身のサブスクリプションのリソースだけです。SAP のサブスクリプションの中のリソースの問題は、SAP に問い合わせます。顧客は RISE のプロジェクトで、自分の Azure 環境、SAP が管理するワークロード、オンプレミスの間のインターフェースと受け渡しの地点を文書にします。文書にする項目は、アドレス空間、ファイアウォール、ルーティング、ファイル共有、DNS など。各インターフェースの担当者と、リソースが動いている場所も書いておき、トラブルシューティングやサポートの時に素早く引けるようにします。[^c1-40]

SAMPLE

接続の方式は、仮想ネットワーク ピアリングが優先です。最も性能が高く、プライベートなアドレス空間のまま通信が流れます。ピアリングした 2 つのネットワークは、接続の上では 1 つに見えます。トラフィックはインターネットを通りません。ピアリングの料金はかかります。代替は、VPN ゲートウェイ同士の vnet-to-vnet 接続です。スループットは両側のゲートウェイ SKU が上限になります。耐障害性のため、ゾーン冗長の仮想ネットワーク ゲートウェイを使います。[^c1-41]

RISE は SAP のテナントにあるので、異なるテナント間のピアリングになります。SAP が提供するネットワークのリソース ID を使ってピアリングを作り、SAP が承認します。相手のテナントのゲスト ユーザーを追加して招待を受け入れる手順も入ります。アドレス空間が重なるネットワーク同士はピアリングできません。IP アドレスの範囲は、事前に重ならないように決めます。詳しい手順は、SAP の担当に確かめます。[^c1-41]

Azure Virtual WAN のハブも使えます。RISE のワークロードを、vWAN ハブにつながるスポークとして扱います。vWAN ハブは、顧客がデプロイして管理します。ピアリングも VPN vnet-to-vnet も、vWAN で使えます。[^c1-41]

そのほかの決まりが 3 つあります。

- SAP は、一般に、RISE のワークロードへプライベート エンドポイントによる接続を顧客に提供しません。
- RISE の中で SAP が作った専用の ExpressRoute や VPN は、SAP が管理する仮想ネットワークにしか届かず、顧客自身の仮想ネットワークへのアクセスには使えません。
- インターネットとの通信は、既定では有効ではありません。既定のネットワークはプライベート IP の範囲だけです。

RISE との VNet ピアリングの実装、名前解決、オンプレミス [1.3.2]

ピアリングは、同じリージョンでも、グローバル ピアリングで離れたリージョンの間でも張れます。ただし、遅延とピアリングの費用の面から、RISE のリージョンは顧客のワークロードと同じリージョンに合わせます。世界中に拠点がある会社の中央の S/4HANA のように、グローバルに張る必要がある場合は、顧客側もマルチリージョンのネットワークを持ち、SAP のピアリングを各地域のハブにローカルで張る構成にします。[^c1-41]

ピアリングした両側の仮想ネットワークは NSG で保護し、SAP とデータベースのポートだけを許します。オプションのプレミアム サービスである Firewall as a Service（FWaaS）を有効にする場合は、RISE の VNet の 1 サブネットと顧客側の 1 サブネットの間で、サブネット ピアリングを設定します。仮想ネットワーク全体のピアリングは使いません。顧客側のサブネットには NVA などの経路のアプライアンスを置き、RISE と顧客のネットワークの間のトラフィックは、両側のアプライアンスを通ります。ファイアウォールのログは、RISE LogServ で取れます。[^c1-41]

オンプレミスへの経路は、顧客の既存のハブにある ExpressRoute か VPN のゲートウェイを使います。RISE の仮想ネットワークを、顧客のハブにつながるスポークとして扱います。ピアリングで「リモート ゲートウェイ トランジット」を有効にすると、オンプレミスから RISE のネットワークへ届きます。仮想ネットワークが持てるゲートウェイは、ローカルかリモートかを問わず 1 つだけです。そのため、リモート ゲートウェイ トランジットを使う場合、RISE の仮想ネットワークにゲートウェイを足すことはできません。[^c1-41]

DNS は、ゾーンを SAP に委任する形で統合します。

1. 顧客が、サブドメイン（ゾーン）を SAP に委任する。例は ecs.contoso.com。
2. 委任したゾーンでは、SAP の DNS サーバーがマスターになります。

SAMPLE

3. 顧客の DNS サーバーへ、DNS ゾーン転送で複製する。

RISE の仮想ネットワークでは、SAP の VM の 2 台が DNS サーバーになり、カスタム DNS を設定します。顧客側の仮想ネットワークも、ハブ仮想ネットワークの顧客 DNS サーバーを参照するカスタム DNS にします。任意で、Azure のサービスから来る要求を SAP の DNS サーバーへ転送するプライベート DNS フォワーダーも置けます。ゾーン転送が使えるのは、AD DS や BIND のような、顧客が運用するカスタム DNS サーバーです。[^c1-41]

ここで落とし穴があります。Azure 提供の DNS と Azure プライベート DNS ゾーンは、DNS ゾーン転送をサポートしません。そのため、SAP の DNS 複製の受け側にはできません。また、SAP は通常、委任したゾーンに外部の DNS サービス プロバイダーを使うことをサポートしません。[^c1-41]

RISE への移行は数か月以上かけて段階的に進みます。そのため、各フェーズでユーザーが届く経路と、データ転送の経路を計画します。後の工程でデータを移す最重要のシステムを考えずに、一時的な VPN を作らないようにします。多くのプロジェクトでは、最も大きく重要なシステムを中盤か終盤に移すからです。[^c1-41]

RISE の SAP と顧客の Azure サービスをつなぐ [1.3.3]

RISE の SAP とつなぐ時に使えるポートは決まっています。RFC（BAPI と IDoc）、OData と REST/SOAP 用の https、HANA への直接接続用の ODBC/JDBC です。これらはプライベートなピアリング経由で使い、パブリックな https は、SAP が管理する Application Gateway を通る経路もあります。ODBC/JDBC の直接接続は、SAP と合意してユーザーと経路を開けてもらった場合だけ使えます。[^c1-41]

SAP BTP との接続は、パブリックなインターフェース経由が基本です。SAP BTP と RISE の SAP がどちらも Azure で動いている場合、このインターネット向けの通信は、既定で Azure のバックボーンの中にとどまり、パブリックなインターネットには出ません。[^c1-67]顧客の Azure サブスクリプションの中のサービスは、中央のファイアウォールや送信用のパブリック IP のような、構成した送信の方法で BTP にアクセスし、SAP Cloud Connector が必要な場合も、顧客の VM で動かします。BTP の SAP Data Intelligence のように、パブリック エンドポイントではなく、別の仮想ネットワーク ピアリングでアクセスするサービスもあります。SAP Private Link Service は、BTP から始まる一方向の要求について、BTP のサービスをプライベート IP の範囲で顧客の Azure ネットワークにつなぎ、RISE で使えるかどうかは SAP に確かめます。[^c1-41]

送信の経路は、誰が持つかで分かれます。RISE の SAP が BTP などの公開エンドポイントへ出ていく通信は、SAP RISE/ECS が管理する経路を通ります。顧客自身のアプリが BTP や RISE の公開エンドポイントへ出ていく通信は、顧客が管理する経路を通ります。RISE のインターネット通信は、NSG、ASG、WAF 付きの Application Gateway、プロキシなどで保護され、すべて SAP が管理します。この経路は、通常 RISE の仮想ネットワークの中にとどまり、顧客の仮想ネットワークは通りません。[^c1-41]

データ統合のサービスは、接続の担当を分けて考えます。Data Factory や Synapse の統合ランタイム（IR）や、On-premises data gateway の VM は、顧客のサブスクリプションと仮想ネットワークに顧客がデプロイして運用します。RISE が提供するのはポートの公開までで、接続するアプリの詳細は把握もサポートもしません。Azure Monitor for SAP solutions と Azure Center for SAP solutions は、RISE とは一切統合できません。SAP のサブスクリプションの中のリソースに、顧客はアクセスできないからです。[^c1-42]

SAMPLE

SAP データを Azure のデータ サービスへ [1.3.4]

Azure Data Factory、Synapse Analytics、Microsoft Fabric、Microsoft Purview は、統合ランタイム（IR）を経由して SAP と接続します。Azure IR と self-hosted IR のどちらを使えるかは、コネクタで決まります。SAP のコネクタの多くは、self-hosted IR だけで使えます。SAP ECC コネクタは、両方で使えます。[^c1-43]

IR によって、ネットワークの経路が変わります。Azure IR は、RISE が Application Gateway で公開するパブリック IP に、https でアクセスします。self-hosted IR は、ピアリングで張ったプライベートな経路を、プライベートなアドレスだけで使い、NSG の規則が、どのアプリが SAP と通信できるかを制限します。SAP table、SAP BW、SAP OpenHub のコネクタは SAP .NET コネクタを使い、SAP 側の関数モジュールを RFC で実行し、HANA への ODBC/JDBC は、合意があれば self-hosted IR から使えます。[^c1-43]

Logic Apps、Power Apps、Power BI は、On-premises data gateway を経由して SAP とやり取りします。ゲートウェイは Azure またはオンプレミスで動く VM で、SAP RFC のランタイムとドライバーのサポートを含みます。顧客の環境にデプロイした Azure API Management は、要求のスロットリング、使用量のクォータ、SAP Principal Propagation を提供し、Microsoft 365 で認証された呼び出し元の SAP 側の権限を保ちます。Power Apps、Power BI、Azure Functions、App Service などの利用側を統制して守るのも、この API Management。[^c1-68]SAP のデータに外部アプリから触れる時の影響は、SAP のライセンスの詳細を SAP に確かめます。[^c1-43]

データのアーカイブは、データの置き場所の階層で考えます。HANA のデータは、Hot、Warm、Cold の 3 階層です。Hot は、インメモリの頻繁にアクセスされるデータ、Warm は、HANA のストレージ階層、Cold は、低コストのストレージにある稀にしか使わないデータです。関連する略称は次の通りです。[^c1-44]

略称	意味
NSE	Native Storage Extension（インメモリの列ストアのディスク拡張）
DLM	Data Lifecycle Management
NLS	Near-Line Storage
ADLS	Azure Data Lake Storage

Warm 階層の選択は、製品で決まります。Native HANA は Dynamic Tiering、Extension Node、NSE から選びます。S/4HANA と Business Suite は NSE だけで、BW/4HANA と BW on HANA は、NSE か Extension Node です。Cold 階層は、S/4HANA と Business Suite が SAP IQ、BW が NLS（SAP IQ か Hadoop）か Data Intelligence と ADLS、Native HANA が DLM と Data Intelligence か Hadoop です。[^c1-44]

NSE には前提があります。SAP HANA 2.0 SPS 04 以降が必要です。NSE のバッファー キャッシュは、既定で HANA のメモリの 10% です。データのアーカイブと違って元に戻せますが、HANA のディスク サイズは減りません。Extension Node は、スケールアウト構成が必要で、追加のライセンスは不要（HANA の標準ライセンス）です。標準ノードと OS、ネットワーク、ディスクを共有できません。[^c1-44]

RISE の ABAP 環境から Azure のサービスを呼ぶには、ABAP SDK for Azure と Microsoft AI SDK for SAP を使います。導入には、abapGit を先に設定しておく必要があります。[^c1-68]

SAMPLE

RISE と Microsoft Entra ID、Microsoft Sentinel、顧客のセキュリティ [1.3.5]

RISE の SAP でも、Microsoft Entra ID の SSO の実装手順は、通常の SAP と変わりません。NetWeaver、Fiori、HANA 向けの Entra のチュートリアルをそのまま使います。方式の使い分けは、1.2.3 の表の通りで、SAML/OAuth と SNC の設定は顧客が行い、SPNEGO は顧客と SAP が一緒に行います。RISE では Windows のシステムが顧客の AD ドメインに統合されません。Kerberos の SSO にドメイン統合は不要で、クライアント端末が読んだドメインのトークンを SAP システムと安全にやり取りします。AD ベースの SSO の変更は、SAP に連絡します。SAP SSO Secure Login Client 以外のサードパーティ製品を使う場合は、RISE の管理対象のシステムの構成を変える必要が出ることがあるので、SAP の関与が要ります。[^c1-77][^c1-45]

Microsoft Sentinel には、SAP 向けのソリューションが 2 種類あります。Microsoft Sentinel solution for SAP applications は、アプリ層、DB、OS を対象にします。SAP BTP 向けのソリューションは独立していて、単独でも展開できます。前者は、SAP ECC、Business Suite、NetWeaver 系（任意のクラウドとオンプレミス）と、S/4HANA Cloud Private Edition（RISE）向けに認定されています。[^c1-46]

RISE でのデプロイの責任は、顧客にあります。Sentinel のソリューションは、顧客の Azure サブスクリプションにデプロイして、顧客がすべて管理します。SAP 経由ではありません。データ コネクタ エージェントは、顧客のサブスクリプション内の中継用の VM かコンテナーで動きます。SAP BTP への接続は、Audit Log Management Service の SAP の公開 API を使います。[^c1-45]

RISE の共有責任モデルには、ログの範囲の制約があります。Sentinel のソリューションで統合できるのは、SAP のアプリ層だけです。RISE のインフラと OS のログは、オプションの SAP LogServ 経由でしか取れず、LogServ は Sentinel との統合をネイティブにサポートします。自動応答（SOAR）の最初の定番のシナリオは、事前に作られたプレイブックで、Teams で確認しながら SAP のユーザーをブロックする流れ。この連携の型は、任意のインシデントの種類に使え、BTP や Microsoft Entra ID の側のアクセスも、ブロックの対象にできます。[^c1-77]Microsoft Security Copilot は、Sentinel のソリューションを通した取り込みで、RISE の SAP にも使えます。[^c1-45]

場面で考えます。RISE の SAP で、OS のレベルの不審な操作も Sentinel で検知したい、という要望が出たとします。Sentinel のソリューションは、SAP のアプリ層までしか見られません。OS とインフラのログは、SAP LogServ を契約して、その出力を Sentinel につなぎ、ソリューションそのものは、顧客の Azure サブスクリプションに顧客が展開します。

セキュリティで顧客が担うのは、Entra ID による SSO の設定、接続（ピアリング、NSG、DNS）、顧客のサブスクリプションの中の監視と Sentinel の運用です。SAP が担うのは、RISE のインフラと OS、SAP のサブスクリプションの中のリソースの運用、LogServ、FWaaS の運用です。RISE の SAP は、Azure Monitor for SAP solutions とも ACSS とも統合されず、SAP 自身の監視とレポートが、サービス記述書に定めた形で提供されます。[^c1-45]

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、AZ-120 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

AZ-120 学習用テキスト(無料サンプル)

版
2026年11月版(AZ-120 出題範囲(Microsoft Learn 公式 Study guide・Skills measured as of April 17, 2026)準拠)

発行
IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ
info@shikaku-doujou.com

Microsoft、Azure および Microsoft の製品名・サービス名は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

SAP、SAP HANA、SAP NetWeaver、SAP S/4HANA ほか SAP の製品名・サービス名は、SAP SE のドイツおよびその他の国における商標または登録商標です。本教材は公式シラバスの内容を基に作成したもので、Microsoft Corporation および SAP SE との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。

SAMPLE