

SAP Lens



SAP Lens: AWS Well-Architected Framework

Table of Contents

개요	i
렌즈 사용 방법	1
정의	3
워크로드 컨텍스트 점검 항목	5
Well-Architected 설계 원칙	6
운영 우수성	6
1 - 상태를 이해하고 대응할 수 있도록 SAP 워크로드를 설계	6
2 - SAP 변경의 결함 축소, 수정 용이화 및 워크플로 개선	17
3 - 워크로드가 어떻게 작동할지 이해	24
4 - 정기적으로 SAP 워크로드 검증 및 개선	29
보안	36
5 - 보안 표준 및 SAP 워크로드에 해당 표준이 적용되는 방식 이해	36
6 - 인프라 및 소프트웨어 제어를 사용하여 보안 구성 오류 감소	41
7 - 자격 증명 및 권한을 통해 SAP 워크로드에 대한 액세스 제어	49
8 - 저장 및 전송 중 SAP 데이터 보호	55
9 - 보안 이벤트 로그, 테스트 및 대응을 위한 보안 전략 구현	61
안정성	64
10 - 내결함 설계	64
11 - 장애 탐지 및 대응	73
12 - 데이터 복구 계획	82
성능 효율성	87
13 - 최적의 컴퓨팅 솔루션 선택	87
14 - 최적 스토리지 솔루션 선택	93
15 - 운영 체제, 데이터베이스 및 SAP 애플리케이션 계층에 대한 튜닝 옵션 평가	99
16 - 지속적인 성능 및 최적화 옵션 이해	104
비용 최적화	110
17 - SAP 아키텍처 패턴에서 비용 효율성 평가	110
18 - 비용 효율성을 위한 SAP 컴퓨팅 리소스 평가	122
19 - 스토리지 비용 효율성을 위해 SAP 데이터 사용 최적화	131
20 - 가시성, 계획 및 거버넌스로 비용 관리	139
결론	146
기여자	147
문서 이력	148
원칙별 설계 원칙	149

운영 우수성	149
보안	149
안정성	149
성능 효율성	149
비용 최적화	150
고지 사항	151
AWS Glossary	152

개요

게시 날짜: 2021년 10월 28일 ([문서 이력](#))

이 백서에서는 AWS Well-Architected Framework용 SAP Lens에 대해 설명합니다. 이 백서는 AWS 기반 SAP 워크로드가 Well-Architected 방식으로 설계되도록 보장하기 위해 고객에 의해 검증된 설계 원칙 및 모범 사례를 모은 것입니다. SAP Lens는 [AWS Well-Architected Framework](#)에 대한 보충 자료로 사용할 수 있습니다. 이 프레임워크는 AWS에서 안전하고, 고성능이고, 탄력적이고, 효율적인 애플리케이션 및 워크로드를 빌드하기 위한 기반을 제공합니다.

SAP Lens는 AWS가 고객, AWS 파트너 및 SAP 전문가 커뮤니티로부터 수집한 인사이트를 기반으로 합니다. 렌즈는 SAP 실행에 대한 클라우드 네이티브 접근 방식을 채택하는 데 도움이 되도록 설계되었습니다. 운영 우수성, 보안, 안정성, 성능 효율 및 비용 최적화라는 AWS Well-Architected Framework의 다섯 가지 원칙에 맞춰 가장 일반적인 개선 영역을 강조합니다.

이 백서에서 SAP는 AWS에서 실행되는 소프트웨어를 의미하며 전사적 자원 관리(ERP) 애플리케이션으로 가장 잘 알려진 회사 SAP에서 제공합니다. 이 지침은 SAP Business Suite, SAP S/4HANA 및 지원 제품을 포함하여 AWS에서 실행될 수 있는 모든 SAP 소프트웨어를 다루고자 했습니다. 권장 사항이 SAP 애플리케이션 또는 데이터베이스와 관련된 경우 해당 항목이 강조 표시됩니다(예: SAP HANA 데이터베이스).

이 문서가 대상으로 하는 독자는 AWS에서 SAP 시스템을 구축, 운영, 유지 관리하는 SAP 기술 아키텍트, 클라우드 아키텍트 및 팀원입니다.

렌즈 사용 방법

이 렌즈를 사용하여 구현 전, 도중 및 이후에 SAP on AWS 워크로드를 평가합니다. 이 렌즈는 AWS Well-Architected Framework에 대한 추가 콘텐츠를 제공하고 SAP 워크로드 설계의 기초가 되는 모범 사례를 해석 및 채택하는 방법을 명확하게 설명합니다.

SAP 및 엔터프라이즈 요구 사항을 해결하려면 엔터프라이즈 팀과 긴밀히 협력하면서 이 렌즈와 프레임워크를 함께 사용할 것을 권장합니다. 중복을 피하기 위해 AWS Well-Architected Framework에 대한 링크를 제공했습니다. 여기에 제공된 지침은 더 포괄적이거나 특정 SAP 컨텍스트를 다루지 않습니다.

이 렌즈를 사용하려면 다음 단계를 따르세요.

1. 이 문서와 더 광범위한 AWS Well-Architected Framework 및 원칙 백서를 숙지합니다.
2. SAP 관련 설계 문서, 운영 절차 및 모니터링 기록(사용 가능한 경우)을 수집합니다.

3. SAP 워크로드 구현 및 운영을 이 문서에 설명된 모범 사례와 비교합니다.
4. 각 모범 사례에 대해 준수 여부를 기록하고 필요한 모범 사례를 우선적으로 평가합니다.
5. 워크로드가 Well-Architected 방식으로 설계되지 않은 영역을 해결하기 위한 솔루션으로 제공된 제안을 사용합니다.

추가로 전문가 지원이 필요한 경우 AWS 계정 팀에 연락하여 SAP 전문 솔루션 아키텍트를 고용하세요.

워크로드를 검토한 후에는 워크로드가 Well-Architected 방식으로 설계된 영역과 개선이 필요한 영역을 보여주는 모범 사례 목록이 작성됩니다.

- Well-Architected 방식으로 설계된 아키텍처 구성 요소: 팀 간에 지식을 공유하여 조직 전체에서 이를 확대합니다.
- 워크로드가 아직 준수하지 않는 모범 사례: 비즈니스에 대한 기술 부채 및 위험으로 간주합니다. 내부 위험 관리 프로세스에 따라 이러한 위험을 지속적으로 모니터링하고 개선합니다.
- 추가 심층 분석 또는 개선 지원이 필요한 영역: AWS Professional Services에 문의하거나 [AWS SAP 인증 파트너 목록](#)에 나열된 AWS 파트너와 상의합니다.

자세한 내용은 다음 링크 및 정보를 참조하세요.

- AWS 설명서: [The Review Process\(검토 프로세스\) - AWS Well-Architected Framework](#)

정의

용어	설명	예(해당하는 경우)
SAP 워크로드	워크로드는 비즈니스 가치를 제공하는 SAP 리소스의 모음입니다. SAP 컨텍스트에서는 SAP의 고객 대면 구성 요소 및 SAP 백엔드 프로세스가 포함됩니다. 워크로드는 단일 AWS 계정 내 리소스의 하위 집합으로 구성되거나 여러 AWS 계정에 걸친 리소스의 집합이 될 수 있습니다.	
SAP 제품	모든 산업에서 비즈니스 프로세스에 대한 솔루션을 제공하는 엔터프라이즈 소프트웨어 회사인 SAP의 제품입니다. 때로는 SAP 솔루션 이라고 합니다.	SAP S/4HANA 온프레미스 에디션, Concur, Qualtrics
SAP 시스템	아키텍처(더 큰 메커니즘의 일부로 함께 작동하는 구성 요소의 집합)의 논리적 그룹화로, 일반적으로 SAP 시스템 식별자(SID)로 식별됩니다.	프로덕션 ERP 시스템
SAP 시스템 식별자(SAP SID/DB SID)	SAP 시스템을 고유하게 식별하는 데 사용되는 문자 및 숫자의 조합입니다.	PRD, HDB, PR1
SAP 환경	하나 이상의 SAP 제품 또는 기술 환경의 통합된 그룹화입니다. 연결되어 프로덕션까지의 경로를 형성합니다.	샌드박스, 개발, QA, 훈련, 테스트, 사전 프로덕션 및 프로덕션.
SAP 인스턴스 또는 호스트	인스턴스는 AWS 클라우드에서 가상 서버로 실행되는 Amazon Machine Image(AMI)의 복사본입니다. SAP 컨텍스트에서는 일반적으로 Amazon EC2 서비스의 컴퓨팅 인스턴스입니다.	

용어	설명	예(해당하는 경우)
SAP 기술 구성 요소	하나의 인스턴스 또는 호스트에서 실행되는 SAP 시스템의 구성 요소를 그룹화하는 관리 단위입니다. SAP 애플리케이션의 기술적 아키텍처 빌딩 블록입니다.	애플리케이션 서버 (PAS 또는 AAS), SAP HANA 데이터베이스, 웹 디스패처
서비스(AWS 서비스)	비즈니스 또는 조직의 요구 사항에 맞게 조합하여 사용되는 200개 이상의 클라우드 서비스입니다. 다양한 AWS 서비스에 대한 자세한 내용은 Amazon Web Services 개요 백서를 참조하세요.	Amazon EC2, Amazon S3, Amazon EFS
SAP 배포/배포 패턴	SAP 프로비저닝 도구(SUM, SWPM)의 옵션을 참조하여 SAP를 배포하는 방법을 설명하는 데 사용됩니다.	고가용성 (HA), 분산형, 독립 실행형
SAPS 등급(여러 위치에서 SAPS 라고 함)	SAP 애플리케이션 성능 표준(SAPS) - SAP 환경에서 시스템 구성의 성능을 설명하는 하드웨어 독립적 측정 단위입니다. 이 표준은 영업 및 유통(SD) 벤치마크에서 파생되며, 여기서 100 SAPS는 시간당 2,000개의 완전히 비즈니스 처리된 주문 라인 항목으로 정의됩니다. 자세한 내용은 다음을 참조하세요. SAP Standard Application Benchmarks(SAP 표준 애플리케이션 벤치마크) .	Amazon EC2 인스턴스 유형 <i>c5.large</i> 는 3,650 SAPS를 제공합니다.

AWS 설명서: [AWS 용어집](#)

워크로드 컨텍스트 점검 항목

비즈니스의 컨텍스트를 더 잘 이해하려면 다음 정보를 수집해야 합니다.

ID	우선순위	워크로드 컨텍스트
<input type="checkbox"/> C1	필수	워크로드의 이름
<input type="checkbox"/> C2	필수	비즈니스 목적, 핵심 성과 지표(KPI) 및 워크로드의 의도된 사용자가 포함된 설명
<input type="checkbox"/> C3	필수	렌즈 검토를 주도하는 검토 소유자
<input type="checkbox"/> C4	필수	워크로드를 유지 관리할 책임이 있는 워크로드 소유자
<input type="checkbox"/> C5	필수	워크로드를 후원하는 비즈니스 이해 관계자
<input type="checkbox"/> C6	필수	정보 보안, 재무, 법률 등 워크로드에 이해 관계가 있는 비즈니스 파트너
<input type="checkbox"/> C7	권장	워크로드를 설명하는 아키텍처 설계 문서
<input type="checkbox"/> C8	권장	워크로드와 연결된 AWS 계정 ID
<input type="checkbox"/> C9	권장	워크로드와 관련된 규정 준수 요구 사항(있는 경우)

Well-Architected 설계 원칙

이 섹션에서는 SAP 워크로드를 설계 및 운영할 때 관련된 설계 원칙, 모범 사례 및 개선 제안 사항에 대해 설명합니다.

또한 각 Well-Architected 원칙에 수록된 지침을 읽고 적용하는 것이 좋습니다. 여기에는 모든 워크로드와 관련된 운영 우수성, 보안, 안정성, 성능 효율성 및 비용 최적화에 대한 기초 모범 사례가 포함되어 있습니다.

원칙

- [운영 우수성](#)
- [보안](#)
- [안정성](#)
- [성능 효율성](#)
- [비용 최적화](#)

설계 원칙의 전체 목록은 다음을 참조하세요. [원칙별로 배열된 설계 원칙](#).

운영 우수성

운영 우수성 원칙은 효과적으로 워크로드를 개발 및 실행하고, 운영에 대한 인사이트를 얻고, 지원 프로세스를 지속적으로 개선하여 비즈니스 가치를 제공할 수 있는 능력에 초점을 맞춥니다.

이 섹션에서는 SAP 워크로드에 대한 지침을 제공하도록 특별히 맞춤화된 일련의 설계 원칙 및 권장 사항을 제공합니다. 유효 [운영 우수성 원칙](#)에는 보다 광범위한 설계 원칙 및 권장 사항이 포함되어 있습니다. 다음 SAP 지침과 함께 읽을 것을 적극 권장합니다.

1 - 상태를 이해하고 대응할 수 있도록 SAP 워크로드를 설계

해당 상태를 파악할 수 있도록 SAP 워크로드를 어떻게 설계합니까? 모든 구성 요소에서 내부 및 외부 상태를 파악하는 데 필요한 정보를 제공하도록 SAP 워크로드를 설계합니다. 인프라, SAP 기술/기초, 프런트 엔드 및 네트워크 구성 요소를 고려합니다. 실시간 모니터링이 가능하도록 지표를 캡처하는 모니터링 및 로깅 접근 방식을 설계하고 수정 및 사후 이벤트 분석이 가능하도록 기록 로깅을 설계합니다.

ID	우선순위	모범 사례
□ BP 1.1	필수	SAP on AWS 모니터링을 위한 사전 조건을 구현
□ BP 1.2	필수	SAP에 대한 인프라 모니터링을 구현
□ BP 1.3	필수	SAP에 대한 개별 애플리케이션 모니터링을 구현
□ BP 1.4	적극 권장	워크로드 구성 모니터링을 구현
□ BP 1.5	적극 권장	사용자 활동 모니터링을 구현
□ BP 1.6	적극 권장	종속성 모니터링을 구현
□ BP 1.7	권장	SAP 워크로드에 대한 단일 창 상태 모니터링을 구현
□ BP 1.8	권장	자동 응답 및 복구 기술을 사용하여 모니터링 경고에 대응

자세한 내용은 다음 링크 및 정보를 참조하세요.

- AWS 설명서: [AWS Data Provider for SAP\(SAP용 AWS Data Provider\)](#)
- AWS 서비스: [Amazon CloudWatch](#)
- SAP on AWS 블로그: [SAP용 서버리스 모니터링](#)
- SAP on AWS 블로그: [AWS DevOps for SAP - driving innovation and lowering costs\(SAP용 AWS DevOps - 혁신을 촉진하고 비용을 절감\)](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)
- SAP Note: [1656250 - SAP on AWS: Support Prerequisites\(1656250 - SAP on AWS: 지원 사전 조건\)](#) [SAP 포털 액세스 권한 필요]
- SAP 설명서: [SAP Solution Manager 7.2 - Application Operations\(애플리케이션 운영\)](#)

모범 사례 1.1 - SAP on AWS 모니터링을 위한 사전 조건 구현

SAP on AWS에 대한 SAP 인증 요구 사항은 SAP Note 1656250에 나와 있습니다. 이 노트에는 SAP용 AWS Data Provider를 설정하고, Amazon CloudWatch 세부 모니터링을 활성화하고, SAP NetWeaver 솔루션에 SAP 고급 모니터링을 사용하기 위한 지침이 포함되어 있습니다. 이러한 사전 조건을 활성화하면 AWS 및 SAP에서 SAP 워크로드 상태를 완전히 이해하고 조사하는 데 도움이 됩니다. 이러한 사전 조건을 전체 SAP 모니터링 전략에 반영해야 합니다.

제안 사항 1.1.1 - SAP 지원 사전 조건을 확인

SAP 지원 포털에서 SAP Note 1656250을 읽고 SAP on AWS 워크로드에 대한 최신 지원 요구 사항을 확인합니다. 이 노트에서 제공하는 세부 지침을 따릅니다.

- SAP Note: [1656250 - SAP on AWS: Support Prerequisites\(1656250 - SAP on AWS: 지원 사전 조건\)](#) [SAP 포털 액세스 권한 필요]

제안 사항 1.1.2 - SAP NetWeaver 워크로드용 AWS Data Provider를 설치

SAP용 AWS Data Provider는 SAP NetWeaver 워크로드를 지원하는 각 EC2 인스턴스에 반드시 설치해야 합니다. SAP용 AWS Data Provider는 AWS 서비스에서 성능 관련 지표를 수집하여 SAP 내부 애플리케이션 모니터링 시스템에 제공하는 에이전트입니다. 트랜잭션 코드 ST06n 및 Solution Manager 모니터링과 같이 일반적으로 SAPOSCOL 서비스에 수집되는 외부 지표를 사용하는 SAP 도구가 AWS 지표에 액세스하려면 SAP용 AWS Data Provider가 필요합니다.

SAP가 특정 간격으로 모니터링 데이터를 수신하는 데 필요한 세부 모니터링 및 증가된 API 호출로 인해 SAP용 AWS Data Provider 실행과 관련된 간접 비용이 발생합니다. 자세한 내용은 [SAP용 AWS Data Provider 설치](#) 를 참조하세요. 때문에 SAP 지원 및 분석이 필요한 경우 SAP용 AWS Data Provider를 비프로덕션 환경에서만 활성화하는 것을 고려해야 할 수도 있습니다.

- AWS 설명서: [AWS Data Provider for SAP\(SAP용 AWS Data Provider\)](#)

제안 사항 1.1.3 - SAP 워크로드에 대한 모니터링 전략을 수립

내부 및 외부 관점 모두에서 SAP 애플리케이션의 현재 및 과거 상태를 관찰하는 방법을 결정합니다. 최종 사용자 경험을 제공하기 위해 함께 작동하는 모든 구성 요소를 고려합니다. 내부 SAP 애플리케이션 지표 모니터링, 외부 사용자 성능 및 안정성 모니터링 외에도 기본 AWS 컴퓨팅, 스토리지 및 네트워크 서비스에서 지표를 캡처할 방법을 고려합니다. 각 구성 요소에 대해 다양한 도구를 평가하고 필요한 경우 근본 원인 분석을 수행하기 위해 이러한 도구를 단일 위치(예: 로그 집계)로 모을 수 있는 방법을 결정합니다. 이 정보를 사용하여 임계값이 위반되었을 때 수행할 경고 임계값 및 수정 조치를 설계하는 방법을 결정합니다.

설계의 출발점으로 사용자 지정 SAP 모니터링 지표를 수집할 수 있는 SAP Solution Manager 모니터링, 서드 파티 모니터링 도구 및 CloudWatch 대시보드의 기능을 이해합니다.

- AWS 설명서: [SAP NetWeaver on AWS: 모니터링 가이드](#)
- SAP on AWS 블로그: [SAP NetWeaver용 서버리스 모니터링](#)

- SAP on AWS 블로그: [SAP HANA용 서버리스 모니터링](#)
- AWS 서비스 동영상: [Gaining Better Observability of Your VMs with Amazon CloudWatch\(Amazon CloudWatch를 사용하여 VM에 대한 관찰 가능성 향상\)](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)
- SAP 설명서: [SAP Solution Manager 7.2 - Application Operations\(애플리케이션 운영\)](#)
- SAP 설명서: [SAP NetWeaver Alert Monitor](#)

모범 사례 1.2 – SAP에 대한 인프라 모니터링 구현

SAP 애플리케이션을 실행하고 사용자를 지원하는 데 사용되는 지원 서비스에 대한 정보를 제공하도록 인프라 모니터링을 설정합니다. 예를 들면 CPU 및 메모리 사용률, 스토리지 및 파일 시스템 사용률, 성능(IOPS 및 처리량), 네트워크 처리량이 있습니다. 온프레미스 Active Directory 서비스, DNS, 서드 파티 도구(예: 고가용성(HA) 및 백업 소프트웨어) 등 SAP에서 사용되는 모든 종속 기초 서비스를 포함합니다. DataDog, Splunk, DynaTrace, Avanza와 같이 이 정보의 연관성을 분석 및 시각화하는 데 도움이 될 수 있는 AWS Marketplace의 AWS 도구 및 SAP 관련 도구를 평가합니다. 이 정보를 사용하여 추세를 식별하고 시정 조치가 필요한 시기를 결정합니다.

제안 사항 1.2.1 - SAP를 지원하는 서비스에 대한 CloudWatch 지표 및 경보를 구현

모든 SAP 시스템에 대한 경보가 포함된 Amazon CloudWatch 세부 모니터링 지표 및 임계값을 구현합니다. 이러한 지표 및 경보에는 SAP 시스템 가용성 및 성능에 영향을 미칠 수 있는 일반적인 문제에 대한 모니터링이 포함되어야 합니다. 공통 인프라 모니터링 영역은 Amazon Elastic Compute Cloud(EC2) 인스턴스, Amazon Elastic Block Storage(Amazon EBS) 볼륨, Elastic Load Balancing(ELB)에 중점을 둡니다.

공통 모니터링 항목에는 다음이 포함됩니다.

- Amazon EC2 높은 CPU 사용률
- Amazon EC2 높은 메모리 사용률
- Amazon EBS 스토리지 페이지징
- Amazon EBS 스토리지 처리량
- Amazon EBS 스토리지 IOPS
- Amazon EBS 스토리지 공간 여유 및 볼륨 사용 %
- Amazon EC2 네트워크 포화도
- ELB/ALB 상태 및 대상 그룹 상태

시스템을 과거에 프로덕션 환경에서 사용했을 때 정상 패턴을 기준으로 경고 임계값을 설정합니다. 경고 임계값을 지속적으로 검토 및 조정하여 문제를 예방합니다.

시작하려면 다음 리소스를 검토하세요.

- SAP on AWS 블로그: [SAP NetWeaver용 서버리스 모니터링](#)
- SAP on AWS 블로그: [SAP HANA용 서버리스 모니터링](#)
- AWS 설명서: [CloudWatch 사용자 지정 지표 생성](#)
- AWS 설명서: [CloudWatch 대시보드 생성](#)
- AWS 설명서: [CloudWatch 경고 사용](#)

제안 사항 1.2.2 - SAP 서비스에 대한 AWS 서비스 할당량 모니터링을 구현

환경의 필수 SAP 리소스에 대한 [AWS 서비스 할당량](#) 을 추적하기 위한 모니터링 도구 또는 프로세스를 구현합니다. SAP 환경은 종종 Amazon EC2 인스턴스 유형을 혼합하여 사용할 수 있다는 점과 일부 유형은 [온디맨드 서비스 할당량](#) 이 다르다는 점을 고려합니다. 예를 들면 x1* 및 u* EC2 인스턴스 유형의 서비스 할당량은 c5 , m5 및 r5 인스턴스 유형의 결합 할당량과 별개입니다. 새로운 워크로드를 계획하거나 기존 워크로드를 확장할 때 서비스 할당량이 이를 지원하는지 확인하고 할당량 증가가 필요한 경우 AWS Support에 요청합니다.

- AWS 설명서: [Service Quotas - AWS 일반 참조](#)
- AWS 설명서: [온디맨드 인스턴스 - Amazon Elastic Compute Cloud Service 할당량](#)
- AWS 설명서: [할당량 증가 요청 - Service Quotas](#)

모범 사례 1.3 - SAP에 대한 개별 애플리케이션 모니터링 구현

애플리케이션 및 데이터베이스 모니터링을 설정하여 내부 상태 및 비즈니스 성과 달성 관련 정보를 제공합니다. 예를 들면 트랜잭션 응답 시간, 사용 가능한 작업 프로세스, 대기열 깊이, 오류 및 덤프 메시지, 중단된 배치 작업, 트랜잭션 처리량이 있습니다. 이 정보를 사용하여 시정 조치가 필요한 시기를 결정합니다.

제안 사항 1.3.1 - SAP 애플리케이션을 지원하는 데이터베이스에 대한 모니터링을 구현

SAP 데이터베이스를 지속적으로 모니터링하고 SAP 시스템 가용성 및 성능에 영향을 미칠 수 있는 일반적인 문제에 대한 경고를 설정합니다. 공통 모니터링 항목에는 다음이 포함됩니다.

- 데이터 영역의 여유 공간
- 로깅 영역의 여유 공간

- 과도한 잠금 활동
- 캐시 사용률
- 평균 쿼리 응답 시간
- 필요한 보안 패치 및 핫 픽스
- 상위 테이블 크기 및 증가율

시스템을 과거에 프로덕션 환경에서 사용했을 때 정상 패턴을 기준으로 경고 임계값을 설정합니다. 경고 임계값을 지속적으로 검토 및 조정하여 문제를 예방하고 워크로드 변동 또는 증가에 대응합니다.

특정 데이터베이스에 대한 모니터링을 활성화하는 자세한 방법은 데이터베이스 소프트웨어 공급자 설치 및 운영 가이드를 참조하세요.

제안 사항 1.3.2 - SAP 트랜잭션 및 도구를 사용하여 SAP 애플리케이션을 이해

내부 상태 및 비즈니스 성과 달성에 대한 정보를 제공하도록 SAP 애플리케이션을 구성합니다. 이 정보를 사용하여 대응이 필요한 경우를 확인합니다. 공통 모니터링 항목에는 다음이 포함됩니다.

- 애플리케이션(ASCS, PAS, AAS) 및 데이터베이스 서비스의 가용성
- 활성 및 동시 사용자 수
- 사용자에게 대한 작업 프로세스의 가용성
- 사용자 트랜잭션의 응답 시간
- 배치 및 비대화형 트랜잭션의 응답 시간
- 오류 메시지 및 덤프
- 실패한 작업
- 가득 찬 대기열 및 느린 대기열

SAP Solution Manager에서 [SAP EarlyWatch Alert 보고 시스템](#) 을 설정하여 SAP 시스템의 상태에 대한 정기 보고서를 생성합니다. 이러한 보고서에서 발견된 문제를 정기적으로 검토 및 수정하여 문제를 예방하고 워크로드 서비스 중단을 방지합니다.

- SAP Note: [2729186 - EWA 생성의 일반 프로세스](#) [SAP 포털 액세스 권한 필요]
- SAP 설명서: [SAP Solution Manager 7.2 - Application Operations\(애플리케이션 운영\)](#)
- SAP Lens [성능 효율성]: [모범 사례 16.1 - 성능 평가를 위한 데이터 확보](#)

제안 사항 1.3.3 - 데이터 복구 및 보호 메커니즘에 대한 모니터링을 구현

장애 또는 재해 발생 시 SAP 데이터를 보호하는 메커니즘에 대한 모니터링을 구현합니다. 공통 모니터링 항목에는 다음이 포함됩니다.

- 정기 데이터베이스 백업에 대한 경고(예: AWS Backint Agent를 사용하여 Amazon S3로 백업)
- 데이터베이스 복제에 대한 경고(예: 가용 영역 간의 HANA 시스템 복제 실패 또는 지연)
- 파일 스토리지 백업에 대한 경고(예: EBS 스냅샷, Amazon EFS 백업 또는 Amazon FSx 백업)
- 리전 간에 데이터 복원력을 제공하는 복구 메커니즘에 대한 경고(예: 리전 간 복제, Amazon S3 sync 또는 CloudEndure Disaster Recovery를 사용하는 Amazon S3 버킷)
- 계정 간에 데이터 복원력을 제공하는 복구 메커니즘에 대한 경고(예: WORM S3 버킷 또는 로깅 계정에 대한 동일 리전 복제를 사용하는 Amazon S3 버킷)

자세한 내용은 다음 링크를 참조하세요.

- AWS 블로그: [AWS Backup Audit Manager를 사용하여 백업 규정 준수 모니터링, 평가 및 입증](#)
- SAP 설명서: [SAP HANA 시스템 복제 확인 및 모니터링](#)

제안 사항 1.3.4 - 독립적 관찰을 위해 SAP 모니터링 데이터를 SAP 도구 외부에 노출

SAP 모니터링 도구는 애플리케이션 및 운영 체제 수준 모니터링으로 제한되며 SAP 서비스 가용성 및 상태에 대한 엔드투엔드 보기를 제공하는 광범위한 지원 서비스가 아닙니다. 보다 전체적인 외부 모니터링 및 시각화 도구를 선택하고 이 도구에 지표를 제공하도록 SAP 애플리케이션을 구성합니다.

이전 모범 사례에서 수집한 지표를 사용하고 해당 결과를 외부에 제공하여 추세를 모니터링, 경고 및 보고할 수 있는 독립적인 도구를 확보합니다. 독립적인 도구를 사용하면 SAP 시스템의 가용성이 없어도(즉, SAP가 재해 또는 장애 모드에 있는 경우에도) 관찰 가능성, 근본 원인 분석, 기록 및 추세 보고가 가능합니다.

- SAP on AWS 블로그: [SAP NetWeaver용 서버리스 모니터링](#)
- SAP on AWS 블로그: [SAP HANA용 서버리스 모니터링](#)
- AWS 설명서: [CloudWatch 사용자 지정 지표 생성](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)

모범 사례 1.4 - 워크로드 구성 모니터링 구현

현재 구성 및 구성 변경에 대한 정보를 제공하도록 워크로드를 설계 및 구성합니다. 예를 들면 EC2 인스턴스 신규 생성 또는 제거, 크기 조정 이벤트, 코드 변경, 패치 수준, 보안 그룹 구성, 리소스 삭제 등

이 이에 해당합니다. 이 정보를 사용하여 대응이 필요한 경우를 확인하고 변경이 예상 또는 허용되었는지 여부를 파악합니다. 구성 변경의 비용 영향을 모니터링하고 필요한 경우 예산을 조정 또는 분석합니다.

제안 사항 1.4.1 - 워크로드 구성 모니터링을 구현

특히 SAP 프로덕션 계정에서 높은 우선 순위 및 중요한 이벤트를 모니터링하도록 AWS CloudTrail을 설정 및 구성합니다. 예를 들면 새 Amazon EC2 인스턴스, Amazon EC2 폐기 또는 변경, 보안 그룹 변경, AWS KMS 및 IAM 보안 변경 이벤트가 있습니다. 이러한 이벤트를 사용하여 CloudWatch 로그 경보(필요한 경우)를 구성하고 예상치 않은 변경이 발생할 경우 조치를 취합니다.

- AWS 설명서: [AWS CloudTrail이란 무엇입니까?](#)
- AWS 서비스: [AWS CloudTrail](#)
- AWS 설명서: [Amazon CloudWatch Logs를 사용하여 CloudTrail 로그 파일 모니터링](#)
- AWS 설명서: [AWS CloudTrail 보안 모범 사례](#)

제안 사항 1.4.2 - 워크로드 구성 적용 및 수정을 구현

SAP 프로덕션 애플리케이션을 지원하는 AWS 리소스의 구성 정책을 추적, 평가 및 적용하도록 AWS Config를 설정 및 구성합니다. 일반적인 예로는 SAP 백업이 포함된 S3 버킷에 대한 읽기 전용 보호 적용, 필수 Amazon EC2 EBS 암호화, 공통 네트워크 포트 차단, 모든 리소스에 필수 태그가 있는지 확인 등이 있습니다. AWS Config [관리형 규칙](#) 을 사용하여 SAP를 지원하는 AWS 환경의 보안 및 변경 제어 태세를 개선합니다. AWS 태그를 사용하여 구성 규칙을 적용하고 가능한 경우 자동 수정을 적용합니다.

- AWS 서비스: [AWS Config](#)
- AWS 설명서: [AWS Config 시작하기](#)
- AWS 설명서: [AWS Config 규칙 사용](#)
- SAP on AWS 블로그: [AWS Config를 사용하여 SAP 시스템 감사 - 1부](#)
- SAP on AWS 블로그: [AWS Config를 사용하여 SAP 시스템 감사 - 2부](#)
- SAP on AWS 블로그: [SAP on AWS 태깅 권장 사항](#)

제안 사항 1.4.3 - 워크로드 비용 모니터링을 구현

결제 임계값을 초과할 경우(또는 초과가 예상될 경우) 알림을 제공하는 사용자 지정 예산을 사용하여 [AWS Budgets](#) 를 설정 및 구성합니다. 예산을 추정 SAP 환경 지출에 부합하도록 설정하고 이상을 모

니터링하여 비용 초과를 방지합니다. 예산 보고서를 사용하여 예약 인스턴스 및 Savings Plans의 사용 및 적용 범위를 모니터링합니다. SAP 워크로드 간에 비용 할당 및 사용 현황을 파악하는 데 도움이 되도록 AWS 태그를 사용합니다.

- AWS 블로그: [AWS Budgets 시작하기](#)
- AWS 블로그: [AWS Budgets 보고서](#)
- AWS 설명서: [AWS Cost Explorer](#)
- AWS 설명서: [AWS Cost Anomaly Detection](#)
- SAP on AWS 블로그: [SAP on AWS 태깅 권장 사항](#)

모범 사례 1.5 - 사용자 활동 모니터링 구현

응답 시간, 활성 사용자 수, 트랜잭션 포기 비율, 주문 처리 시간과 같은 사용자 활동에 대한 정보를 제공하도록 SAP 애플리케이션을 구성합니다. 경험에서 연결이 어떤 역할을 하는지 이해할 수 있도록 내부 접근 방식(SAP 내부 대화 응답 시간 모니터링)과 외부 접근 방식(최종 사용자 위치에 에이전트 또는 로봇을 지리적으로 배포)을 모두 고려합니다. 이 정보를 사용하면 애플리케이션 사용 방법 및 사용 패턴을 파악하고 성능 불량으로 인해 대응이 필요한 경우를 확인할 수 있습니다.

제안 사항 1.5.1 - 최종 사용자 위치에서 사용자 경험 모니터링을 구현

SAP 사용자 경험에서 네트워크 및 연결이 어떤 역할을 하는지 이해할 수 있도록 최종 사용자 위치에 사용자 에이전트 또는 로봇을 지리적으로 배포하여 외부 모니터링 접근 방식을 고려합니다. 종종 이러한 유형의 최종 사용자 위치 기반 모니터링은 중앙 인프라 및 애플리케이션에서 감지할 수 없는 문제에 대한 인사이트와 조기 경고를 제공할 수 있습니다.

최종 사용자 위치에서 SAP 애플리케이션의 응답성을 측정할 수 있도록 최종 사용자 경험 보고를 제공하는 SAP 또는 서드 파티 도구를 구현합니다. 예를 들어 SAP는 Solution Manager에서 최종 사용자 경험 모니터링을 제공하며, 여러 서드 파티 제품은 원격 위치에 로봇(또는 모니터링 스크립트)을 배포하여 사용자 경험을 측정할 수 있습니다.

- SAP 설명서: [SAP 사용자 경험 모니터링](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)

모범 사례 1.6 - 종속성 모니터링 구현

종속된 리소스의 상태에 대한 정보(예: 도달 가능성 또는 응답 시간)를 제공하도록 워크로드를 구성합니다. 외부 종속성의 예에는 인터페이스(예: SAP PI/PO를 통한), 외부 데이터 스토어, DNS, 온프레미

스 구성 요소, Active Directory 컨트롤러, 네트워크 디바이스가 포함될 수 있습니다. 이 정보를 사용하여 대응이 필요한 경우를 확인합니다. 엔드투엔드 종속성의 상태를 모니터링할 수 있도록 교차 기술 지표를 제공할 수 있는 타사 모니터링 도구를 고려합니다.

제안 사항 1.6.1 - 주요 SAP 인터페이스 및 시스템 간 비즈니스 프로세스에 대한 상태 추적을 구현

SAP 워크로드가 종속된 주요 인터페이스를 식별 및 모니터링합니다. 이러한 인터페이스 엔드포인트의 상태, 오류, 대기열 길이 및 성공 비율을 모니터링합니다. SAP 또는 서드 파티 통합 도구에서 기본 제공하는 메커니즘을 사용하여 인터페이스 장애 또는 지연에 대한 경고를 설정하고 이를 모니터링 도구에 제공합니다. 모든 인터페이스 경로를 고려합니다.

- AWS 호스팅 SAP 시스템 간(RFC 또는 웹 서비스/HTTPS를 통해 직접)
- AWS 호스팅 SAP 시스템과 온프레미스 시스템 간(HTTPS/SFTP - SAP PI 또는 서드 파티 통합 플랫폼을 통해)
- AWS 호스팅 SAP 시스템과 SAP Business Technology Platform 간(SAP Cloud Connector를 통해)
- AWS 호스팅 SAP 시스템과 외부 시스템 간(일반적으로 HTTPS를 통해 인터넷/VPN을 경유)

SAP 환경과 비 SAP 환경 전반에서의 시스템 간 종속성 모니터링을 위해 Solution Manager 비즈니스 프로세스 모니터링을 고려합니다.

- SAP 설명서: [SAP 비즈니스 프로세스 및 인터페이스 모니터링](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)

제안 사항 1.6.2 - SAP가 종속된 엔터프라이즈 서비스에 대한 상태 추적을 구현

SAP 워크로드는 일반적으로 비즈니스 사용자에게 대해 정상 상태를 유지하기 위해 몇 가지 기초 엔터프라이즈 서비스에 종속됩니다. 모니터링 접근 방식 및 도구에서 이러한 기초 서비스를 고려합니다. 기초 서비스의 예로는 온프레미스 시스템 연결을 위한 Direct Connect, 인증/SSO를 위한 Active Directory, 시간 동기화를 위한 Network Time Protocol(NTP), 바이러스 백신 서비스 및 운영 체제 패치 리포지토리(예: Microsoft Windows Update 또는 SUSE 패치)에 대한 연결이 있습니다.

- AWS 블로그: [AWS Systems Manager 통합 Amazon CloudWatch 에이전트 - Linux 및 Windows용 통합 지표 및 로그 수집](#)
- AWS 설명서: [CloudWatch 에이전트를 사용하여 Amazon EC2 인스턴스 및 온프레미스 서버로부터 지표 및 로그 수집](#)
- AWS 설명서: [AWS Direct Connect에 대한 고급 모니터링 기능](#)

모범 사례 1.7 - SAP 워크로드에 대한 단일 창 상태 모니터링 구현

워크로드 전반에 걸친 트랜잭션 흐름 관련 정보를 제공하도록 SAP 애플리케이션, AWS 서비스 및 종속 구성 요소를 구성합니다. 여러 소스의 지표를 결합하여 SAP 워크로드의 상태에 대한 단일 창 시각화를 생성하고 주요 사용자가 이 대시보드에 액세스할 수 있도록 합니다. 이 정보를 사용하면 대응이 필요한 경우를 확인하고 비즈니스에 악영향을 미치는 문제의 원인을 신속하게 파악할 수 있습니다.

제안 사항 1.7.1 - 애플리케이션 지표, 워크로드 구성, 사용자 지표 및 종속성 상태를 단일 위치에 결합

최종 사용자 비즈니스 프로세스에 대한 SAP 워크로드 및 해당 상태의 엔드투엔드 모니터링이 가능하도록 애플리케이션 모니터링 지표, 워크로드 구성 데이터, 사용자 지표 및 종속성 상태를 단일 위치 또는 도구에 결합합니다. 이 작업은 SAP Solution Manager, 맞춤형 CloudWatch 대시보드 및 지표 또는 서드 파티 모니터링 도구를 사용하여 달성할 수 있습니다.

모범 사례는 워크로드 가용성에 대한 드릴다운 보기가 가능하도록 트래픽 상태 및 추세가 포함된 비즈니스 대면 상태 대시보드를 생성하는 것입니다. 드릴다운 기능을 통해 사용자와 운영자는 기술 스택에서 문제 또는 성능 저하를 일으킬 수 있는 특정 구성 요소를 평가할 수 있습니다.

- AWS 설명서: [CloudWatch 대시보드 생성](#)
- SAP on AWS 블로그: [SAP NetWeaver용 서버리스 모니터링](#)
- SAP on AWS 블로그: [SAP HANA용 서버리스 모니터링](#)
- AWS Marketplace: [SAP 모니터링을 위한 제품 및 도구](#)
- SAP 설명서: [SAP Solution Manager 7.2 - Application Operations\(애플리케이션 운영\)](#)

모범 사례 1.8 - 자동 응답 및 복구 기술을 사용하여 모니터링 경고에 대응

이벤트 대응을 자동화하면 수동 프로세스에서 발생하는 오류를 줄일 수 있으며 일관된 방식으로 즉시 대응할 수 있습니다.

제안 사항 1.8.1 - 자동화 서비스를 사용하여 이벤트 응답을 자동화

모니터링 도구에서 트리거된 이벤트에 대한 수정 작업 실행을 자동화하는 방법에는 여러 가지가 있습니다. 일반적으로 모든 SAP 애플리케이션 및 데이터베이스 이벤트를 응답에서 이벤트 기반 자동화를 제공할 수 있는 단일 채널로 전달하도록 노력해야 합니다.

AWS 리소스의 상태 변경으로 인해 발생하는 이벤트 또는 SAP로부터의 사용자 지정 이벤트에 응답하려면 [EventBridge 규칙](#) 을 작성하여 이벤트 [대상](#) (예: Lambda 함수, Amazon Simple Notification Service(Amazon SNS) 주제, Amazon ECS 태스크, AWS Systems Manager Automation)에서 작업

을 호출할 수 있습니다. AWS Systems Manager Automation을 사용하여 `sapcontrol` 명령을 호출하고 SAP 시스템 태스크를 자동으로 수행할 수 있습니다.

리소스의 임계값(예: 대기 시간)을 초과하는 지표에 응답하려는 경우에는 [CloudWatch 경보](#) 를 생성하여 [Amazon EC2 작업](#) , [Auto Scaling 작업](#) 을 사용해 작업을 하나 이상 수행하거나 [Amazon SNS 주제](#) .

경보에 대한 응답으로 사용자 지정 작업을 수행해야 하는 경우에는 Amazon SNS 알림 또는 AWS Systems Manager Automation을 통해 Lambda를 호출합니다(예: `aws:runCommand` 를 사용). [AWS 블로그: AWS Systems Manager를 사용하여 분산 SAP HANA 시스템 자동 시작 또는 중지](#) 를 참조하세요.

직원들이 정보를 계속 확인할 수 있도록 Amazon SNS를 사용하여 이벤트 알림 및 에스컬레이션 메시지를 게시합니다.

AWS는 AWS 서비스 API 및 SDK를 통해 서드 파티 시스템도 지원합니다. AWS 파트너 및 서드 파티에서 제공하는 다양한 모니터링 도구를 모니터링, 알림 및 응답에 사용할 수 있습니다. 이러한 도구의 예로는 Avanza, New Relic, Splunk, Loggly, SumoLogic, Datadog가 있습니다.

조직에 적용 가능한 경우 이벤트 및 상호 작용을 서드 파티 ITIL 도구로 푸시하는 것을 고려합니다(예: [AWS를 ServiceNow로 통합](#)).

자동 절차에서 오류가 발생하는 경우를 대비해 중요 수동 절차를 사용 가능한 상태로 유지해야 합니다.

2 - SAP 변경의 결함 축소, 수정 용이화 및 워크플로 개선

귀사는 어떻게 결함을 줄이고 수정 작업을 쉽게 수행하고 프로덕션으로 이어지는 흐름을 개선하십니까? 리팩터링, 품질과 관련된 빠른 피드백 및 버그 수정이 가능하도록 프로덕션 환경으로 변경 사항을 전달하는 흐름을 개선하는 방식을 도입합니다. 이러한 방식을 도입하면 유용한 변경 사항을 프로덕션 환경으로 빠르게 전달할 수 있고, 문제 배포 가능성을 제한할 수 있으며, 배포 활동을 통해 발생하는 문제를 빠르게 파악하고 해결할 수 있습니다.

ID	우선순위	모범 사례
<input type="checkbox"/> BP 2.1	필수	버전 관리 및 구성 관리 사용
<input type="checkbox"/> BP 2.2	필수	코드 품질 개선을 위한 사례 구현
<input type="checkbox"/> BP 2.3	필수	빌드 및 배포 관리 시스템 사용
<input type="checkbox"/> BP 2.4	필수	여러 환경 사용

ID	우선순위	모범 사례
□ BP 2.5	필수	변경 사항 테스트 및 확인
□ BP 2.6	적극 권장	작게 자주 발생하고 되돌릴 수 있는 변경 사항 적용
□ BP 2.7	권장	변경 사항의 테스트, 통합 및 배포를 자동화

자세한 내용은 다음 링크 및 정보를 참조하세요.

- AWS 동영상: [운영 설계를 업무에 두세요](#)
- AWS 설명서: [AWS 개발자 도구](#)
- AWS 설명서: [AWS Launch Wizard for SAP](#)
- SAP on AWS 블로그: [DevOps for SAP – Driving Innovation and Lowering Costs\(SAP용 DevOps - 혁신을 촉진하고 비용을 절감\)](#)

모범 사례 2.1 - 버전 관리 및 구성 관리 사용

구성 관리 시스템에서는 수동 프로세스에서 발생하는 오류와 변경 사항 배포를 위한 작업량을 줄일 수 있습니다. 이렇게 하면 변경 사항을 추적하고, 새 버전을 배포하고, 기존 버전의 변경 사항을 감지하고, 장애 시 알려진 정상 상태로 롤백하는 등 이전 버전으로 되돌릴 수 있습니다. 구성 관리 시스템의 버전 제어 기능을 인프라, 데이터베이스, 애플리케이션, SAP 사용자 정의 코드 및 개발(예: ABAP, Java, UI5/JavaScript) 등 SAP 전반의 모든 절차에 통합합니다.

각 구성 유형마다 다른 버전 관리 시스템을 고려하되 지표를 중앙 릴리스 계획 도구로 통합합니다. 환경 간에 전송할 수 없는 구성 및 바이너리 버전 관리가 관리되는 방식을 고려합니다(예: SAP Kernel 버전이 전체 환경에서 일치하는지 확인할 수 있는 방법).

제안 사항 2.1.1 - SAP 개발 코드 및 버전 관리를 관리하기 위한 SAP 변경 제어 또는 기타 서드 파티 도구를 구현

SAP 애플리케이션을 지원하는 모든 개발 접근 방식 및 사용자 정의 코드(예: ABAP, Java, UI5/JavaScript 및 기타 확장 또는 스크립팅 영역)에 대한 변경 제어를 구현하도록 합니다. 모든 SAP 애플리케이션과 여러 SAP 배포 패턴에서 코드 배포를 오케스트레이션하는 방법(예: AWS 및 SAP Business Technology Platform에서 호스트되는 관련 개발을 동시에 릴리스하는 방법)을 고려합니다.

- AWS 서비스: [AWS CodeCommit](#)
- AWS 동영상: [AWS CodeCommit 소개](#)

- SAP on AWS 블로그: [SAP용 AWS DevOps 도구, 1부: Cloud Foundry](#)
- SAP on AWS 블로그: [SAP용 AWS DevOps 도구, 2부: SAP Fiori Apps](#)
- SAP 설명서: [SAP 변경 제어 관리](#)
- SAP 설명서: [SAP BTP의 모범 사례 - 수명 주기 관리](#)

제안 사항 2.1.2 - SAP 애플리케이션에 대한 구성 관리 시스템을 구현

ABAP, Java 및 기타 SAP 기술을 위한 구성 관리 도구를 구현하고 환경 간에 전송할 수 없는 구성 및 바이너리 버전 관리가 관리되는 방식을 고려합니다(예: SAP Kernel 버전이 전체 환경에서 일치하는지 확인할 수 있는 방법). SAP Solution Manager를 사용하여 SAP 애플리케이션에 대한 구성 및 버전 변경을 계획 및 구현합니다.

- SAP 설명서: [고급 변경 및 전송 시스템\(CTS+\)](#)
- SAP 설명서: [SAP Solution Manager: 환경 변경 계획](#)

제안 사항 2.1.3 - 운영 체제에 대한 구성 관리 시스템을 구현

AMI 베이킹 또는 현재 위치 구성 관리 소프트웨어(예: Ansible, Chef 또는 Puppet)를 사용하여 SAP 워크로드 운영 체제 간에 구성 관리를 조정합니다. 취약성에 대해 경고하고 운영 체제에 패치를 적용하여 강화하도록 안내하는 보안 중심 구성 관리 도구를 고려합니다.

- AWS 설명서: [AWS Systems Manager - 상태 관리자](#)
- AWS 설명서: [Amazon EC2의 구성 관리](#)
- AWS 설명서: [AWS OpsWorks란 무엇입니까?](#)
- AWS 설명서: [Amazon Inspector란 무엇입니까?](#)

제안 사항 2.1.4 - 데이터베이스에 대한 구성 관리 시스템을 구현

데이터베이스 소프트웨어 공급 업체와 협력하여 데이터베이스에 대한 구성 관리 접근 방식을 이해합니다.

- SAP 설명서: [SAP HANA 플랫폼 수명 주기 관리](#)

제안 사항 2.1.5 - 인프라에 대한 구성 관리 시스템을 구현

코드형 인프라(IaC) 접근 방식을 사용하여 SAP 워크로드를 지원하는 AWS 리소스를 프로비저닝 및 관리합니다. AWS CloudFormation 및 AWS Cloud Development Kit는 프로그래밍 방식으로 AWS 리소스

의 구성을 프로비저닝하고 관리하는 데 사용할 수 있는 도구입니다. 규칙 및 정책을 작성하여 주기적으로 인프라를 평가함으로써 규정 준수를 평가하고 문제를 해결할 수 있는 구성 감사 및 제어 도구를 고려합니다.

- AWS 설명서: [AWS Launch Wizard for SAP](#)
- AWS 설명서: [AWS Systems Manager 인벤토리](#)
- AWS 설명서: [AWS Systems Manager Change Manager](#)
- SAP on AWS 블로그: [코드형 인프라 예: Terraform 및 SAP on AWS](#)
- SAP Lens [안정성]: [모범 사례 11.3 - 서비스 가용성 복원을 위한 접근 방식 정의](#)

모범 사례 2.2 - 코드 품질 개선을 위한 사례 구현

코드 품질을 개선하고 결함을 최소화하는 사례를 구현합니다. 테스트 중심 개발, 코드 검토, 표준 도입 등을 예로 들 수 있습니다. SAP Code Inspector 도구 사용을 최소화합니다.

제안 사항 2.2.1 - 코드 품질 개선을 위한 사례를 구현

테스트 중심 개발, 페어 프로그래밍, 코드 검토, 표준 도입 등을 예로 들 수 있습니다.

제안 사항 2.2.2 - SAP 개발에 Amazon Inspector 도구를 사용하고 이 프로세스를 CI/CD 파이프라인에 통합

SAP 워크로드에서 코드 검사 및 린팅을 자동화하기 위해 다음 도구를 고려합니다.

- AWS 설명서: [Amazon CodeGuru - AWS Java 및 Python 개발용](#)
- SAP 설명서: [SAP Code Inspector - ABAP 및 SAP 관련 개발용](#)

모범 사례 2.3 - 빌드 및 배포 관리 시스템 사용

빌드 및 배포 관리 시스템을 사용합니다. ABAP 변경 및 전송 시스템(CTS), 웹 IDE 또는 SAP 도구와 같은 SAP 인증 빌드 및 배포 시스템을 사용 중인지 확인합니다. 이러한 시스템에서는 수동 프로세스에서 발생하는 오류와 변경 사항 배포를 위한 작업량을 줄일 수 있습니다.

제안 사항 2.3.1 - SAP 빌드 및 배포 시스템을 구현

ABAP 변경 및 전송 시스템(CTS), 웹 IDE, SAP BTP 지속적 전달 서비스 또는 기타 SAP 도구와 같은 SAP 인증 빌드 및 배포 시스템을 구현합니다.

- AWS 동영상: [소프트웨어 개발을 위한 지속적 통합 모범 사례](#)

- SAP on AWS 블로그: [SAP용 AWS DevOps 도구, 2부: SAP Fiori Apps](#)
- SAP 설명서: [고급 변경 및 전송 시스템\(CTS+\)](#)
- SAP 설명서: [BTP에 애플리케이션 배포](#)

모범 사례 2.4 - 다중 환경 사용

여러 SAP 환경을 사용하여 워크로드를 실험, 개발 및 테스트합니다. 프로덕션 환경에 배포하는 단계에 가까워질수록 제어 수준을 높이면 배포되었을 때 워크로드가 의도한 대로 작동할 것이라는 신뢰성을 높일 수 있습니다. 일반적으로 SAP 환경에서는 최소한 개발, 테스트 및 프로덕션을 위한 3티어 환경이 필요합니다.

제안 사항 2.4.1 - 실험에 임시 환경을 사용

기술 테스트 및 개발자 팀에 제어가 최소화된 샌드박스 또는 임시 환경을 제공하여 실험 및 위험 완화가 가능하도록 합니다.

- AWS 설명서: [AWS Launch Wizard for SAP](#)
- SAP on AWS 블로그: [코드형 인프라 예: Terraform 및 SAP on AWS](#)

제안 사항 2.4.2 - 병렬 작업이 가능하고 민첩성을 개선할 수 있는 개발 환경을 제공

병렬 작업이 가능하고 개발 및 테스트 민첩성을 제고할 수 있도록 비프로덕션 환경을 제공합니다. 개발자가 혁신을 위해 필요한 수단을 사용할 수 있도록 프로덕션 환경과 인접한 환경에서는 더욱 엄격한 제어 기능을 구현합니다. 일반적으로 SAP 환경에서는 최소한 개발, 테스트 및 프로덕션을 위한 3티어 환경이 필요합니다.

- AWS 설명서: [AWS Launch Wizard for SAP](#)

제안 사항 2.4.3 - 릴리스 품질을 개선할 수 있도록 가능한 한 프로덕션과 근사한 통합 테스트 환경을 제공

테스트 및 스테이징 환경은 릴리스 전에 아키텍처 및 코드 상호 작용 문제를 식별할 수 있도록 프로덕션 환경의 인터페이스, 보안, 복원력 및 성능 특성을 최대한 근사하게 미러링해야 합니다. 환경 비용 효율을 개선하기 위해 사용하지 않을 경우에는 클러스터의 보조 리소스를 종료하거나 이 환경의 애플리케이션 서버 성능을 수평적으로 또한 수직적으로 축소하는 것을 고려합니다.

- SAP on AWS 블로그: [AWS Systems Manager를 사용하여 분산 SAP HANA 시스템 자동 시작 또는 중지](#)

제안 사항 2.4.4 - 코드형 인프라(IaC) 및 구성 관리 시스템을 사용하여 환경을 일관되게 배포

코드형 인프라(IaC) 및 구성 관리 시스템을 사용하여 프로덕션 환경의 제어 기능과 일치하는 방식으로 구성된 환경을 배포합니다. 그러면 배포된 시스템이 정상적으로 작동합니다. 자동화 및 규정 준수에 사용할 수 있도록 태깅 및 리소스 그룹을 사용하여 환경 메타데이터에 레이블을 지정하고 향상시킵니다.

- SAP on AWS 블로그: [코드형 인프라 예: Terraform 및 SAP on AWS](#)
- SAP on AWS 블로그: [SAP on AWS 태깅 권장 사항](#)
- AWS 설명서: [AWS Launch Wizard for SAP](#)
- AWS 설명서: [AWS 리소스 그룹이란 무엇입니까?](#)

제안 사항 2.4.5 - 사용하지 않을 경우 비프로덕션 환경 끄기

사용되고 있지 않은 환경은 유휴 리소스 관련 비용이 발생하지 않도록 해제합니다. 예를 들어 개발 시스템은 야간 시간과 주말에 해제합니다.

- SAP on AWS 블로그: [AWS Systems Manager를 사용하여 분산 SAP HANA 시스템 자동 시작 또는 중지](#)

모범 사례 2.5 - 변경 사항 테스트 및 확인

개발, 테스트, 프로덕션 등의 모든 수명 주기 단계에서 변경 사항을 테스트하고 결과를 확인해야 합니다. 테스트 결과를 사용하여 새 기능을 확인하고 배포 실패의 위험과 영향을 완화합니다. 테스트 및 확인을 자동화하면 검토의 일관성을 보장하고, 수동 프로세스로 인해 발생하는 오류를 줄이고, 작업량을 줄일 수 있습니다.

제안 사항 2.5.1 - 모든 수명 주기 단계(예: 개발, 테스트, 프로덕션)에서 변경 사항을 테스트하고 결과를 확인

제안 사항 2.5.2 - 변경 사항 및 주요 프로젝트를 릴리스할 때 비교할 수 있도록 기능 테스트, 성능 및 복원력 전반에서 테스트 결과의 기준을 유지

제안 사항 2.5.3 - 각 변경 수준에 필요한 테스트 수준을 이해 예: 전체 테스트 vs 소규모 변경에 대한 타겟 회귀 테스트 프로덕션 환경으로 릴리스하는 데 필요한 테스트 정의 및 변경 사항 테스트 범위에 합의

제안 사항 2.5.4 - 가능한 경우 서드 파티 도구 및 테스트 하니스를 사용하여 테스트를 자동화 먼저 정기적인 변경 유형과 빈번한 릴리스에 중점을 둡니다.

모범 사례 2.6 - 소규모로 자주 발생하고 되돌릴 수 있는 소규모 변경 사항 적용

되돌릴 수 있는 소규모 변경 작업을 자주 수행하면 변경의 영향과 범위가 감소합니다. 많은 SAP NetWeaver 솔루션이 '패치 포워드(patch forward)' 접근 방식만 지원하지만 사용자 지정 개발에서 기능 토글을 사용하여 롤백을 허용하는 것을 고려합니다. 이렇게 하면 문제를 더 빠르고 쉽게 해결할 수 있으며 변경 사항 롤백 옵션을 사용할 수 있습니다.

제안 사항 2.6.1 - 가능한 경우 개발 및 릴리스를 자주 발생하는 소규모 변경 사항으로 분할

제안 사항 2.6.2 - 많은 SAP 솔루션이 '패치 포워드(patch forward)' 접근 방식만 지원하고 복원 가능한 전송은 허용하지 않으므로 사용자 지정 개발에서 기능 토글을 사용하여 롤백/철회가 아닌 기능 비활성화를 허용하는 것을 고려

제안 사항 2.6.3 - 되돌릴 수 없는 SAP 변경 사항의 경우 전체 시스템 스냅샷, 데이터베이스 백업 및 복구 옵션 등 추가 롤백 옵션을 고려

- AWS 설명서: [Amazon EBS 크래시 일관성 스냅샷](#)
- AWS 설명서: [AWS Backint for SAP HANA](#)

모범 사례 2.7 - 변경 사항의 테스트, 통합 및 배포 자동화

워크로드 빌드, 배포 및 테스트를 자동화합니다. 이렇게 하면 수동 프로세스에서 발생하는 오류와 변경 사항 배포를 위한 작업을 줄일 수 있습니다.

제안 사항 2.7.1 - 코드 체크 인에서 빌드, 테스트, 배포 및 확인까지의 전체 통합 및 배포 파이프라인을 완전히 자동화

제안 사항 2.7.2 - SAP Solution Manager ChaRM, Focused Build 또는 서드 파티 변경 및 릴리스 관리 도구를 구현하여 빌드에서 배포 파이프라인까지 애플리케이션 변경을 위한 전체 프로세스를 조정

- SAP 설명서: [SAP Solution Manager 변경 요청 관리](#)
- SAP 설명서: [SAP Focused Build](#)
- AWS Marketplace: [DevOps용 제품 및 도구](#)
- AWS Marketplace - [테스트용 제품 및 도구](#)
- SAP on AWS 블로그: [SAP용 AWS DevOps 도구, 1부: Cloud Foundry](#)

3 – 워크로드가 어떻게 작동할지 이해

귀사가 워크로드를 지원 및 운영할 준비가 되어 있는지 어떻게 알 수 있습니까? 회사의 [워크로드](#), 프로세스 및 절차, 인력의 운영 준비 상태를 평가하여 [워크로드](#) 와 관련된 운영 위험을 이해합니다. 일반적인 작업에 대한 런북, 문제에 대한 플레이북을 작성하고 최대한 많은 작업을 자동화하여 복원력을 개선하고 오류를 줄입니다.

ID	우선순위	모범 사례
□ BP 3.1	필수	직원의 역량 확보
□ BP 3.2	필수	클라우드 운영 모델이 운영 목표와 일치하는지 확인
□ BP 3.3	필수	설계 표준을 공유하고 신입 지원 담당 직원에게 절차를 교육
□ BP 3.4	필수	런북을 사용하여 SAP 환경 작업을 수행
□ BP 3.5	필수	플레이북을 사용하여 문제 조사
□ BP 3.6	적극 권장	자동화를 사용하여 SAP 환경 작업을 수행

자세한 내용은 다음 링크 및 정보를 참조하세요.

- AWS 백서: [AWS 클라우드 운영 모델](#)
- AWS 서비스: [AWS Config](#)
- AWS 설명서: [AWS Systems Manager 기능](#)
- SAP on AWS 블로그: [DevOps for SAP – Driving Innovation and Lowering Costs\(SAP용 DevOps - 혁신을 촉진하고 비용을 절감\)](#)

모범 사례 3.1 - 직원의 역량 확보

운영 요구 사항에 대한 실무 지원을 제공할 적절한 수의 숙련된 인력이 있고 해당 인력이 적절한 SAP, AWS 또는 서드 파티 자격증을 보유하고 있는지 검증하는 메커니즘을 확보합니다. 효과적인 지원을 유지하기 위해 필요한 경우 직원을 교육하고 직원의 역량을 조정합니다.

제안 사항 3.1.1 - SAP 운영 팀의 교육 및 자격증 요구 사항을 평가

환경 및 종속성에 따라 다양한 자격증이 적용될 수 있습니다. 팀이 기술 스택을 지원할 수 있는 자격증 요구 사항을 평가합니다.

- AWS 설명서: [AWS 교육](#)
- AWS 설명서: [AWS 자격증](#)
- 운영 체제 자격증
 - SUSE 설명서: [SUSE Enterprise Linux Certifications](#)
 - Red Hat 설명서: [Red Hat Enterprise Linux Certifications](#)
 - Microsoft 설명서: [Microsoft Windows Certifications](#)

모범 사례 3.2 - 클라우드 운영 모델이 운영 목표와 일치하는지 확인

배포 속도, 보안, 운영 및 클라우드 플랫폼 지원 책임에 대해 식별된 비즈니스 요구 사항에 부합하도록 SAP 워크로드에 적합한 클라우드 운영 모델을 식별합니다. 적합한 클라우드 운영 모델은 성공적인 클라우드 도입과 향상된 비즈니스 민첩성을 확보하는 데 중요합니다.

제안 사항 3.2.1 - 비즈니스 목표에 적합한 클라우드 운영 모델을 채택

IT 및 비즈니스 요구 사항에 따라 적합한 클라우드 운영 모델을 채택합니다. 어느 팀이 워크로드를 빌드하고 운영할지 결정합니다. SAP Basis/Technology 팀과 개발 팀 모두 DevOps 모델에서 SAP 워크로드를 빌드하고 실행하는 소유권 공유 모델로 전환하도록 계획합니다.

- AWS 지침: [AWS 클라우드에서 운영 현대화](#)
- AWS 백서: [클라우드 운영 모델 구축](#)
- AWS 동영상: [트랜스포메이션 가속화를 위한 클라우드 운영 모델](#)

모범 사례 3.3 - 설계 표준을 공유하고 신입 지원 담당 직원에게 절차를 교육

팀 간에 기존 모범 사례, 설계 표준, 점검 항목, 운영 절차 및 거버넌스 요구 사항을 공유합니다. 모든 팀이 SAP 워크로드의 구성 요소 전반에 대한 지원 절차를 인지하고 있어야 합니다.

제안 사항 3.3.1 - 팀 간에 기존 모범 사례, 설계 표준, 점검 항목, 운영 절차 및 지침과 거버넌스 요구 사항을 공유하여 개발 작업의 복잡성을 줄이고 혜택을 극대화

제안 사항 3.3.2 - 지속적인 개선 및 혁신을 지원하기 위해 설계 표준에 대한 변경 사항, 추가 및 예외를 요청할 절차가 있는지 확인

제안 사항 3.3.3 - 팀이 게시된 콘텐츠를 활용하고 재작업 및 불필요한 작업을 제한할 수 있도록 해당 콘텐츠를 지속적으로 확인

제안 사항 3.3.4 - 팀이 SAP 워크로드의 다양한 구성 요소에 대한 지원 호출을 로그하는 방법을 숙지

누가 운영 체제, 데이터베이스 및 SAP 애플리케이션에 대한 지원을 제공합니까? 예를 들어 AWS 또는 운영 체제 공급 업체 중 누가 클러스터링 또는 패치 문제에 대한 지원을 직접 제공하는지 파악합니다. EC2 포함 운영 체제 라이선스의 경우 AWS가 이 지원을 직접 제공합니다.

- AWS 설명서: [AWS Support에 사례를 로그하는 방법](#)
- AWS 설명서: [AWS Support](#)
- SAP Note: [1656250 - SAP on AWS: Support prerequisites\(1656250 - SAP on AWS: 지원 사전 조건\)](#) [SAP 포털 액세스 권한 필요]

모범 사례 3.4 - 런북을 사용하여 SAP 환경 작업 수행

런북은 특정 결과를 달성하기 위한 문서화된 절차입니다. 절차를 런북으로 문서화하면 적절하게 파악한 이벤트에 일관된 방식으로 신속하게 대응할 수 있습니다. 실행되는 일반적인 SAP 작업을 이해하고 검토 주기를 사용하여 버전이 지정된 설명서를 작성합니다.

- AWS Well-Architected Framework [운영 우수성]: [운영 준비](#)
- AWS 설명서: [AWS Incident Manager를 사용한 런북 및 자동화](#)

제안 사항 3.4.1 - SAP 보안 작업용 런북을 작성

다음과 같은 일반적인 SAP 보안 작업을 위한 런북을 작성하는 것을 고려합니다.

- 사용자 프로비저닝 및 자격 증명 관리
- Firefighter 액세스 권한
- 권한 부여 변경
- 보안 및 권한 부여 감사
- 암호화 키 교체
- TLS 인증서 관리

제안 사항 3.4.2 - SAP 크기 조정 및 성능 작업용 런북을 작성

일반적인 크기 조정 및 성능 작업을 위한 런북을 작성하는 것을 고려합니다.

- 디스크 볼륨 크기 조정
- SAP 애플리케이션 서버의 수평적 및 수직적 크기 조정
- 데이터 서버 크기 조정
- 로드 밸런싱에서 서버 추가 또는 제거

제안 사항 3.4.3 - 장애 시 SAP 작업용 런북을 작성

장애 시 작업을 위한 런북을 작성하는 것을 고려합니다.

- 시스템 재시작 및 시스템 재시작 순서
- SAP 백업 및 복원
- 클러스터 장애 조치
- 스토리지 장애
- 중요한 인터페이스 재시작 및 재생
- DNS 및 네트워크 라우팅 변경
- 랜섬웨어 복구

제안 사항 3.4.4 - SAP 유지 관리 작업용 런북을 작성

유지 관리 작업을 위한 런북을 작성하는 것을 고려합니다.

- SAP 시작 및 중지
- SAP 새로 고침/시스템 복사본
- 일별 상태 확인
- 오류 관리/ABAP 덤프
- SAP 애플리케이션, 운영 체제 및 데이터베이스에 패치 적용
- 로그 교체, 정리 및 아카이빙

SAP 환경의 데이터베이스 및 애플리케이션 로그 및 추적 파일 정리를 고려합니다. SAP Note: [2399996 - SAP HANA Cleanup 자동화](#) [SAP 포털 액세스 권한 필요]

모범 사례 3.5 - 플레이북을 사용하여 문제 조사

잘 알려지지 않은 문제에 일관되고 신속하게 대응할 수 있도록 플레이북에 조사 프로세스를 문서화합니다. 이러한 플레이북을 운영뿐만 아니라 비프로덕션 환경 및 지정된 연습 세션(예: 게임 데이)에서도 정기적으로 사용하여 검증하고 발전시킵니다.

제안 사항 3.5.1 - 사고 대응에 사용할 문제 플레이북을 작성

자주 발생하는 문제와 식별된 각 문제에 사용되는 문제 해결 단계를 이해하고 검토 주기를 사용하여 버전이 지정된 설명서를 작성합니다. 제안된 플레이북에는 다음 항목이 포함되어야 합니다.

- 성능 문제 조사
- 용량 문제 조사
- 인증 및 로그온 문제 조사
- 보안 사고 조사
- 연결 및 네트워킹 조사
- 랜섬웨어 및 바이러스 조사
- 인터페이스 오류 조사
- 배치 작업 오류 조사
- 배포 또는 전송 오류 조사

플레이북에 관련된 지원 기능 및 팀과의 통합 및 의사 소통 단계가 포함되어 있는지 확인합니다. 일반적인 의사 소통 단계에는 크리티컬 인시던트 데스크, 보안 사고 대응 팀 및/또는 변경 관리 팀에 대한 알림 및 진행 상황 업데이트가 포함됩니다.

제안 사항 3.5.2 - 정기적으로 SAP 게임 데이를 실시하여 운영 절차를 테스트하고 플레이북을 검증

운영 팀에서 정기적으로 SAP 게임 데이를 실행하는 것을 고려합니다. 게임 데이에서는 장애나 이벤트를 시뮬레이션하여 시스템, 프로세스 및 팀 대응을 테스트합니다. 게임 데이의 목적은 이례적인 이벤트 발생 시 팀이 수행해야 할 작업을 실제로 수행해보는 것입니다. 팀이 대응 방법을 체득할 수 있도록 게임 데이를 정기적으로 진행해야 합니다. 게임 데이에서는 운영, 보안, 안정성, 성능 및 비용 영역을 확인해야 합니다. 전용 실험 환경을 사용하여 실제 시나리오를 시뮬레이션하여 운영 절차 및 복구 프로세스를 검증하고 연습합니다.

모범 사례 3.6 - 자동화를 사용하여 SAP 환경 작업 수행

SAP 환경 구축 및 환경 운영에 대한 자동화 파이프라인을 빌드합니다. 코드형 인프라 기술(예: CloudFormation, Launch Wizard for SAP)을 사용한 자동화를 통해 반복 가능하고 민첩한 환경 생성 또

는 확장이 가능합니다. 자동화된 파이프라인 및 환경 운영은 수동 프로세스에서 발생하는 오류와 변경 사항 배포를 위한 작업을 줄이며 비즈니스 요구에 대응하는 속도를 향상합니다.

자동화된 방식으로 일반적인 환경 작업(예: 시스템 복사, SAP 시작, SAP 중지, SAP 크기 조정)을 수행할 수 있는 자동화된 SAP 환경 작업 파이프라인을 만듭니다. 시간 기반 시스템 종료 또는 사용자 로드 에 따른 자동 크기 조정과 같은 운영 이벤트에 응답하여 이러한 파이프라인을 호출합니다.

제안 사항 3.6.1- 코드형 인프라 기술을 구현하여 SAP 환경에 대한 반복 가능한 코드 기반 빌드 파이프라인을 구축

AWS CloudFormation, AWS Cloud Development Kit 또는 AWS Launch Wizard for SAP 같은 도구를 사용하여 반복 가능하고 제어되며 신속한 환경 배포를 생성합니다.

- SAP on AWS 블로그: [코드형 인프라 예: Terraform 및 SAP on AWS](#)
- AWS 설명서: [AWS Launch Wizard for SAP](#)

제안 사항 3.6.2 - 자동화를 사용하여 일반적인 SAP 환경 작업 구현

오케스트레이션 및 코드형 인프라(IaC) 도구의 조합을 사용하여 자동화된 방식으로 일반적인 SAP 환경 작업을 수행합니다. 배포 파이프라인에서 일반적인 SAP 환경 작업을 수행하기 위해 AWS CloudFormation, AWS Systems Manager – Run Automations, SAP Landscape Management(LaMa), AWS Lambda 같은 도구를 오케스트레이션할 수 있습니다.

도구 간의 복잡한 또는 심층적인 통합이 필요한 경우 서드 파티 자동화 도구를 고려합니다(예: Terraform, Ansible, Chef).

자동 복구 및 자체 유지 환경이 가능하도록 SAP 워크로드 이벤트에 대한 응답으로 자동화된 작업을 사용하는 것을 고려합니다.

- SAP Note: [2574820 - Amazon Web Services\(AWS\)용 SAP Landscape Management Cloud Manager](#) [SAP 포털 액세스 권한 필요]
- AWS 설명서: [AWS Launch Wizard for SAP](#)
- AWS 설명서: [AWS Systems Manager Automation](#)
- AWS Marketplace: [DevOps용 제품 및 도구](#)

4 – 정기적으로 SAP 워크로드 검증 및 개선

SAP 워크로드가 계속 효율적으로 작동하는지 확인하려면 어떻게 해야 합니까? 정기적으로 SAP 워크로드를 개선하고 AWS의 신규 서비스 릴리스를 활용하는 것을 목표로 합니다. SAP 워크로드를 유지

관리하는 데 시간과 리소스를 투자합니다. SAP 워크로드의 효율을 향상하기 위해 점진적 개선을 지속하는 것을 목표로 합니다. 성능, 복원력 또는 비용 효율성을 개선하는 수정 조치를 통해 패치를 적용하고, 소규모 변경을 수행하고, 이전 설계 결정을 재평가하도록 계획합니다.

ID	우선순위	모범 사례
□ BP 4.1	필수	SAP 워크로드의 수명 주기 이벤트를 이해 및 계획
□ BP 4.2	필수	소프트웨어를 최신 상태로 유지하기 위해 정기적으로 패치 관리를 수행
□ BP 4.3	적극 권장	정기적으로 비즈니스 연속성 계획 및 장애 복구를 테스트
□ BP 4.4	적극 권장	주기적 워크로드 검토를 수행하여 복원력, 성능, 민첩성 및 비용을 최적화

모범 사례 4.1 - SAP 워크로드의 수명 주기 이벤트 이해 및 계획

SAP 워크로드는 새로운 소프트웨어 및 취약성 패치, 운영 체제 및 데이터베이스 커널, 지원 에스컬레이션을 제공하기 위해 SAP에 크게 의존합니다. SAP는 정기적으로 SAP 소프트웨어 릴리스에 대한 정보(릴리스 유형, 유지 관리 기간, 예정된 가용성 및 업그레이드 경로)를 [Product Availability Matrix\(PAM\)](#) 및 SAP Note에 게시합니다. 각 SAP 애플리케이션에 고유한 세부 정보를 얻고 이를 로컬에서 추적하여 SAP 소프트웨어가 최신 상태인지, 지원 대상인지, 유지 관리 관점에서 언제 수명이 종료되는지 파악해야 합니다.

PAM은 지원되는 데이터베이스 플랫폼 및 운영 체제 등 플랫폼 가용성 및 호환성에 대한 정보도 제공합니다. 이는 SAP 워크로드의 이러한 기본 구성 요소에 패치 및 업그레이드를 적용하는 데 도움이 됩니다. 또한 운영 체제 공급 업체에는 자체 패치 및 지원 수명 주기가 있으므로 업그레이드와 같은 SAP 유지 관리 및 수명 주기 이벤트를 계획할 때 이를 고려해야 합니다.

제안 사항 4.1.1 - 주요 지원 및 수명 주기 날짜를 고려하여 SAP 애플리케이션의 운영 로드맵을 작성

모든 SAP 소프트웨어 애플리케이션, 커널 버전, 운영 체제 및 데이터베이스 버전을 중앙 레지스터에 나열하고 지원되는 버전 및 유지 관리 기간에 대한 PAM 정보와 통합합니다. 이 목록을 통합 보기로 사용하여 SAP를 최신 상태 및 지원 대상으로 유지하는 데 필요한 모든 구성 요소의 패치, 업그레이드 및 플랫폼 변경을 계획합니다.

- SAP 설명서: [SAP 릴리스 및 유지 관리 전략: Product Availability Matrix](#) [SAP 포털 액세스 권한 필요]

제안 사항 4.1.2 - 자격 증명, 인증서 및 라이선스 만료 캘린더를 유지

앞서 언급한 주요 SAP 수명 주기 이벤트 및 패치와 함께 사소한 시스템 이벤트를 계획하기 위한 운영 캘린더를 유지하도록 합니다. 이러한 유지 관리 이벤트의 예로는 시스템 자격 증명 만료, 인증서 만료(예: 시스템 간 STRUST 통합), 필요한 라이선스 갱신 작업 또는 업데이트(예: 마이그레이션, 개발 또는 POC를 위한 임시 SAP 또는 데이터베이스 라이선스)가 있습니다.

- AWS 설명서: [AWS Certificate Manager](#)

제안 사항 4.1.3 - SAP 소프트웨어 수명 종료가 도래하기 전에 업그레이드 또는 대안을 계획

주요 SAP 수명 주기 이벤트 및 운영 유지(패치, 소프트웨어 업그레이드, 마이그레이션 및 리플랫폼(필요한 경우))를 시각화하는 SAP 환경 로드맵을 작성합니다. 이 수명 주기 캘린더를 비즈니스 및 기술 이해 관계자에게 전달합니다. 이러한 SAP 수명 주기 작업/프로젝트에 자금을 조달하기 위한 투자를 계획합니다. 유지 관리 기간이 발생할 수 있고 가동 중지 또는 재시작이 필요한 경우 비즈니스 이해 관계자와 함께 미리 계획합니다.

- SAP 설명서: [SAP Roadmap Explorer](#)

제안 사항 4.1.4 - 최신 정보 및 지원 조언을 위해 주요 SAP Note를 구독

지원 가능성 변경 사항 또는 업데이트에 대한 알림을 받고 조언을 얻기 위해 SAP 워크로드에 대한 주요 SAP Note 및 기술 자료 문서(KBA)를 구독합니다. '즐거찾기' SAP Note 기능을 사용하여 SAP 워크로드에 대해 자주 액세스하고 중요한 노트의 목록을 유지하면 손쉽게 액세스하고 비교할 수 있습니다.

- [SAP Support Portal - Favorite SAP Notes](#) [SAP 포털 액세스 권한 필요]

모범 사례 4.2 - 소프트웨어를 최신 상태로 유지하기 위해 정기적으로 패치 관리 수행

정기적으로 패치 관리를 수행하여 기능을 확인하고, 문제를 해결하고, 거버넌스 규정 준수 상태를 유지합니다. 운영 체제, 데이터베이스 및 SAP 애플리케이션 계층의 패치를 고려합니다. 패치 프로세스가 기존 서버에 패치를 적용하는 것인지, 새 서버를 프로비저닝하고 여기에 패치를 적용하는 것인지 파악합니다. 패치 관리를 자동화하여 수동 프로세스에서 발생하는 오류와 패치 관련 작업을 줄이고 주요 SAP, 데이터베이스 및 커널 패치 적용에 필요한 애플리케이션 가동 중지 시간을 단축합니다

제안 사항 4.2.1 - SAP 패치 관리 절차를 구현하여 정기적으로 SAP Security Note 및 새로 릴리스된 패치를 검토

운영 체제, 데이터베이스 및 SAP 애플리케이션 계층의 패치를 고려합니다.

AWS 설명서: [AWS 보안 공지](#)

SAP 설명서: [SAP EarlyWatch Alert](#)

SAP 설명서: [SAP Security News](#)

운영 체제	Guidance
SUSE Linux Enterprise Server	SUSE Update Advisories
Red Hat Enterprise Linux	Red Hat Security Advisories
Microsoft Windows	Microsoft Security Alerts
Oracle Enterprise Linux	Oracle Security Alerts

이 항목에 대한 추가 설명은 [보안]: [모범 사례 6.2 - 운영 체제 빌드 및 보호](#) 를 참조하세요.

제안 사항 4.2.2 - SAP 환경 전반에서 패치를 일치 및 자동화할 수 있도록 AWS Systems Manager 및 AWS OpsWorks와 같은 자동화된 도구를 고려

- AWS 설명서: [AWS Systems Manager 패치 관리자](#)
- AWS 설명서: [AWS OpsWorks](#)
- AWS 설명서: [AWS OpsWorks란 무엇입니까?](#)
- SAP Lens [보안]: [모범 사례 6.2 - 운영 체제 빌드 및 보호](#).

모범 사례 4.3 - 정기적으로 비즈니스 연속성 계획 및 장애 복구 테스트

SAP 시스템은 일반적으로 주요 고객 대면 트랜잭션에 사용되는 비즈니스 중요 시스템입니다. 장애 또는 재해 상황에서 IT 운영을 신속하게 재개하고 데이터 손실을 최소화하는 것은 운영 우수성을 유지하는 데 매우 중요합니다. 비즈니스 연속성 계획(BCP) 및 장애 복구 절차는 장애 발생 시 운영 팀 및 시스템이 무엇을 언제 해야 하는지 숙지하고 워크로드 서비스를 즉각적으로 재개할 수 있도록 하는 데 필요합니다.

시스템 및 지원 팀이 발전함에 따라 정기적으로 BCP 절차 및 장애 복구 계획을 테스트, 개선 및 구체화하는 것이 서비스를 성공적으로 재개하는 데 중요합니다. 실제 위기 상황이 아닐 때 BCP 및 복구 계획을 테스트하면 실제 시스템 장애 또는 재해가 발생할 경우 서비스를 성공적으로 재개할 수 있는 능력을 확신할 수 있고 복구 시간 목표(RTO) 및 복구 시점 목표(RPO)를 달성할 수 있습니다.

제안 사항 4.3.1 - BCP 및 장애 복구 테스트 캘린더를 작성

SAP 워크로드에 대한 정기(최소 1년) BCP 및 장애 복구 테스트를 예약하는 캘린더를 만듭니다. 절차를 숙지하고 일치된 예상을 할 수 있도록 기술 운영 팀, 지원 담당자 및 비즈니스 이해 관계자를 이 테스트에 참여시킵니다. 가능한 한 실제 상황에서 시스템을 테스트하는 것을 목표로 합니다.

다음 시나리오를 테스트하고 각 시나리오에 대한 복구 지표를 검증하는 것을 고려합니다.

- SAP 애플리케이션 서비스 장애
 - (예: SAP 애플리케이션 서비스가 구성 변경으로 인해 시작되지 않음)
- 단일 인스턴스 호스트 장애
 - (예: SAP 애플리케이션 서버 EC2 인스턴스에 연결할 수 없음)
- 단일 스토리지 볼륨 장애
 - (예: 단일 EBS 볼륨에 연결할 수 없음)
- 네트워크 장애 및 이중화 연결로 전환
 - (예: 온프레미스 Direct Connect 연결이 끊어짐)
- 클러스터링된 기본 구성 요소와 보조 구성 요소 간에 자동 장애 조치
 - (예: SUSE HAE 클러스터가 강제로 프라이머리 HANA 데이터베이스를 대체 가용 영역의 세컨더리 데이터베이스로 이동)
- 기본 구성 요소와 보조 구성 요소 간의 수동 장애 조치
 - (예: 수동으로 Oracle DataGuard를 대체 가용 영역의 세컨더리 데이터베이스로 전환)
- 여러 이중화 구성 요소 간의 로드 밸런싱
 - (예: 가용 영역 간 고가용성 페어의 기본 웹 디스패처에서 장애가 발생)
- 대체 AWS 리전에서 SAP 애플리케이션 복구(필요한 경우)
- 랜섬웨어 발생 시 백업에서 복구
 - (예: Amazon S3 WORM 백업에서 전체 SAP ERP 시스템을 복구)

제안 사항 4.3.2 - 워크로드 변경의 일부로 정기적으로 BCP 및 장애 복구 절차를 검토 및 업데이트

시간이 흐르면서 워크로드가 발전하고 변경되는 과정에서 BCP 및 복구 절차를 고려해야 합니다. 코드 또는 인프라 변경이 RTO 또는 RPO에 영향을 줄 수 있는 경우 설명서 및 구성을 업데이트하고 릴리스 프로세스 또는 정기 테스트 일정의 일부로 새 BCP 및 복구 절차를 테스트해야 합니다.

- AWS 설명서: [비즈니스 연속성 계획\(BCP\) 정의](#)
- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#)
- SAP Lens [안정성]: [모범 사례 11.4 - 주기적으로 복원력 테스트 수행](#)

모범 사례 4.4 - 주기적 워크로드 검토를 수행하여 복원력, 성능, 민첩성 및 비용 최적화

SAP on AWS를 실행할 때 점진적 개선을 지속하기 위한 시간 및 리소스를 계획하고 투입하여 워크로드의 효과 및 효율을 향상합니다. AWS는 SAP 워크로드를 최적화하는 데 활용할 수 있는 새로운 서비스, 접근 방식, 향상된 SLA 및 가격 인하를 정기적으로 출시합니다. 신규 서비스 릴리스가 SAP 워크로드에 적용 가능한지 파악 및 검증하고, 적절한 경우 프로덕션 환경에서 구현하여 워크로드를 향상합니다.

제안 사항 4.4.1 - SAP 워크로드에 대한 정기 검토를 계획

AWS 팀, AWS 파트너 또는 내부 전문가와 공동으로 Well-Architected Framework SAP Lens(이 문서)를 사용하여 주기적으로 SAP 워크로드를 검토합니다. 적어도 매년 한 번 워크로드를 검토하도록 계획합니다. 개선 작업 및 문제 해결을 식별 및 검증하고, 이에 대한 우선 순위를 지정하고, 이를 백로그에 통합합니다.

제안 사항 4.4.2 - Amazon EC2 인스턴스 크기 조정 및 성능을 검토

과거 CloudWatch 지표를 확인하여 SAP 워크로드의 CPU 및 메모리 사용률을 검토합니다. 각 SAP 구성 요소에서 CPU 또는 메모리 사용률이 낮은지 검토하고 워크로드 요구 사항에 더 잘 부합하도록 EC2 인스턴스의 크기를 조정할 것을 고려합니다. 성능 적합성 및 비용 최적화를 위해 새로 출시되고 SAP 인증을 받은 EC2 인스턴스 유형을 고려합니다. 운영 백로그에서 새로운 개선 사항을 활용하도록 계획합니다.

SAP 워크로드의 Amazon EC2 사용률에 대한 자세한 내용은 [비용 최적화](#) 를 참조하세요.

- AWS 설명서: [SAP용 Amazon EC2 인스턴스 유형](#)

제안 사항 4.4.3 - Amazon EBS 크기 조정 및 성능을 검토

CloudWatch 기록 지표에서 볼륨 소비, 처리량 및 IOPS 사용량을 확인하여 SAP 워크로드 전체의 스토리지 사용량을 검토합니다. 각 SAP 구성 요소에서 스토리지 크기가 과도하거나 처리량/IOPS 사용률이 낮은지 검토하고 워크로드 요구 사항에 더 잘 부합하도록 Amazon EBS 스토리지 크기 및 유형을 적절히 선택할 것을 고려합니다. 성능 적합성 및 비용 최적화를 위해 새로 출시되고 SAP 인증을 받은 Amazon EBS 유형을 고려합니다. 운영 백로그에서 새로운 개선 사항을 활용하도록 계획합니다.

- AWS 설명서: [올바른 크기 조정](#)
- SAP Lens [비용 최적화]: [모범 사례 18.4 - 필요한 특성을 기반으로 스토리지 옵션의 비용 영향 평가](#).

제안 사항 4.4.4 - SAP 워크로드 운영의 민첩성 또는 효율성을 개선하는 새로운 서비스를 검토

SAP 워크로드의 운영을 개선할 수 있는 새로운 지원 서비스 릴리스를 검토합니다. AWS Support 계약의 일부로 테크니컬 어카운 관리자(TAM)가 있는 경우 신규 서비스 브리핑 및 최적화 논의에서 도움을 받을 수 있습니다.

공유 파일 스토리지, 인터페이스 서비스(예: AWS Transfer, API Gateway), 보안 서비스(예: Amazon GuardDuty, AWS Firewall), 백업 도구(예: AWS Backint) 및 자동화 도구(예: Launch Wizard for SAP) 같은 새로운 릴리스를 고려합니다.

운영 백로그에서 새로운 개선 사항을 활용하도록 계획합니다.

- AWS 설명서: [“새로운 소식” 피드](#)
- AWS 설명서: [Support의 사전 예방적 서비스](#)

제안 사항 4.4.5 - SAP on AWS 블로그 및 발표를 모니터링

새로 출시된 서비스 발표, 혁신 접근 방식 및 가격 인하에 대한 최신 정보를 받을 수 있도록 SAP on AWS 블로그 피드 및 AWS ‘새로운 소식’ 피드를 구독하는 것을 고려합니다.

- [SAP on AWS 블로그 피드](#)

제안 사항 4.4.6 - 신규 및 개선된 AWS 서비스를 활용할 수 있도록 주기적 개선 작업을 계획

운영 예산이 새로운 AWS 서비스의 구현 및 테스트와 주기적인 워크로드 개선을 위해 계획된 지원 팀 활동을 지원할 수 있도록 해야 합니다.

보안

보안 원칙에는 클라우드 기술을 활용하여 보안을 강화하고 데이터, 시스템 및 자산을 보호하는 능력이 포함됩니다. 이 렌즈에서는 SAP에 대한 몇 가지 핵심 원칙과 리소스를 집중적으로 설명합니다. 이러한 사례의 대부분은 SAP에만 해당하는 것이 아니므로 기업의 핵심 원칙을 고려하고 전체 환경에서 제어를 설정하는 데 초점을 맞추는 것이 좋습니다. 유효 [보안 원칙](#)에는 보다 광범위한 설계 원칙 및 권장 사항이 포함되어 있습니다. 다음 SAP 지침과 함께 읽을 것을 적극 권장합니다.

배포 전략(AWS 기반, 온프레미스 또는 하이브리드)에 관계없이 SAP Security Notes and News(SAP Security Note 및 뉴스)에서 권장하는 지침을 따르고 SAP 워크로드와 관련된 최신 보안 권장 사항을 따라야 합니다.

5 - 보안 표준 및 SAP 워크로드에 해당 표준이 적용되는 방식 이해

어떻게 SAP 워크로드의 중요성에 부합하도록 보안 표준 및 제어를 정의합니까? 표준은 제품, 조직, 산업 또는 관할 지역에 대한 모범 사례에 따라 시스템을 보호하는 데 필요한 정책 및 절차를 정의하는 게시된 문서로, SAP 워크로드를 평가할 수 있는 프레임워크를 제공합니다. 일부 표준은 규제 요구 사항을 준수하기 위한 필수 사항이며 다른 표준은 선택 사항이지만 역할 및 책임을 설정하는 데 도움이 됩니다.

ID	우선순위	모범 사례
□ BP 5.1	필수	보안 역할 및 책임 정의
□ BP 5.2	적극 권장	SAP 워크로드 내에서 데이터 분류
□ BP 5.3	적극 권장	애플리케이션 및 데이터 분류에 따라 필요한 보안 제어 결정
□ BP 5.4	적극 권장	보안 제어 구현을 위한 전략 수립

모범 사례 5.1 - 보안 역할 및 책임 정의

SAP 워크로드를 보호하기 위한 요구 사항을 정의하여 해결해야 하는 위험을 식별하고 보안 관련 역할 및 책임이 적절하게 할당되도록 할 수 있습니다. 제안 사항에서는 보안 전략을 수립하기 위한 기준을 설정할 수 있도록 AWS, SAP 및 기타 서비스 공급 업체에 대한 표준을 논의합니다.

제안 사항 5.1.1 - AWS 공동 책임 모델을 숙지

AWS는 클라우드 자체의 보안을 책임지고, 고객은 클라우드 내부의 보안을 책임집니다. 다음 리소스를 인지하고 이해해야 합니다.

- AWS 설명서: [AWS 공동 책임 모델](#)
- AWS 설명서: [손상 및 침해에 대한 AWS 대응](#)
- AWS 설명서: [AWS 사용 제한 정책](#)

AWS 공동 책임 모델의 맥락에서 고객과 파트너 간의 책임 분담을 이해합니다.

제안 사항 5.1.2 - 규정 준수 인증서, 보고서 및 증명을 포함하여 SAP 및 AWS 전반의 보안 기초를 이해

SAP 및 AWS가 지원하는 보안 표준 및 규정 준수 인증을 이해합니다. 소속 산업 및 국가와 관련된 표준을 확인합니다(예: PCI-DSS, GDPR, HIPAA). 이러한 제어를 통해 자체 규정 준수 및 인증 프로그램을 강화하고 보안 표준을 충족하는 데 필요한 작업을 줄일 수 있습니다.

자세한 내용은 SAP 및 AWS 설명서를 참조하세요.

- AWS 설명서: [AWS 규정 준수](#)
- AWS 설명서: [AWS 규정 준수 센터](#)
- AWS 설명서: [규정 준수 프로그램](#)
- AWS 설명서: [규정 준수 서비스 범위](#)
- SAP 설명서: [Trust Center](#)

제안 사항 5.1.3 - SAP 워크로드를 지원하는 서비스 공급 업체의 보안 기초를 평가

서드 파티 조직에 의존하여 SAP 워크로드의 전부 또는 일부를 관리하는 경우 서드 파티가 필요한 보안 제어를 충족할 수 있는 능력을 평가합니다. 여기에는 기업에 부과된 법률 및 규정 요구 사항이 포함됩니다.

모범 사례 5.2 - SAP 워크로드 내에서 데이터 분류

데이터 민감도는 위험을 완화하는 데 필요한 제어에 영향을 줄 수 있습니다. 업계 또는 조직 내의 표준 프레임워크를 참조하고 채택하여 SAP 워크로드 및 그 안에 포함된 데이터를 분류하는 것이 좋습니다.

제안 사항 5.2.1 - 데이터 분류 및 처리 요구 사항을 결정

이미 조직에 마련된 데이터 분류 프레임워크가 있는지 파악합니다. 이러한 프레임워크는 기밀성, 무결성 및 가용성을 보호해야 하는 데이터와 같이 정보의 민감도에 따라 데이터를 분류하는 데 도움이 될

수 있습니다. 산업, 비즈니스 또는 IT 요구 사항에 따라 사용자 정의할 수 있는 [미국 정보 분류 체계](#) 같은 표준 분류 모델이 있습니다.

분류에 적합한 지침에 따라 데이터를 처리하는 방법을 이해합니다. 여기에는 표준 또는 규제 요구 사항(예: PCI-DSS 또는 GDPR)과 관련된 특정보안 제어 및 일반적인 개인 정보 보호 고려 사항(예: 개인 식별 정보(PII) 처리)이 포함됩니다. 다음 문서는 추가 정보를 제공합니다.

- AWS 설명서: [데이터 분류: 안전한 클라우드 도입 백서](#)
- AWS 설명서: [일반 데이터 보호 규정\(GDPR\) 센터](#)
- [정보 시스템 및 조직에 대한 NIST 보안 및 개인 정보 보호 통제](#)
- [ISO 27001 – 부록 A.8: 자산 관리](#)
- Well-Architected Framework [보안]: [데이터 보호](#)

제안 사항 5.2.2 - 특정 처리 규칙이 적용되는 SAP 데이터 유형을 식별

SAP 시스템이 지원하는 비즈니스 프로세스에 따라 데이터 처리 및 저장에 대한 요구 사항이 있을 수 있습니다. 지역 및 산업별 지침을 숙지합니다. SAP 예에는 다음이 포함될 수 있습니다.

- 저장된 카드 소지자 데이터를 보호하고 PCI 규정 준수를 보장하기 위해 디지털 결제 추가 기능이 필요한지 여부를 평가합니다.
- HR 데이터의 데이터 상주 요구 사항을 평가합니다. 예를 들어 일부 국가 및 관할 지역은 데이터를 특정 지리적 위치에 저장하도록 요구할 수 있습니다.
- 민감한 데이터를 난독 처리하되 데이터 무결성을 유지하기 위해 비프로덕션 시스템에서 어떤 데이터를 스�크램블링해야 하는지 고려합니다.

제안 사항 5.2.3 - 정의된 프레임워크에 따라 모든 워크로드를 분류

SAP 시스템을 해당 비즈니스 용도 및 중요한 데이터 유형의 존재에 따라 분류합니다. SAP ERP와 같은 트랜잭션 시스템은 SAP BW와 같은 분석 시스템 또는 Solution Manager와 같은 관리 시스템보다 민감한 데이터를 포함할 가능성이 높지만 기능 및 보안 전문가가 이를 확인해야 합니다.

또한 비프로덕션 워크로드에도 동일한 제어가 적용되는지 평가합니다. 예를 들어 비프로덕션 워크로드가 프로덕션 데이터를 포함하는 경우 동일한 보안 제어를 준수해야 합니까?

모범 사례 5.3 – SAP 워크로드에 대한 특정 보안 제어가 필요한지 평가

데이터 분류를 기반으로 이전 모범 사례에서 설정한 표준 및 요구 사항을 충족하는 데 도움이 될 수 있는 제어를 평가합니다. 여기에는 위치, AWS 계정 전략, 비프로덕션 SAP 워크로드에 대한 스크램블링 요구 사항이 포함됩니다.

제안 사항 5.3.1 - 지리적 위치 요구 사항 평가

SAP 워크로드는 하나 이상의 AWS 리전 및 가용 영역(AZ)에 배포될 수 있습니다. 각 AWS 리전은 지리적 영역 내에서 물리적으로 분리된 여러 개의 격리된 AZ로 구성됩니다. 리전에서 대기 시간 및 복원력을 평가하는 것 외에 보안 및 규정 준수 요구 사항을 충족할 수 있는지 고려해야 합니다. 특정 운영 관할 지역이 적용되는 격리된 리전의 예는 다음과 같습니다.

- AWS GovCloud(미국) - 민감한 데이터, 규제 대상 워크로드를 호스트하고 가장 엄격한 미국 정부 보안 및 규정 준수 요구 사항을 해결하도록 설계되었습니다.
- 중국 내 Amazon Web Services - AWS는 중국의 법률 및 규제 요구 사항을 충족할 수 있도록 현지 파트너와 협력했습니다.

일부 산업 및 국가에는 IT 시스템에서 처리 및 저장되는 모든 고객 콘텐츠가 특정 국가의 국경 내에 유지되어야 한다는 데이터 상주 요구 사항이 있습니다.

- AWS 설명서: [AWS에서 데이터 상주 해결](#)

위치를 결정하기 전에 해당 AWS 리전에서 서비스 가용성을 검토하여 필요한 서비스를 사용할 수 있는지 확인하세요.

- AWS 설명서: [리전별 제품 서비스](#)

제안 사항 5.3.2 - SAP 워크로드에 필요한 AWS 계정 전략을 결정

AWS에서 SAP 워크로드를 실행할 때 중요한 고려 사항 하나는 조직의 보안 제어를 충족하기 위해 채택하는 AWS 계정 전략입니다. SAP 워크로드를 비 SAP 워크로드와 분리하고 프로덕션을 비프로덕션과 별도의 계정에 유지하는 것을 고려해야 합니다.

AWS Organizations 및 AWS Control Tower 사용을 포함하여 조직의 기존 AWS 계정 관리 전략을 이해합니다. 보안 및 로그 기능을 별도의 계정으로 격리하는 것을 고려합니다. 자세한 내용은 다음을 참조하세요.

- Well-Architected Framework [보안]: [AWS 계정 관리 및 분리](#)

- AWS 설명서: [모범 사례 AWS 환경 구축](#)
- AWS 설명서: [여러 계정을 사용하여 AWS 환경 구성](#)

계정 전략은 AWS 내의 네트워크 구성에도 영향을 줍니다. SAP 워크로드에 적절한 AWS 계정 전략을 결정하는 과정에서 다음을 고려해야 합니다.

- 교차 계정 액세스 요구 사항(예: 비프로덕션 시스템과 프로덕션 시스템 간의 통신을 허용하도록 [VPC 피어링](#) 또는 [Transit Gateway](#) 를 설정할 필요성). 환경에서 SAP Transports의 이동을 예로 들 수 있습니다.
- SAP 워크로드와 다른 AWS 계정에 배포된 공유 서비스(예: 디렉터리 관리 리소스) 및 네트워크 관리 구성 요소에 대한 종속성

제안 사항 5.3.3 - 데이터 스크램블링에 대한 제어를 검토(해당하는 경우)

많은 SAP 고객은 회귀 및 성능 테스트를 포함하여 테스트 목적으로 프로덕션 데이터의 복사본을 사용합니다. 프로덕션 데이터의 복사본을 생성하는 경우 프로덕션 데이터가 의도하지 않은 액세스 및 수정으로부터 보호되도록 어떤 제어를 추가해야 하는지 결정합니다.

다음 옵션을 고려하세요.

- SAP 또는 서드 파티 공급 업체가 제공하는 기존 데이터 스크램블링 메커니즘
- 프로덕션 데이터를 복사하는 동안 액세스를 제한하기 위해 추가 계정 또는 네트워크 제어를 사용
- 프로덕션과 동일한 제어가 적용되는 비프로덕션 계정을 사용

모범 사례 5.4 - 보안 제어 구현을 위한 전략 수립

데이터 분류를 기반으로 비즈니스 요구 사항을 평가한 후에는 더 광범위한 조직의 보안 제어와 사용 가능한 애플리케이션 지침 및 공개 표준을 균형 있게 고려한 전략을 수립합니다. 구현 노력을 고려하고 위험을 확인합니다.

제안 사항 5.4.1 - 위험을 평가하기 위한 매트릭스 식별

특정 산업 및 지리적 위치에 대해 다양한 위험 관리 프레임워크를 사용할 수 있습니다. 조직에서 채택한 위험 프레임워크 및 해당 프레임워크가 SAP 워크로드와 관련된 위험 관리에 적용되는 방식을 이해합니다.

- AWS 설명서: [위험 매트릭스 예](#)

- AWS 설명서: [클라우드에 대한 거버넌스, 위험 및 규정 준수 프로그램 크기 조정](#)
- [NIST 위험 관리 프레임워크](#)

제안 사항 5.4.2 - 조직에 부과된 보안 및 규정 준수 요구 사항을 평가

클라우드 혁신 센터, 법무 팀, 규정 준수 팀 및 관리형 서비스 공급 업체에 문의하여 해당 보안 기준과 제어가 시행되는 방식을 이해합니다. 이러한 모든 제어가 SAP 워크로드에 용이하게 적용될 수 있는지 평가하고 예외가 필요할 수 있는 영역(예: AWS 서비스 허용 및 거부 목록, 인바운드 및 아웃바운드 트래픽 흐름, 액세스 제한)을 식별합니다.

제안 사항 5.4.3 - 예외에 대한 프로세스를 식별 및 합의

일부 상황에서는 SAP에 대한 소프트웨어, 비즈니스 또는 지원 요구 사항에 따라 표준 보안 패턴에서 벗어나야 할 수 있습니다. 변경 자문 위원회 또는 보안 설계 기관과 예외를 합의 및 문서화하는 프로세스를 식별하고 정기적으로 프로세스를 재평가합니다.

AWS 설명서: [클라우드에서 변경 관리](#)

6 – 인프라 및 소프트웨어 제어를 사용하여 보안 구성 오류 감소

SAP 애플리케이션과 기본 데이터베이스, 운영 체제, 스토리지 및 네트워크를 어떻게 보호합니까? SAP 소프트웨어 솔루션과 관련 기본 구성(예: 운영 체제 및 데이터베이스 패치, 파라미터, 클라우드 서비스, 인프라)을 강화하는 것이 좋습니다. 강화는 조직이 결정한 적절한 수준에서 프로덕션 및 비프로덕션을 모두 포함한 모든 SAP 환경의 안전을 보장하는 데 도움이 됩니다.

SAP 환경의 보안 관련 작업에 대한 지침은 [AWS 공동 책임 모델](#) 을 참조합니다. 예를 들어, EC2 인스턴스에 대한 펌웨어 업데이트는 AWS의 책임인 ‘클라우드 자체의 보안’ 작업이지만, 동일한 EC2 인스턴스에 대한 운영 체제 및 애플리케이션 관리는 고객의 책임인 ‘클라우드 내부의 보안’ 작업입니다.

ID	우선순위	모범 사례
<input type="checkbox"/> BP 6.1	필수	SAP 네트워크 설계에 보안 및 감사를 기본적으로 포함
<input type="checkbox"/> BP 6.2	필수	운영 체제 빌드 및 보호
<input type="checkbox"/> BP 6.3	필수	데이터베이스 및 애플리케이션 보호
<input type="checkbox"/> BP 6.4	필수	해당되는 모든 소프트웨어에 업그레이드 및 패치를 적용하기 위한 계획 수립

자세한 내용은 다음 정보를 참조하세요.

- AWS 설명서: [AWS 보안 백서](#)
- SAP Note: [2191528 - 보안 취약성을 보여주는 서드 파티 보고서](#) [SAP 포털 액세스 권한 필요]
- SAP 설명서: [ABAP 플랫폼 보안 가이드](#)

모범 사례 6.1 - SAP 네트워크 설계에 보안 및 감사를 기본적으로 포함

SAP 워크로드를 호스트하는 네트워크에 대한 액세스를 보호하는 것은 악의적 활동에 대한 1차 방어선입니다. 비즈니스 요구 사항과 특정 SAP 솔루션을 평가하여 사용해야 하는 포트, 프로토콜 및 트래픽 패턴을 결정합니다. 조직의 보안 표준과 네트워크 설계를 단순화하는 데 사용할 수 있는 도구 및 패턴을 고려합니다. 정기적으로 또는 변경 사항이 발생할 때마다 감사를 실시합니다.

제안 사항 6.1.1 - SAP의 네트워크 트래픽 흐름을 이해

먼저 트래픽 흐름을 이해하는 데서 시작합니다. SAP 워크로드의 네트워크 트래픽 패턴은 인바운드 트래픽, 아웃바운드 트래픽 및 내부 트래픽으로 분류할 수 있습니다. 규칙 세트를 정의하는 데 도움이 되도록 소스 및 대상이 신뢰할 수 있는 네트워크 경계에 속하는지 여부를 식별해야 합니다.

알려진 인바운드 트래픽 및 아웃바운드 트래픽 흐름(예: 사용자 액세스 및 인터페이스 연결) 외에도 SAProuter를 통한 SAP Support, 소스 IP 주소를 기반으로 액세스를 제한하는 SAP SaaS 제품에 대한 연결 등 SAP 관련 요구 사항을 고려합니다.

내부 트래픽의 경우 구성 요소와 시스템 간 트래픽은 물론 AWS 및 공유 서비스도 고려합니다. 예를 들어 [VPC 흐름 로그](#) 및 [VPC Reachability Analyzer](#) 같은 도구는 Amazon VPC로 들어오고 나가는 트래픽 흐름을 이해하는 데 도움이 될 수 있습니다.

자세한 내용은 다음 정보를 참조하세요.

- SAP 설명서: [모든 SAP 제품용 TCP/IP 포트](#)

제안 사항 6.1.2 - 트래픽 흐름을 허용 및 제한하는 옵션을 평가

먼저 온프레미스 네트워크의 사용자 및 시스템을 SAP 시스템이 실행되는 AWS 계정에 연결하는 방법을 이해합니다. 자세한 내용은 다음을 참조하세요. [네트워크와 Amazon VPC 간 연결 옵션](#).

VPC로 들어오고 나가는 네트워크 트래픽의 흐름을 제어하는 두 가지 기본 방법에는 [보안 그룹](#) 및 [네트워크 액세스 제어 목록](#) (네트워크 ACL)을 사용하는 것이 포함됩니다. 보안 그룹은 EC2 인스턴스 수준에서 가상 방화벽 역할을 하여 인바운드 및 아웃바운드 트래픽을 통제합니다. 보안 그룹은 상태 유지

그룹입니다. 네트워크 ACL은 VPC에 대한 선택적 보안 계층으로, 하나 이상의 서브넷으로 들어오고 나가는 트래픽을 통제하는 방화벽 역할을 합니다. 보안 그룹과 달리 네트워크 ACL은 무상태 그룹입니다.

또한 VPC 외부 네트워크 구성 요소의 종속성도 고려합니다. 여기에는 Amazon CloudWatch 엔드포인트와 같이 AWS가 제공하는 외부 네트워크 구성 요소가 포함될 수 있습니다. 또한 운영 체제 패치를 위한 소프트웨어 리포지토리와 같은 인터넷 호스팅 서비스도 포함될 수 있습니다.

AWS의 표준 옵션 외에 SAP 자체에서도 [SAProuter](#), [SAP Web Dispatcher](#) 및 SAP Gateway [네트워크 액세스 제어 목록 사용 등 추가 네트워크 보안 옵션을 제공합니다](#). 이러한 옵션은 AWS 서비스 및 구성과 함께 작동하여 SAP 시스템에 대한 네트워크 액세스를 허용 또는 제한합니다.

자세한 내용은 다음 정보를 참조하세요.

- SAP on AWS 블로그: [SAP on AWS의 VPC 서브넷 영역 조정 패턴](#)
- Well-Architected Framework [보안]: [인프라 보호 – 네트워크 보호](#)
- Well-Architected Framework [관리 및 거버넌스 렌즈]: [네트워크 연결](#)
- SAP 설명서: [네트워크 및 통신 보안](#)

제안 사항 6.1.3 – 설계 지침 및 AWS 도구를 사용하여 네트워크 보안을 단순화

SAP 시스템은 복잡한 통합 요구 사항이 있는 경우가 많으며 클라우드는 네트워크 보안 관리를 단순화하는 추가 방법을 제공합니다. 다음 접근 방식을 고려하세요.

- 관리를 단순화하기 위해 가능하면 개별 IP 주소 또는 IP 범위를 참조하지 않습니다.
- 모든 SAP 워크로드에서 표준 세트의 SAP 시스템 번호를 사용하여 필요한 네트워크 포트의 범위를 축소합니다.
- [VPC 엔드포인트](#) 를 사용하면 Amazon S3, Amazon CloudWatch와 같은 AWS 서비스에 액세스하기 위해 VPC로부터 아웃바운드 인터넷 액세스가 필요하지 않습니다. 가능한 경우 또한 비즈니스 요구 사항에 따라 필요하지 않은 경우 이러한 서비스로 들어오고 나가는 SAP 트래픽이 공용 인터넷을 통과하여 모든 트래픽이 AWS 관리형 네트워크 구성 요소를 통해 라우팅되는 것을 방지할 수 있습니다.
- IP 주소 범위가 아닌 다른 보안 그룹을 참조하는 [VPC 접두사 목록](#) 및/또는 [보안 그룹 규칙](#) 을 사용하여 보안 그룹을 단순화합니다.
- 자동화를 통해 보안 그룹을 생성, 업데이트 및 관리하여 구성 드리프트를 방지합니다.
- VPC 및 AWS 계정 전체에 대한 중앙 집중식 보안 그룹 관리를 제공하기 위해 [AWS Firewall Manager](#) 를 사용하는 것을 고려합니다.

- 백엔드 시스템 진입 지점을 모호하게 만들기 위해 [SAProuter](#) , [SAP Web Dispatcher](#) 및 Elastic Load Balancing을 사용하는 것을 고려합니다.
- 보다 세부적인 액세스 제어를 제공하기 위해 여러 [SAP Internet Communication Manager\(ICM\)](#) 진입 지점을 사용하는 것을 고려합니다.

자세한 내용은 다음 정보를 참조하세요.

- SAP 설명서: [Network-based Access Control Lists](#)
- SAP 설명서: [모든 SAP 제품용 TCP/IP 포트](#)

모범 사례 6.2 - 운영 체제 빌드 및 보호

SAP 소프트웨어의 기반이 되는 운영 체제를 보호하면 악의적인 행위자가 SAP 애플리케이션 내의 데이터에 무단으로 액세스하거나, 소프트웨어 가용성에 영향을 미치거나, 미션 크리티컬 구현을 교란할 가능성이 줄어듭니다. 운영 체제를 보호하는 데 도움이 되도록 SAP, 운영 체제 공급 업체, 데이터베이스 공급 업체 및 AWS의 지침을 따릅니다. 선택한 SAP 솔루션 및 운영 체제에 따라 서비스를 활성화/비활성화하고, 특정 커널 파라미터를 설정하고, 다양한 조합의 보안 패치를 적용해야 할 수 있습니다. SAP 요구 사항과 조직의 요구 사항이 부합하는지 확인하고 충돌을 식별합니다.

제안 사항 6.2.1 – 안전한 운영 체제를 프로비저닝하기 위한 접근 방식을 결정

Amazon Machine Image(AMI)는 EC2 인스턴스를 시작하는 데 필요한 정보를 제공합니다. AMI가 운영 체제 수준에서 안전하다고 확신할 수 있어야 합니다. 그렇지 않으면 AMI가 재사용되고 업데이트되는 과정에서 보안 허점이 많은 수의 인스턴스로 전파될 수 있습니다.

AMI는 운영 체제 공급 업체가 제공하는 표준 이미지일 수도 있고, 자체적으로 빌드하는 사용자 지정 이미지일 수 있습니다. 어떤 경우든 운영 체제가 처음부터 안전하고 지속적으로 유지 관리되도록 하기 위한 일관된 접근 방식이 필요합니다. 이미지 보안 일관성을 달성하는 데 [AWS CloudFormation](#) 같은 코드형 인프라(IaC) 도구를 사용하면 도움이 됩니다. HANA 기반 SAP 솔루션의 경우 [AWS Launch Wizard](#) for SAP는 보안 구성 요소의 설치를 자동화하도록 사용자 지정할 수 있는 사전 및 사후 설치 스크립트 등 설치 프로세스를 단순화합니다.

자세한 내용은 AWS Well-Architected Framework [보안 원칙]의 컴퓨팅 리소스 보호에 대한 지침, 특히 취약성 관리 수행 및 공격 표면 축소에 대한 정보를 참조하세요.

- Well-Architected Framework [보안]: [컴퓨팅 보호](#)

제안 사항 6.2.2 – 안전한 운영 체제를 유지 관리하기 위한 접근 방식을 결정

Well-Architected Framework [보안 원칙]의 컴퓨팅 보호에서 언급했듯이 선택한 운영 체제가 EC2 Image Builder에서 지원되는 경우 SAP 관련 AMI의 빌드, 테스트, 배포 및 지속적인 패치 관리를 단순화할 수 있습니다. 또한 보안 패치 적용을 자동화하여 운영 체제의 보안 태세를 유지하기 위해 AWS Systems Manager 패치 관리자도 조사해야 합니다.

- Well-Architected Framework [보안]: [컴퓨팅 보호](#)
- AWS 설명서: [EC2 Image Builder](#)
- AWS 설명서: [AWS Systems Manager 패치 관리자](#)

제안 사항 6.2.3 – 운영 체제에 적용 가능한 추가 보안 권장 사항을 검토

SAP 소프트웨어의 기본 운영 체제를 강화하는 데 필요한 항목의 전체 목록을 결정합니다. 예를 들어 Linux 기반 시스템에서는 파일 시스템 권한을 SAP 지침에 따라 설정해야 하며 Windows 기반 시스템에서는 관리자 그룹 액세스를 제한하는 것이 모범 사례입니다.

다음과 같은 SAP 관련 권장 사항이 환경에 관련될 수 있습니다.

- SAP 설명서: [SAP NetWeaver 보안 가이드 - 운영 체제 보안](#)

운영 체제	Guidance
모든 지원되는 UNIX/Linux 운영 체제	<ul style="list-style-type: none"> • SAP 설명서: UNIX/LINUX의 SAP 시스템 보안
SUSE Linux Enterprise Server	<ul style="list-style-type: none"> • SAP Note: 2684254 - SAP HANA DB: SAP 애플리케이션 15용 SLES 15 / SLES의 권장 OS 설정 [SAP 포털 액세스 권한 필요] • SAP Note: 2578899 - SUSE Linux Enterprise Server 15: 설치 노트 [SAP 포털 액세스 권한 필요] • 운영 체제별 설명서: SUSE Hardening Guide
Red Hat Enterprise Linux	<ul style="list-style-type: none"> • SAP Note: 2777782 - SAP HANA DB: RHEL 8의 권장 OS 설정 [SAP 포털 액세스 권한 필요] • SAP Note: 2772999 - Red Hat Enterprise Linux 8.x 설치 및 구성 (SELinux 지원에 대한 언급 포함) [SAP 포털 액세스 권한 필요]
Microsoft Windows	<ul style="list-style-type: none"> • SAP 설명서: Windows에서의 SAP 시스템 보안

운영 체제	Guidance
	<ul style="list-style-type: none"> SAP Note: 1837765 - Windows에서 <SID>adm and SAPService<SID>의 보안 정책 [SAP 포털 액세스 권한 필요]
Oracle Enterprise Linux	<ul style="list-style-type: none"> (지침은 SAP 또는 공급 업체 설명서 참조)

제안 사항 6.2.4 – 운영 체제의 보안 태세를 검증

운영 체제를 안전하게 배포하고 패치를 적용했으면 운영 체제 보안 태세를 검증함으로써 운영 체제가 위반 없이 지속적으로 고도의 보안을 유지하도록 할 수 있습니다. 서드 파티 호스트 침입 방지, 침입 탐지, 바이러스 백신 및 운영 체제 방화벽 소프트웨어를 사용하여 이 유효성 검사를 자동화하는 것을 고려합니다.

자세한 내용은 다음 정보를 참조하세요.

- Well-Architected Framework [보안]: [안전한 작동](#)
- Well-Architected Framework [보안]: [탐지](#)
- Well-Architected Framework [보안]: [컴퓨팅 보호](#)

모범 사례 6.3 - 데이터베이스 및 애플리케이션 보호

데이터베이스 및 애플리케이션 계층에서 보안 경계는 필수입니다. 읽기 전용 수준에서 액세스 권한을 얻더라도 악의적인 행위자가 중요한 비즈니스 데이터의 보안을 손상시킬 수 있기 때문입니다. 모든 경우에 데이터베이스 액세스 보호 및 애플리케이션 보안에 대한 표준 SAP 모범 사례를 따르세요. 이는 온프레미스 및 클라우드 기반 설치 모두에 적용되며 SAP 시스템에 지원되는 각 기본 데이터베이스에 대한 지침이 있습니다.

제안 사항 6.3.1 - 선택한 데이터베이스의 데이터베이스 보안에 대한 SAP 지침을 준수

해당 지침은 다음을 참조하세요.

데이터베이스	설명서
SAP HANA	<ul style="list-style-type: none"> AWS 설명서: AWS SAP HANA Security SAP 설명서: SAP HANA Security Guide(SAP HANA 보안 가이드)

데이터베이스	설명서
	<ul style="list-style-type: none"> SAP 설명서: SAP HANA Administration Guide(SAP HANA 관리 가이드) SAP Note: 2159014 - FAQ: SAP HANA Security [SAP 포털 액세스 권한 필요]
SAP ASE	SAP 설명서: Security Administration in SAP ASE(SAP ASE의 보안 관리)
IBM Db2	(지침은 SAP 또는 공급 업체 설명서 참조)
Oracle	SAP 설명서: SAP Database Guide(SAP 데이터베이스 가이드) - Oracle
Microsoft SQL Server	SAP Note: 3019299 - Security Audit Questions or Security Customization in NetWeaver and SQL Server systems(NetWeaver 및 SQL 서버 시스템의 보안 감사 질문 또는 보안 사용자 지정) [SAP 포털 액세스 권한 필요]
SAP MaxDB	SAP 설명서: SAP MaxDB Security Guide(SAP MaxDB 보안 가이드)

제안 사항 6.3.2 – 애플리케이션 보안에 대한 SAP 지침을 준수

SAP NetWeaver 기반 솔루션의 경우 SAP NetWeaver Security Guide에서 권장 지침을 참조할 수 있습니다.

- SAP 설명서: [ABAP 플랫폼 보안 가이드](#)

모범 사례 6.4 - 해당되는 모든 소프트웨어에 업그레이드 및 패치를 적용하기 위한 계획 수립

SAP와 기본 운영 체제 및 데이터베이스 공급 업체는 정기적으로 표준 보안 업데이트를 릴리스하고 취약성을 수정하기 위한 긴급 업데이트도 제공합니다. 각 공급 업체의 최신 보안 정보를 확인하세요. 보안 허점이 발생하지 않도록 SAP 애플리케이션과 모든 기본 구성 요소를 정기적으로 최신 보안 수정 사항으로 업데이트할 것을 권장합니다. 또한 중요한 보안 패치가 릴리스될 때 긴급 수정 사항을 적용할 계획을 수립하는 것이 좋습니다.

제안 사항 6.4.1 - 운영 체제, 데이터베이스 및 소프트웨어 솔루션 공급 업체에서 알림을 구독

다양한 공급 업체 포털에서 보안 업데이트를 구독하면 새로운 보안 문제 및 수정 사항이 릴리스될 경우 이를 인지하는 데 도움이 됩니다. 그러면 필요한 변경을 계획하는 데 도움이 됩니다.

- AWS 설명서: [AWS 보안 공지](#)
- SAP 설명서: [SAP EarlyWatch Alert](#)
- SAP 설명서: [SAP Security News](#)

운영 체제	Guidance
SUSE Linux Enterprise Server	SUSE Update Advisories
Red Hat Enterprise Linux	Red Hat Security Advisories
Microsoft Windows	Microsoft Security Alerts
Oracle Enterprise Linux	Oracle Security Alerts

제안 사항 6.4.2 – 비즈니스 및 구현 작업에 대한 권장 변경 사항 및 위험을 검토

SAP 팀은 시스템 가동 시간의 필요성과 SAP 보안을 개선하기 위해 권장된 시스템 변경의 중요성을 합리적으로 절충하는 방법을 알아야 합니다. 그렇지 않으면 서비스 중단, 재정적 영향, 생산성 손실과 같은 불필요한 위험이 발생할 수 있습니다. 공급 업체가 취약성을 수정할 수 있도록 권장하는 변경 사항 및 구현 단계를 검토하고 즉시 구현 계획을 수립합니다. 이는 이 렌즈에서 논의된 운영 우수성 모범 사례, 특히 보안을 위한 런북 작성과 직접적인 관련이 있습니다.

- SAP Lens [운영 우수성]: [제안 사항 3.4.1 - SAP 보안 작업용 런북을 작성](#)

제안 사항 6.4.3 – 적시에 취약성을 해결하기 위한 계획을 수립

새로운 SAP 보안 권장 사항 및 보안 관련 패치를 최대한 신속하게 적용하는 것이 AWS 기반 SAP 솔루션 및 다른 위치에 설치된 솔루션 모두에 가장 중요합니다. 주기적으로 [SAP Security Notes and News](#)를 검토하고 여기에 수록된 패치, 노트 및 권장 사항을 사용하여 보안 문제를 신속하게 수정하는 프로세스를 생성합니다. 경우에 따라 SAP 관리자는 근본적인 취약성을 해결할 수 있을 때까지 임시로 완화 또는 제어 조치를 취해야 할 수도 있습니다. 또한 사고 대응에 대한 보안 원칙 권장 사항을 따릅니다.

- Well-Architected Framework [보안]: [사고 대응](#)
- SAP 설명서: [SAP Security Notes and News](#)

7 – 자격 증명 및 권한을 통해 SAP 워크로드에 대한 액세스 제어

SAP 워크로드에 대한 액세스는 어떻게 제어합니까? AWS, SAP 및 서드 파티가 제공하는 메커니즘을 사용하여 최종 사용자와 인터페이스 시스템이 적절하게 식별되고 인증되도록 합니다. 최소 권한만 부여하도록 권한이 어떻게 제어됩니까? 액세스 감사 및 보고 방법은 무엇입니까? 먼저 사용자 범주를 식별한 다음 제어 및 자격 증명 관리 접근 방식을 통해 체계적으로 SAP 워크로드에 대한 액세스를 제한합니다.

ID	우선순위	모범 사례
□ BP 7.1	필수	SAP 사용자 범주 및 액세스 메커니즘 이해
□ BP 7.2	필수	SAP 워크로드에 대한 권한 있는 액세스 관리
□ BP 7.3	필수	조직의 자격 증명 관리 접근 방식 및 SAP에 대한 적용 이해
□ BP 7.4	적극 권장	사용자 액세스 및 권한 부여 변경 및 이벤트에 대한 로깅 및 보고 구현

모범 사례 7.1 - SAP 사용자 범주 및 액세스 메커니즘 이해

SAP 시스템에 액세스하는 사용자의 유형이 적용해야 할 보안 제어를 결정합니다. 각 사용 사례를 검토하여 전략을 개발할 수 있습니다. 여기에는 해당 요구 사항을 지원하기 위해 자격 증명, 인증, 도구 및 메커니즘을 관리하는 방법이 포함되어야 합니다.

제안 사항 7.1.1 - 데이터 액세스 권한 및 허용된 작업을 이해

SAP 시스템에는 고도로 민감한 비즈니스 데이터가 포함되는 경우가 많습니다. 사용자 유형을 정의할 때 데이터 액세스 권한을 이해해야 합니다. (예를 들어 관리 데이터베이스 사용자는 애플리케이션 사용자에게 대한 세분화된 제어 권한이 없으며, 따라서 더 중요할 수 있습니다.) 또한 [보안]: [모범 사례 5.2 - SAP 워크로드 내에서 데이터 분류](#)를 참조하세요.

SAP 시스템 액세스와 관련하여 다음 질문을 고려합니다.

- 관리 또는 서비스 사용자가 수행한 작업을 고유하게 식별 가능한 개인이 추적할 수 있어야 합니까?
- 어느 애플리케이션 계층에서 액세스 권한이 부여됩니까?
- 권한을 통해 기능 하위 집합에 대한 액세스를 제한할 수 있습니까?

- 특정 서비스만 공개하는 것과 같이 다른 제어를 통해 기능 하위 집합에 대한 액세스를 제한할 수 있습니까?
- 수행한 작업을 감사해야 합니까?

제안 사항 7.1.2 – 사용자가 SAP 시스템에 액세스하는 네트워크 및/또는 위치를 이해

네트워크 및/또는 위치는 종종 보안 위협 프로필에 영향을 미치며 사용자를 신뢰할 수 있는지 여부를 결정할 수 있습니다. 일반적으로 이것은 무단 액세스를 방지하기 위한 제어와 결합됩니다([모범 사례 6.1 - SAP 네트워크 설계에 보안 및 감사를 기본적으로 포함](#) 참조).

이는 설계에 영향을 미칠 수 있습니다. 예를 들어 신뢰할 수 없는 인터넷 사용자 또는 디바이스는 SAP 워크로드에 액세스하려면 회사 네트워크의 신뢰할 수 있는 사용자와 비교할 때 추가 인증 요소가 필요할 수 있습니다.

모범 사례 7.2 - SAP 워크로드에 대한 권한 있는 액세스 관리

가능한 경우 최소 권한 접근 방식을 채택합니다. 사용성 및 효율성을 관리하면서 최소한의 사용자 집합에게 특정 역할을 수행하는 데 필요한 최소한의 액세스 권한만 부여합니다. 관리 계정(예: <sid>adm)이 있습니다. 기본적으로 이 계정은 SAP 워크로드의 안정성 및 데이터 보안에 상당한 영향을 미칩니다. 이 위험을 제한할 수 있는 방법을 고려합니다.

제안 사항 7.2.1 – AWS 자격 증명 및 인증을 관리

AWS Identity and Access Management(IAM)를 사용하면 AWS 서비스 및 리소스에 대한 액세스를 안전하게 관리할 수 있습니다. IAM을 사용하여 다양한 SAP 및 클라우드 관리 작업에 대한 AWS 사용자 및 그룹을 생성하고 관리할 수 있습니다. IAM 권한을 사용하여 AWS 리소스에 대한 사용자 액세스를 허용 및 거부할 수 있습니다. 표준 지침, 특히 권한 있는(루트) 액세스 권한 제한 및 보호에 대한 지침을 준수해야 합니다.

- AWS 설명서: [IAM 보안 모범 사례](#)

사용자에게 부여되지는 않지만 SAP 애플리케이션의 운영에 필요한 액세스 권한은 최소 권한만 부여하도록 특히 주의해야 합니다.

- AWS 설명서: [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여하기](#)

제안 사항 7.2.2 – SAP 관리 자격 증명 및 인증을 관리

필요한 경우 제한된 기간 동안만 승격된 권한을 승인 및 부여하는 프로세스를 구현합니다. 액세스 권한이 부여된 사용자 및 이유를 기록하는 감사 기능을 사용합니다.

권한 있는 계정의 사용자 이름/암호의 사용을 제한합니다. 가능한 경우 직접 액세스를 비활성화합니다. 자격 증명을 안전하게 저장합니다(예: 권한 있는 액세스 관리 솔루션 또는 암호 저장소).

런북, RunCommand 및 Secrets Manager를 사용하여 특정 작업을 위한 운영 체제 직접 액세스를 제한하기 위해 Systems Manager를 사용할 수 있는 방법을 평가합니다.

- AWS 설명서: [SSM Agent를 통해 루트 수준 명령에 대한 액세스 제한](#)
- AWS 설명서: [Parameter Store에서 AWS Secrets Manager 비밀 참조](#)

모범 사례 7.3 - 조직의 자격 증명 관리 접근 방식 및 SAP에 대한 적용 이해

일반적인 SAP 워크로드의 여러 시스템으로 구성되므로 자격 증명도 여러 개입니다. 이러한 사용자를 관리하기 위한 중앙 집중식 접근 방식은 보안 위험과 운영 복잡성을 줄일 수 있습니다. 중앙 집중식 사용자 관리, 통합 인증(SSO) 및 멀티 팩터 인증을 고려하여 접근 방식에서 AWS 서비스 및 서드 파티 도구를 사용하는 방법에 초점을 맞춥니다.

제안 사항 7.3.1 – 명명된 사용자에게 대한 자격 증명 공급자를 결정

사용자는 Active Directory와 같은 자격 증명 스토어와 연결됩니다. 이는 역할, 권한, 식별자와 같은 자격 증명 정보를 관리하기 위한 중앙 리포지토리 역할을 합니다. 각 자격 증명 세트에 대해 자격 증명 공급자와 연결할 수 있는지 여부를 판단합니다. 자격 증명 공급자를 사용하면 사용자 인증을 오프로드할 수 있습니다. 통합 인증(SSO)을 용이하게 하고 사용자 자격 증명 수명 주기(예: 입사, 전근, 퇴사)도 관리합니다.

사람과 연결되지 않은 명명된 사용자에게 대한 예외를 고려합니다. 여기에는 배치, 작업 예약, 통합 및 모니터링 사용자가 포함될 수 있습니다.

- AWS 설명서: [AWS Directory Service | Amazon Web Services\(AWS\)](#)

제안 사항 7.3.2 – 인증 메커니즘을 결정

SAP 워크로드의 각 계층에서 지원되는 인증 메커니즘(예: SAML, Kerberos, X.509, SAP Single Sign-On 티켓)을 이해합니다. 애플리케이션과 통합하기 위한 요구 사항을 평가합니다. 여러 사용자 자격 증명을 관리할 때 관리 및 보안에 미치는 영향을 방지하려면 가능한 경우 통합 인증(SSO)을 사용합니다.

- SAP 설명서: [User Authentication and single sign-on\(사용자 인증 및 통합 인증\)](#)

- AWS 설명서: [Cloud applications - AWS Single Sign-On\(클라우드 애플리케이션 - AWS Single Sign-On\)](#)
- SAP on AWS 블로그: [Enable SAP Single Sign On with AWS SSO Part 1: Integrate SAP NetWeaver ABAP with AWS SSO\(AWS SSO를 사용하여 SAP Single Sign On 활성화 1부: SAP NetWeaver ABAP를 AWS SSO와 통합\)](#)
- SAP on AWS 블로그: [Enable SAP Single Sign On with AWS SSO Part 2: Integrate SAP NetWeaver Java\(AWS SSO를 사용하여 SAP Single Sign On 활성화 2부: SAP NetWeaver Java 통합\)](#)
- SAP on AWS 블로그: [Enable Single Sign On for SAP Cloud Platform Foundry and SAP Cloud Platform Neo with AWS SSO\(AWS SSO를 사용하여 SAP 클라우드 플랫폼 Foundry 및 SAP 클라우드 플랫폼 Neo용 통합 인증 활성화\)](#)

제안 사항 7.3.3 – 멀티 팩터 인증을 고려

멀티 팩터 인증(MFA)은 로그인 자격 증명 위에 추가 보호 계층을 더하는 모범 사례입니다. 이러한 멀티 팩터는 SAP 애플리케이션의 보안을 강화합니다. 사용 사례에는 신뢰할 수 없는 디바이스에서 SAP에 액세스, AWS Management Console에 액세스, 백업 삭제 또는 EC2 인스턴스 종료와 같은 권한 있는 작업이 포함됩니다.

- SAP on AWS 블로그: [Securing SAP Fiori with MFA\(MFA를 사용하여 SAP Fiori 보호\)](#)
- AWS 설명서: [Using MFA devices with your IAM sign-in page\(IAM 로그인 페이지에서 MFA 디바이스 사용\) - AWS Identity and Access](#)
- AWS 설명서: [Configuring MFA delete\(MFA 삭제 구성\) - Amazon Simple Storage Service](#)
- AWS 설명서: [Amazon EC2: Requires MFA \(GetSessionToken\) for specific EC2 operations\(Amazon EC2: 특정 EC2 작업에 MFA\(GetSessionToken\) 필요\)](#)

제안 사항 7.3.4 – 인증서 관리 접근 방식을 결정

클라이언트 기반 인증서는 자격 증명 필요 없이 인증에 사용할 수 있습니다. 세션 관리를 위한 시간 기반 만료와 시스템 간 통신을 위한 인증서 교체를 포함하는 접근 방식을 결정합니다. AWS는 SAP에서 신뢰하는 인증 기관을 제공합니다. 인증서는 [AWS Certificate Manager\(ACM\)](#) 를 사용하여 발급 및 관리할 수 있습니다.

- SAP Note: [2801396 - SAP Global Trust List \[SAP 포털 액세스 권한 필요\]](#)
- SAP Note: [3040959 - ABAP에서 CA 서명 서버 인증서를 얻는 방법 \[SAP 포털 액세스 권한 필요\]](#)
- SAP Lens [운영 우수성]: [제안 사항 3.4.1 - SAP 보안 작업용 런북을 작성](#)

- SAP Lens [운영 우수성]: [제안 사항 4.1.2 - 자격 증명, 인증서 및 라이선스 만료 캘린더를 유지](#)

모범 사례 7.4 - 사용자 액세스 및 권한 부여 변경 및 이벤트에 대한 로깅 및 보고 구현

SAP 시스템에서 사용자 액세스 및 권한 부여 이벤트는 정기적으로 기록, 분석 및 감사해야 합니다. SAP 애플리케이션 및 데이터베이스의 보안 이벤트를 아키텍처의 다른 구성 요소와 통합하고 상호 연결합니다. 그러면 심각한 보안 문제 또는 위반이 발생한 경우 엔드투엔드 추적이 가능합니다. 중앙 보안 정보 및 이벤트 관리(SIEM) 시스템에서 이벤트 분석을 자동화합니다. 이를 통해 운영 팀은 정상적인 시스템 제어 범위를 벗어나는 예상치 못한 활동 또는 의심스러운 활동이 발생하는지 파악할 수 있습니다. 그런 다음 필요에 따라 수정할 수 있습니다.

제안 사항 7.4.1 – AWS Identity and Access Management(IAM) 이벤트를 로그

AWS IAM 이벤트의 로그를 유지하는 것을 고려합니다. 이 로그는 AWS 계정 내의 사용자 및 권한 부여 변경 사항을 탐지 또는 감사하는 데 사용할 수 있습니다. 조직에 필요한 보안 정책에 따라 로그 보존 기간 및 로그할 이벤트 유형을 결정합니다.

운영 팀이 SAP 시스템의 인프라 수준에서 감사 질문에 답변할 수 있도록 지원합니다.

- 새 AWS 콘솔/CLI 사용자를 누가 언제 생성했습니까?
- AWS IAM 역할을 누가 언제 수정했습니까?
- AWS 사용자가 마지막으로 로그인한 시간은 언제입니까?
- AWS 계정에 대한 의심스러운 로그인 시도 실패가 있었습니까?

자세한 내용은 다음을 참조하세요.

- AWS 설명서: [IAM 모범 사례: AWS 계정에서 활동 모니터링](#)
- AWS 설명서: [AWS CloudTrail을 사용하여 IAM 및 AWS STS API 호출 로깅](#)
- AWS Well-Architected Framework [보안]: [탐지](#)
- AWS 보안 블로그 [Amazon GuardDuty 조사 결과 시각화](#)

제안 사항 7.4.2 – 운영 체제의 사용자 및 권한 부여 변경 사항을 로그

탐지 또는 감사에 사용할 수 있도록 운영 체제(OS) 사용자 및 권한 부여 이벤트의 로그를 유지하는 것을 고려합니다. 조직에 필요한 보안 정책에 따라 로그 보존 기간 및 로그할 이벤트 유형을 결정합니다.

운영 팀이 SAP 시스템의 운영 체제 수준에서 다음과 같은 감사 질문에 답변할 수 있도록 지원합니다.

- 새 슈퍼 사용자 OS 계정을 누가 언제 생성했습니까?
- OS 계정 권한을 누가 언제 수정했습니까?
- OS 사용자가 마지막으로 로그인한 시간은 언제입니까?
- OS 계정에 대한 의심스러운 로그인 시도 실패가 있었습니까?
- OS 사용자가 승격된 권한을 마지막으로 사용한 시기는 언제입니까?

운영 체제 수준 감사에 대한 자세한 내용은 다음을 참조하세요.

운영 체제	Guidance
SUSE Linux Enterprise Server	Setting Up the Linux Audit Framework Security Guide(Linux Audit Framework 설정 보안 가이드)
Red Hat Enterprise Linux	Chapter 13. Auditing the system Red Hat Enterprise Linux 8 Security Guide(13장. Red Hat Enterprise Linux 8 시스템 감사 보안 가이드)
Microsoft Windows	Windows 감사 정책 권장 사항
Oracle Enterprise Linux	Oracle Linux 8 Enhancing System Security - Auditing and Monitoring(시스템 보안을 개선하는 Oracle Linux 8 - 감사 및 모니터링)

제안 사항 7.4.3 – SAP 애플리케이션, 데이터베이스 사용자 및 권한 부여 이벤트를 로그

탐지 또는 감사에 사용할 수 있도록 SAP 사용자 및 권한 부여 이벤트의 로그를 유지하는 것을 고려합니다. 애플리케이션 스택(예: ABAP 권한 부여)과 데이터베이스(예: SAP HANA)를 모두 고려합니다. 조직에 필요한 보안 정책에 따라 로그 보존 기간 및 로그할 이벤트 유형을 결정합니다.

운영 팀이 SAP 애플리케이션 및 데이터베이스 수준에서 다음과 같은 이벤트에 대한 감사 질문에 답변할 수 있도록 지원합니다.

- 새 SAP 또는 데이터베이스 계정을 누가 언제 생성했습니까?
- SAP 또는 데이터베이스 계정 권한을 누가 언제 수정했습니까?
- SAP 또는 데이터베이스 사용자가 마지막으로 로그인한 시간은 언제입니까?
- 계정에 대한 의심스러운 로그인 시도 실패가 있었습니까?
- 계정이 마지막으로 사용한 민감한 트랜잭션 코드 또는 도구는 무엇입니까?

자세한 내용은 다음을 참조하세요.

- SAP 설명서: [SAP Access Control and Governance | User Access\(SAP 액세스 제어 및 거버넌스 | 사용자 액세스\)](#)
- SAP 설명서: [SAP NetWeaver ABAP: The Security Audit Log\(SAP NetWeaver ABAP: 보안 감사 로그\)](#)
- SAP 설명서: [SAP NetWeaver JAVA: The Security Audit Log\(SAP NetWeaver JAVA: 보안 감사 로그\)](#)
- SAP 설명서: [SAP HANA: Auditing Activity in SAP HANA\(SAP HANA: SAP HANA의 감사 활동\)](#)

제안 사항 7.4.4 – 분석을 위해 보안 정보 및 이벤트 관리(SIEM) 시스템에서 사용자 및 권한 부여 이벤트를 통합

상관 관계 및 분석이 가능하도록 SAP 워크로드 구성 요소 전체에서 모든 사용자 및 권한 부여 이벤트를 중앙 SIEM 도구로 보내는 것을 고려합니다. SAP Enterprise Threat Detection, 서드 파티 추가 기능 같은 도구를 사용하거나 SAP 감사 로그를 애플리케이션 및 데이터베이스 서버에서 수집 및 분석 도구로 직접 보냅니다.

워크로드의 기존 동작을 설정하고 이상 동작을 모니터링하여 보안 사고 탐지를 개선합니다.

실시간으로 워크로드를 모니터링하고, 보안 문제를 식별하고, 근본 원인 분석 및 수정을 신속하게 처리할 수 있도록 [AWS Marketplace SIEM 솔루션](#) 을 고려합니다.

자세한 내용은 다음 리소스를 참조하세요.

- AWS Marketplace: [SIEM 솔루션](#)
- AWS 설명서: [AWS Security Hub](#)
- SAP 설명서: [SAP Enterprise Threat Detection](#)
- Well-Architected Framework [보안]: [Security Incident Response\(보안 사고 대응\)](#)
- AWS 설명서: [AWS Security Incident Response\(AWS 보안 사고 대응\) - 기술 백서](#)

8 - 저장 및 전송 중 SAP 데이터 보호

SAP 데이터를 어떻게 보호합니까? SAP 시스템에서는 종종 비즈니스의 핵심 기능이 실행되고 민감한 엔터프라이즈 데이터가 저장됩니다. 모범 사례는 하나 이상의 암호화 메커니즘을 사용하여 저장 및 전송 중 데이터를 암호화함으로써 내부 또는 외부 보안 요구 사항 및 제어를 충족하는 것입니다. 또한 [AWS 공동 책임 모델](#) 에 나열된 제어 외에 AWS는 여러 암호화 솔루션을 제공합니다. 많은 AWS 서비

스에는 최소한의 작업과 성능 영향으로 암호화를 활성화할 수 있는 기능이 있습니다. 고려할 수 있는 데이터베이스 및 SAP 애플리케이션 계층에 사용할 수 있는 암호화 옵션이 있습니다.

ID	우선순위	모범 사례
□ BP 8.1	적극 권장	저장 데이터 암호화
□ BP 8.2	적극 권장	전송 중 데이터 암호화
□ BP 8.3	적극 권장	데이터 복구 메커니즘을 위협으로부터 보호

모범 사례 8.1 – 저장 데이터 암호화

저장 데이터는 디지털 방식으로 저장된 모든 데이터를 말합니다. AWS는 암호화를 사용하여 이 데이터가 승인된 사용자에게만 표시되고 스토리지 또는 데이터베이스에 대한 액세스가 손상될 경우 애플리케이션과 독립적으로 보호된 상태를 유지하도록 합니다.

제안 사항 8.1.1 – 암호화를 적용할 수준을 정의

일반적으로 암호화를 배포하는 스택이 높을수록 데이터가 안전해집니다. 그러나 보안이 강화되는 한편으로 배포 및 관리 복잡성도 가중됩니다. 해당 서비스 내에서 사용 가능한 저장 데이터 암호화 옵션을 사용하는 것이 좋습니다. 필요한 경우 [보안]: [모범 사례 5.3 – SAP 워크로드에 대한 특정 보안 제어가 필요한지 평가](#)에 정의된 대로 추가 운영 체제 또는 데이터베이스 암호화를 고려합니다.

제안 사항 8.1.2 – SAP 서비스 및 솔루션에 대한 AWS 암호화 옵션을 이해

SAP가 저장 데이터에 사용하는 핵심 AWS 서비스는 Amazon EC2(AMI 및 EBS 볼륨), Amazon FSx for Windows File Server 또는 공유 파일 시스템용 Amazon EFS 및 백업 또는 기타 객체 스토어 사용 사례용 Amazon S3입니다.

- AWS 설명서: [EBS 지원 AMI에서 암호화 사용](#)
- AWS 설명서: [Amazon EBS 암호화](#)
- AWS 설명서: [Amazon EFS 암호화](#) / [Amazon FSx 암호화](#)
- AWS 설명서: [Amazon S3 암호화](#)

이러한 서비스에 저장된 데이터는 AWS KMS의 AWS 또는 고객 관리형 키 중 하나를 사용하여 저장 데이터로 암호화될 수 있습니다.

운영 체제 암호화 옵션에는 BitLocker, DM-crypt, SuSE Remote Disk가 포함됩니다.

다음 링크는 데이터베이스용 암호화 옵션에 대한 정보를 찾는 데 도움이 될 수 있습니다.

데이터베이스	Guidance
SAP HANA	SAP 설명서: 서버 측 데이터 암호화 서비스
SAP ASE	SAP 설명서: SAP ASE 암호화 개요
IBM Db2	IBM 설명서: Db2 암호화 개요
Oracle	SAP Note: 2591575 - SAP NetWeaver와 함께 Oracle 투명한 데이터 암호화(TDE) 사용 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 1380493 - SQL Server 투명한 데이터 암호화(TDE) [SAP 포털 액세스 권한 필요]
SAP MaxDB	SAP 설명서: SAP MaxDB 데이터베이스 관리 - 암호화

제안 사항 8.1.3 – 암호화 방법 및 키 관리 스토어를 정의

일반적으로 키 관리는 엔터프라이즈 수준에서 정의되며, 이에 따라 SAP 워크로드에 사용할 수 있는 키 관리 옵션이 결정됩니다. AWS KMS는 AWS 서비스용 암호화 키의 관리를 단순화하는 안전하고 복원력 있는 서비스입니다. 자체 하드웨어 보안 모듈(HSM)을 관리해야 하는 요구 사항이 있는 경우 AWS CloudHSM을 사용할 수 있습니다.

- AWS 설명서: [AWS 암호화 도구 및 서비스 옵션](#)
- AWS 설명서: [AWS Key Management Service\(AWS KMS\)](#)
- AWS 설명서: [AWS CloudHSM](#)

마스터 키를 보호하기 위한 메커니즘도 고려해야 합니다. 어떻게 키에 대한 액세스를 제한하고, 교체를 관리하고, 복구 가능성을 보장합니까?

HANA 저장 데이터 암호화 루트 키는 파일 시스템(Instance SSFS) 또는 SAP Data Custodian SaaS Solution의 인스턴스 보안 스토어에만 안전하게 저장할 수 있습니다. 인스턴스 스토어를 사용하는 경우 마스터 키는 교체 정책을 적용하여 [AWS Secrets Manager](#) 에 저장할 수 있습니다.

- SAP Note: [2154997 - hdbuserstore 엔트리를 ABAP SSFS로 마이그레이션](#) [SAP 포털 액세스 권한 필요]

- SAP Note: [2755815 - Hana의 저장 데이터 암호화 복구 가능성을 보장하는 방법](#) [SAP 포털 액세스 권한 필요]

모범 사례 8.2 – 전송 중 데이터 암호화

전송 중 데이터 암호화를 사용하면 데이터가 한 지점에서 다른 지점으로 이동하는 동안 데이터를 가로채거나 액세스하거나 변조하기가 더 어려워집니다. 잠재적 위협을 최소화하고 요구 사항에 부합하는 보호 수준을 제공하려면 보안 프로토콜 및 네트워크 수준 암호화를 사용해야 합니다.

Well-Architected Framework [보안]: [전송 중 데이터 보호](#)

제안 사항 8.2.1 – SAP 및 데이터베이스 프로토콜을 기반으로 애플리케이션 트래픽을 암호화

SAP 프로토콜(SAPGUI Dialog, RFC 및 CPIC)을 사용하는 애플리케이션 트래픽의 경우 SAP SNC를 사용하여 전송 계층 보안을 적용합니다.

- SAP 설명서: [SAP 시스템의 SNC 보호 통신 경로](#)

데이터베이스 트래픽의 경우 가능하면 클라이언트와 데이터베이스 간에 보안 연결을 사용합니다.

데이터베이스	Guidance
SAP HANA	SAP 설명서: SAP HANA: 데이터 통신 보호
SAP ASE	SAP 설명서: SAP ASE의 SSL
IBM Db2	SAP Note: 2385640 - DB6: SSL 암호화를 사용해 데이터베이스 연결 [SAP 포털 액세스 권한 필요]
Oracle	SAP Note: 973450 - Oracle Database 네트워크 암호화 및 데이터 무결성 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 1570930 - SAP로 SQL Server 네트워크 암호화 [SAP 포털 액세스 권한 필요]
SAP MaxDB	SAP 설명서: MaxDB 네트워크 및 통신

제안 사항 8.2.2 – 인터넷 프로토콜을 기반으로 SAP 애플리케이션 트래픽을 암호화

인터넷 프로토콜(HTTP, P4(RMI), LDAP)을 기반으로 하는 애플리케이션 트래픽의 경우 SSL/TLS를 사용하여 전송 계층 보안을 적용합니다.

- SAP 설명서: [전송 계층 보안](#)

제안 사항 8.2.3 – 파일 전송 또는 메시지 전송 프로토콜을 기반으로 데이터 교환을 암호화

파일 기반 전송의 경우 AWS는 SFTP 또는 FTPS를 통한 보안 파일 교환을 위해 AWS Transfer Family를 제공합니다. AWS Transfer Family는 Amazon S3 및 Amazon EFS와의 데이터 전송을 지원합니다.

- AWS 설명서: [AWS Transfer Family](#)

메시지 수준 데이터 무결성 검사를 사용하면 데이터가 전송되는 동안 변조되지 않도록 하는 데 도움이 됩니다. 메시지에 포함된 데이터의 무결성을 서명 및 확인할 수 있도록 SAP가 지원하는 하나 이상의 메시지 수준 보안 표준을 사용하는 것을 고려합니다.

- SAP 설명서: [SAP ABAP 웹 서비스 메시지 수준 보안](#)
- SAP 설명서: [SAP NetWeaver 프로세스 통합 보안 가이드](#)
- SAP 설명서: [SAP 클라우드 통합 메시지 수준 보안](#)

IDOC 기반 메시지의 경우 SNC를 사용하여 ALE에서 사용하는 RFC 연결을 보호합니다.

- SAP 설명서: [IDocs에서 민감한 데이터 처리](#)

제안 사항 8.2.4 – 관리 액세스를 암호화

SAP 관리를 위해 Windows 및 SSH 기반 도구를 모두 사용하는 것이 일반적입니다. 배스천 호스트와 같은 보안 제어 외에 이 트래픽을 암호화할 수 있는지 여부를 고려합니다.

또는, [AWS Systems Manager Session Manager](#) 는 암호화를 위해 AWS Management Console을 통해 TLS를 사용하여 운영 체제에 액세스하는 보안 메커니즘을 제공합니다.

- AWS 설명서: [Amazon EC2 Windows 가이드 - 전송 중 암호화](#)
- AWS 설명서: [Amazon EC2 Linux 가이드 - 전송 중 암호화](#)
- AWS 설명서: [AWS Systems Manager의 데이터 보호 - 데이터 암호화](#)

제안 사항 8.2.5 – AWS 서비스의 전송 중 암호화 기능을 평가

애플리케이션 기반 암호화 외에 많은 AWS 서비스가 전송 중 암호화 기능을 제공합니다. 각 서비스에
서 기업 표준, 구현 작업 및 관련 이점을 평가합니다. 다음은 SAP 워크로드와 관련된 몇 가지 예입니다.

- AWS 설명서: [Amazon S3 - 전송 중 암호화](#) - 기본적으로 활성화되며 Amazon S3로의 백업에 권장됩니다.
- AWS 설명서: [Amazon EFS - 전송 중 암호화](#) / [Amazon FSx](#) - 공유 파일 시스템에 필요할 수 있습니다.
- AWS 설명서: [Elastic Load Balancing](#) - 일부 로드 밸런서 유형에서는 이 기능을 사용할 수 없으므로 암호화 요구 사항과 패스스루가 있는 엔드투엔드 TLS가 필요한지 여부를 검토하세요.
- AWS 설명서: [Amazon EC2 - 전송 중 암호화](#) - 최근 세대 인스턴스 유형에만 이 기능이 있습니다.

제안 사항 8.2.6 – 네트워크 수준 암호화를 구현

SAP 고객은 일반적으로 Direct Connect를 단독으로 또는 VPN과 함께 사용하여 AWS의 리소스에 대한 안정적인 연결을 제공합니다.

AWS Direct Connect는 전송 중 트래픽을 암호화하지 않습니다. 암호화가 필요한 경우 예를 들어 VPN over Direct Connect를 사용하여 전송 수준 암호화를 구현해야 합니다.

AWS는 네트워크 채널 암호화에 사용할 수 있는 Site-to-Site VPN을 제공합니다. AWS Marketplace에서 또는 기존 보유 라이선스 사용 모델을 통해 OpenVPN과 같은 서드 파티 VPN 솔루션을 배포하는 것을 선택할 수도 있습니다.

- AWS 설명서: [AWS 관리형 VPN](#)
- AWS 설명서: [AWS Direct Connect + VPN](#)
- AWS 설명서: [소프트웨어 Site-to-Site VPN](#)

모범 사례 8.3 - 데이터 복구 메커니즘을 위협으로부터 보호

악의적인 활동으로부터 보호될 수 있도록 조직의 보안 프레임워크에 명시된 지침을 따릅니다. [eBook: 랜섬웨어로부터 AWS 클라우드 환경 보호](#) 는 네트워크 제어, 패치, 최소 권한 등 사고 발생 이전 및 사고 대응 과정에서 해결해야 할 주요 항목을 개괄합니다. SAP 시스템의 경우 위협은 다른 애플리케이션과 유사하지만 잠재적 영향은 더 큼니다. SAP가 레코드 시스템이거나 미션 크리티컬 트랜잭션에 필요한 경우 악의적인 공격으로부터 백업을 보호하도록 다음 제안 사항을 고려하세요.

- SAP Note: [2663467 - 랜섬웨어 상황을 방지하는 팁](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2496239 - Windows의 랜섬웨어 / 맬웨어](#) [SAP 포털 액세스 권한 필요]

제안 사항 8.3.1 – 별도 계정에서 추가 제어를 사용하여 백업을 보호

데이터의 기본 복사본과 격리된 계정에서 직접 또는 복제를 사용하여 백업을 보호하면 손상된 시스템이 데이터 복구 메커니즘에도 영향을 미치는 위험을 최소화할 수 있습니다.

보조 계정은 사용 사례에 부합하는 액세스 요구 사항이 적용된 '데이터 벙커'로 볼 수 있습니다.

Amazon S3를 사용하는 백업의 경우 추가 제어에 Write-Once-Read-Many(WORM) 모델 또는 [멀티 팩터 인증 삭제](#)를 사용하여 객체를 저장하기 위한 S3 객체 잠금이 포함될 수 있습니다.

복제를 사용하는 경우 [삭제 마커 복제](#) (삭제 마커는 기본적으로 복제되지 않음) 및 [S3 복제 시간 제어](#) 등 사용 가능한 여러 옵션을 파악합니다. 비용을 최적화하려면 기본 버킷과 보조 버킷 모두에서 하우스 키피ング을 수행해야 합니다.

제안 사항 8.3.2 – 복구 능력을 검증

데이터를 악의적인 활동으로부터 보호할 때 백업이 최후 방어선이지만 불완전한 백업 또는 유효하지 않은 백업으로 인해 복구가 불가능하다면 가치가 없을 수 있습니다. 백업에 액세스할 수 없거나 암호를 해독할 수 없는 경우 복구가 불가능할 수 있습니다. 암호화 키 및 자격 증명을 보호하는 방법을 고려합니다.

대체 계정에서 재빌드를 포함하여 악의적인 시나리오에 맞춰 복구 테스트를 수행합니다.

- SAP Lens [운영 우수성]: [모범 사례 4.3 - 정기적으로 비즈니스 연속성 계획 및 장애 복구 테스트](#)

9 - 보안 이벤트 로그, 테스트 및 대응을 위한 보안 전략 구현

적절한 로깅, 테스트 및 문서화된 대응 방법론으로 지원되는 전략적 보안 계획이 있습니까? 전략적 보안 계획을 수립하면 모든 보안 문제에 성공적으로 대응하기 위해 수행해야 하는 사전 예방 및 사후 대응 작업을 구성하는 데 도움이 됩니다. SAP on AWS 워크로드에 대한 보안 사고를 식별하고 해결하는 데 도움이 되는 로깅, 탐지 및 추가 보호를 위한 절차는 Well-Architected Framework 보안 원칙에 자세히 설명된 절차와 동일합니다. 이 섹션의 지침과 함께 보안 원칙 내의 탐지 및 사고 대응에 관한 모범 사례를 검토하세요.

ID	우선순위	모범 사례
□ BP 9.1	필수	SAP 애플리케이션 및 데이터베이스 로그 분석을 위한 보안 전략 이해

ID	우선순위	모범 사례
□ BP 9.2	적극 권장	보안 버그에 대한 주기적 테스트 수행
□ BP 9.3	적극 권장	보안 이벤트 대응 계획 문서화

- Well-Architected Framework [보안]: [탐지](#)
- Well-Architected Framework [보안]: [사고 대응](#)

모범 사례 9.1 - SAP 애플리케이션 및 데이터베이스 보안 로그 분석을 위한 전략 이해

적절한 세분 수준의 보안 로그를 유지하지 않을 경우 사고 대응, 포렌식 보안 분석 및 위협 모델링에 필요한 중요한 데이터가 손실될 수 있습니다. SAP 보안 담당자는 비즈니스 보안 요구 사항에 따라 SAP 시스템에 영향을 미치는 잠재적인 보안 사고를 평가할 수 있어야 합니다. AWS에서 실행되는 SAP 워크로드의 경우 Well-Architected Framework 보안 원칙에 설명된 AWS 서비스는 다음 제안 사항과 함께 유용한 출발점입니다.

- Well-Architected Framework [보안]: [탐지 - 구성](#)

제안 사항 9.1.1 – 보안 이벤트를 탐지하는 데 필요한 로그를 결정

개별 SAP 소프트웨어 및 지원되는 데이터베이스의 경우 적용 가능한 로그(예: [읽기 액세스 로깅](#))은 SAP NetWeaver Guide Finder 및 SAP NetWeaver Security Guide를 참조하세요. 또한 [보안 로깅](#) 및 개발 작업 모범 사례와 관련된 주제에 대한 SAP Advisory를 검토하세요.

- SAP 설명서: [SAP NetWeaver Guide Finder](#)
- SAP 설명서: [ABAP 플랫폼 보안 가이드](#)
- SAP 설명서: [보안 로깅](#)

제안 사항 9.1.2 - 로그 저장 및 분석을 위한 메커니즘을 개발

모든 안전한 SAP 설치에는 잠재적인 보안 이벤트에 관한 관련 데이터가 있어야 하지만, 해당 데이터를 안전하게 저장하고 효율적이고 시기 적절하게 데이터를 검색 및 분석하는 데 필요한 도구를 갖추는 것도 마찬가지로 중요합니다. AWS 내부에서의 옵션 중 하나는 [CloudWatch 에이전트](#)를 사용하여 [Amazon CloudWatch 로그 그룹](#)에 보안과 관련된 인스턴스 로그 및 SAP 애플리케이션 로그를 저장하

는 것입니다. 또한 이러한 로그를 [Amazon S3로 내보내](#) 전체적 로그 분석 및 [서드 파티 로그 분석 솔루션](#) 통합에도 사용할 수 있습니다.

SAP on AWS 보안 로그 어셈블, 결합 및 분석에 관한 도움은 다음을 참조하세요.

- SAP Lens [보안]: [제안 사항 7.4.4 - 분석을 위해 보안 정보 및 이벤트 관리\(SIEM\) 시스템에서 사용자 및 권한 부여 이벤트를 통합](#)
- SAP on AWS 블로그: [SAP HANA 모니터링: Amazon CloudWatch를 사용하는 서버리스 접근 방식](#)
- SAP on AWS 블로그: [SAP 모니터링: Amazon CloudWatch를 사용하는 서버리스 접근 방식](#)

모범 사례 9.2 - 보안 버그에 대한 주기적 테스트 수행

Well-Architected Framework 보안 원칙 사고 대응의 시뮬레이션 섹션에 설명된 대로 런북 작성 및 게임 데이 실시하는 SAP on AWS 워크로드를 포함하여 모든 워크로드에 권장됩니다. 이러한 유형의 주기적 테스트를 통해 새로운 공격 벡터 및 취약성을 식별하고 보안 사고 발생 시 신속하고 효과적인 대응을 위한 SAP 보안 리소스를 준비할 수 있습니다.

Well-Architected Framework [보안]: [사고 대응 - 시뮬레이션](#)

제안 사항 9.2.1 – 표준 보안 및 침투 테스트 외에 SAP 애플리케이션을 대상으로 포함

탐색적 보안 테스트는 보안 환경을 유지하는 데 중요한 부분입니다. AWS에서 표준 침투 테스트를 수행하는 외에 SAP 솔루션을 악의적인 활동의 잠재적 대상으로 추가해야 합니다. SAProuter, Web Dispatcher, Cloud Connector, SAP Fiori와 같이 아키텍처에서 자주 공개되는 SAP 전용 소프트웨어 솔루션을 염두에 두세요.

- AWS 설명서: [침투 테스트](#)

모범 사례 9.3 - 보안 이벤트 대응 계획 문서화

SAP 애플리케이션이 관련된 보안 이벤트를 처리하기 위한 계획이 문서화되어 있지 않으면 보안 팀의 대응이 지연되고, 덜 포괄적이고, 이벤트를 완화하고 원인을 파악하는 데 덜 효과적일 수 있습니다. SAP 애플리케이션에 대한 보안 대응 패턴을 철저히 문서화하세요.

제안 사항 9.3.1 - 사고 관리 계획을 문서화하여 보안 이벤트에 대비

이는 AWS Well-Architected Framework 보안 원칙의 사고 대응 준비 지침과 직접 연결됩니다. 이 문서를 참조하여 SAP 애플리케이션을 적절히 포함시켜야 합니다.

- Well-Architected Framework [보안]: [사고 대응 - 준비](#)

안정성

안정성 원칙에서는 워크로드의 기능이 필요한 때에 기능을 정확하고 일관되게 수행하는 역량에 대해 다룹니다. 여기에는 전체 수명 주기에 걸쳐 워크로드를 운영 및 테스트할 수 있는 기능이 포함됩니다. 많은 비즈니스에서 Well-Architected 방식의 안정성은 SAP 워크로드의 핵심 요구 사항입니다. 많은 SAP 워크로드가 미션 크리티컬한 특성이 있고 SAP 아키텍처 및 이에 따른 제한 사항을 이해해야 하기 때문입니다.

다른 원칙과 마찬가지로 AWS Well-Architected Framework, 특히 기초, 변경 관리 및 장애 관리에 대한 모범 사례를 검토하는 것이 좋습니다. SAP Lens의 안정성을 고려할 때 먼저 이러한 요구 사항을 제기 한 비즈니스 우선 순위를 포함하여 개별 시스템 전반의 비기능적 요구 사항을 명확하고 균형 있게 이해 하는 데 중점을 두어야 합니다. 그런 다음 가용성과 재해 복구(DR)를 구분합니다. 가용성은 구성 요소 장애에도 불구하고 최종 사용자가 SAP 시스템에 계속 액세스할 수 있는 시나리오입니다. 전체 워크로드를 사용할 수 없는 시나리오에서는 DR 이벤트가 선언됩니다.

10 – 내결함 설계

장애를 견디도록 SAP 워크로드를 설계하려면 어떻게 해야 합니까? 비즈니스 요구 사항에서 거슬러 올라가며 SAP 인프라 및 데이터의 가용성 목표를 충족하기 위한 접근 방식을 정의합니다. 각 장애 시나리오에서 복원력 요구 사항, 허용 가능한 데이터 손실 및 평균 복구 시간(MTTR)은 구성 요소 및 해당 구성 요소가 지원하는 비즈니스 애플리케이션의 중요도에 비례해야 합니다. SAP 가용성을 위해 제공 되는 아키텍처 패턴은 대부분의 고객 요구 사항을 충족하지만 정의하는 기준에 따라 조정할 수 있습니다. 이러한 기준에는 각 장애에 대해 인지된 위험 및 영향이 포함되며 비용 및 성능도 고려되어야 합니다. 모든 경우에서 초기 및 주기적 테스트를 사용하여 결정 사항을 검증합니다.

ID	우선순위	모범 사례
□ BP 10.1	필수	비즈니스 요구 사항에 부합하는 SAP 워크로드 가용성 목표에 합의
□ BP 10.2	적극 권장	가용성 및 용량 요구 사항에 적합한 SAP 배포 패턴 선택
□ BP 10.3	적극 권장	중요 SAP 데이터의 가용성을 보장할 수 있도록 접근 방식 정의
□ BP 10.4	권장	비즈니스 요구 사항에 기반한 일련의 기준에 따라 설계 검증

자세한 내용은 다음 정보를 참조하세요.

- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#) (장애 시나리오 및 아키텍처 패턴 포함)
- AWS 설명서: [Amazon Builders' Library: 가용 영역을 사용한 정적 안정성](#)
- AWS 설명서: [여러 데이터 센터 고가용 네트워크 연결](#)
- SAP 설명서: [SAP HANA 시스템 아키텍처 개요](#)

모범 사례 10.1 - 비즈니스 요구 사항에 부합하는 SAP 워크로드 가용성 목표에 합의

가용성 목표에 대한 이해는 조직에 중요한 요소에 집중하기 위한 첫 번째 단계입니다. 그러면 아키텍처 패턴을 평가하는 데 사용할 수 있는 기준을 정의하는 데 도움이 됩니다.

제안 사항 10.1.1 – SAP 애플리케이션 범위 및 상호 종속성을 식별

AWS에서 배포한 또는 배포할 SAP 애플리케이션을 식별합니다. 위치에 관계없이 이러한 애플리케이션의 종속성을 이해합니다.

제안 사항 10.1.2 – 장애 영향을 기반으로 시스템을 분류

계획된 가용성 및 장애 위험에 따른 시스템 분류를 위한 공개 표준은 없습니다. 미션 크리티컬 또는 매우 중요과 같은 용어를 사용하여 시스템을 정의하면 패턴 정의, 애플리케이션 그룹화 식별 및 비용 정당화에 도움이 될 수 있습니다. 프로덕션 애플리케이션은 중단으로 인한 영향이 서로 다를 수 있습니다. 고려해야 할 요소는 다음과 같습니다.

- 수익 창출 또는 수익 보고
- 대외 또는 대내
- 핵심 비즈니스 vs 기술 지원
- 다른 시스템과 밀접함 vs 소결함

비프로덕션 환경도 비즈니스를 간접적으로 지원하는 데 중요한 역할을 할 수 있습니다. 이들 역시 전송 경로(예: 일반 비즈니스 및 프로젝트)와 지원 역할(예: 개발, 단위 테스트, 프로덕션 복사본 및 교육)을 고려하여 프로젝트 단계 및 규모에 따라 분류해야 합니다.

제안 사항 10.1.3 - 중단으로 인한 비즈니스 영향을 평가

영향은 측정 가능하고 중단 기간을 고려해야 합니다. 영향 영역의 예로는 보건 및 안전, 재정, 법률, 규제 또는 브랜드가 있습니다.

제안 사항 10.1.4 - 규정 준수 및 규제 요구 사항을 이해

비즈니스 연속성을 보장하는 데 도움이 되도록 데이터 상주 및 위치 간 거리에 대한 규정 준수 또는 규정 요구 사항을 이해합니다.

제안 사항 10.1.5 - 허용 가능한 최소 가동 시간(%)을 정의

각 시스템 또는 시스템 그룹에 대해 비즈니스 요구 사항에 부합하는 허용 가능한 가용성 비율을 합의하고 문서화합니다. 이 맥락에서 다음 용어가 사용됩니다.

- MTTR - 평균 복구 시간
- RTO - 복구 시간 목표
- RPO - 복구 시점 목표

용어에 대한 전체 설명은 Well-Architected Framework [안정성]: [가용성](#) 에서 찾을 수 있습니다. SAP의 안정성에 대한 추가 정보는 다음 백서에 나와 있습니다.

- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#)

모범 사례 10.2 - 가용성 및 용량 요구 사항에 적합한 아키텍처 선택

SAP on AWS를 배포하는 대부분의 고객의 요구 사항에 적합한 SAP 가용성에 대한 표준 아키텍처 패턴이 있습니다. 다음 제안 사항을 사용하여 가용성 및 용량 요구 사항을 최상으로 충족하는 패턴을 결정합니다. 비즈니스 요구 사항에 대해 각 장애 시나리오의 위험 및 영향을 평가합니다.

SAP의 가용성에 대한 추가 정보는 다음 백서에 나와 있습니다. [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#).

제안 사항 10.2.1 – SAP 시스템에 필요한 모든 구성 요소 및 AWS 서비스를 식별

핵심(데이터베이스, 애플리케이션 서버, 중앙 서비스, 글로벌 파일 시스템)에서 시작하여 선택적 구성 요소(예: 웹 디스패처, SAProuter, 클라우드 커넥터)로 확장되는 SAP 시스템의 모든 필수 기술 구성 요소를 식별합니다. 이러한 구성 요소를 지원하는 데 필요한 AWS 서비스를 결정합니다.

제안 사항 10.2.2 – SLA, 내구성, 가용성 및 기록 데이터를 장애 발생 가능성에 대한 가이드로 사용

장애 발생 가능성은 주관적입니다. 게시된 서비스 수준 계약(SLA) 및 과거 성능은 향후 장애 발생 위험을 안내하는 데만 사용할 수 있습니다. 그러나 다양한 시나리오의 가정된 빈도는 여전히 유용한 데이터

포인트입니다. 통계적으로 1년에 한 번 발생할 가능성이 있는 장애가 아직 발생한 적이 없는 장애보다 설계 결정에 더 큰 영향을 미칠 수 있습니다.

다음 정보를 사용하여 서비스를 더 잘 이해할 수 있습니다.

- [AWS Personal Health Dashboard](#) 는 AWS에 영향을 줄 수 있는 이벤트가 발생할 경우 이를 알리고 수정 지침을 제공합니다.
- [AWS 이벤트 사후 요약](#) 은 AWS 서비스 가용성에 영향을 미치는 모든 주요 서비스 이벤트에 대해 제공됩니다.
- [Amazon 컴퓨팅 서비스 수준 계약](#) 에는 컴퓨팅 서비스에 대한 SLA가 나열되어 있습니다.
- AWS 설명서: [Amazon EBS 내구성 및 가용성](#)
- AWS 설명서: [Amazon EFS 데이터 보호 및 가용성](#)
- AWS 설명서: [AWS Direct Connect 복원력 권장 사항](#)

도메인 이름 서비스, 로드 밸런서, 서버리스 기능 등 다른 지원 서비스의 장애 가능성도 평가해야 합니다.

자세한 내용은 [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\) 백서](#) 에서 확인할 수 있습니다.

제안 사항 10.2.3 – 클러스터링, 복원력 및 로드 밸런싱에 대한 옵션을 평가

SAP 시스템은 가용성을 보장하기 위해 여러 메커니즘을 사용하여 여러 호스트에 분산할 수 있습니다. 예를 들어 클러스터링 솔루션을 사용하여 단일 장애 지점(예: SAP 데이터베이스 및 SAP 중앙 서비스)을 보호할 수 있습니다. SAP 애플리케이션 계층은 수평으로 크기를 조정할 수 있으며 로드 밸런싱을 사용하여 웹 디스패처를 고가용성으로 만들 수 있습니다.

- AWS 설명서: [Windows용 SAP NetWeaver 배포 및 운영 가이드 - 고가용성 시스템 배포](#)
- AWS 설명서: [SAP on AWS – 페이스메이커를 사용한 IBM Db2 HADR](#)
- AWS 설명서: [고가용성을 위한 SQL Server 배포](#)
- SAP 설명서: [High Availability Partners](#)

제안 사항 10.2.4 - 가용 영역 내에서 EC2 인스턴스 패밀리의 가용성을 결정

일부 Amazon EC2 인스턴스 패밀리(예: X 및 U)는 일부 AZ에서 사용할 수 없습니다. AWS 계정 팀 또는 AWS Support에 문의하여 사용하려는 EC2 인스턴스 패밀리가 의도한 가용 영역에서 사용 가능한

지 확인하세요. 논리적 AZ 식별자는 계정마다 다를 수 있습니다. 자세한 내용은 AWS 설명서를 참조하세요.

- AWS 설명서: [AWS 리소스의 AZ ID](#)

제안 사항 10.2.5 – 용량을 보장하기 위한 전략을 조사

용량을 보장할 수 있는 최선의 방법은 장애 발생 시 유사한 크기의 인스턴스를 사용할 수 있도록 하는 것입니다. 다른 전략으로는 클라우드 네이티브 옵션(예: 온디맨드 인스턴스, EC2 인스턴스 복구) 또는 공유 용량 재할당이 있습니다.

최소 2개의 AZ에서 SAP 단일 장애 지점을 지원하는 Amazon EC2 인스턴스의 용량을 약정하여 필요할 때 용량을 사용할 수 있도록 하는 것이 좋습니다.

EC2 용량은 [영역 단위 예약 인스턴스](#) 또는 [온디맨드 용량 예약](#) 을 사용하여 예약할 수 있습니다. 영역 단위 예약 인스턴스와 온디맨드 용량 예약은 모두 동일한 AWS 조직의 AWS 계정 간에 공유할 수 있으므로 심각한 장애(예: 전체 AZ 장애)가 발생한 경우 다른 환경의 희생 용량을 사용하는 접근 방식이 가능합니다.

용량 예약에 대한 추가 지침은 다음에서 확인할 수 있습니다.

- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#)

제안 사항 10.2.6 – 여러 가용 영역에 걸쳐 VPC를 설계

초기 설계가 1~2개의 AZ만 사용하는 경우에도 여러 가용 영역에서 인스턴스를 프로비저닝할 수 있도록 VPC와 서브넷을 설계합니다. 그러면 설계에 복원력이 확보되고 서비스에 대한 연결 및 액세스를 사전에 확인하는 데 도움이 됩니다.

모범 사례 10.3 - 중요 SAP 데이터의 가용성을 보장할 수 있도록 접근 방식 정의

SAP 애플리케이션의 비즈니스 데이터는 주로 데이터베이스에 저장되지만 바이너리(예: 실행 파일, 라이브러리, 스크립트), 구성 및 인터페이스에 대한 파일 기반 데이터도 포함될 수 있습니다. 선택한 접근 방식은 내구성, 일관성 및 복구 옵션이 데이터 중요도 및 허용 가능한 데이터 손실(RPO) 수준에 부합하는지 검토해야 합니다.

제안 사항 10.3.1 – MTTR 요구 사항을 평가하고 그 충족 방법을 식별

[안정성] [제안 사항 10.1.5 - 허용 가능한 최소 가동 시간\(%\)을 정의](#) 에서 각 애플리케이션의 MTTR 요구 사항을 정의합니다. 장애 위험과 시스템 가용성을 보호하기 위한 메커니즘을 평가한 후에는 요구 사항

항이 충족될 수 있는지 확인하고 각 장애 시나리오에 대한 MTTR 기대치를 문서화합니다. 비용, 복잡성 또는 일관성에 대한 절충이 필요한 경우 비즈니스 소유자와 상의하여 합의를 도출합니다.

제안 사항 10.3.2 – 백업으로부터 복구가 필요한 장애 시나리오를 결정

백업은 가용성을 보장 또는 복구하기 위한 보조 메커니즘인 경우가 많지만 대부분의 아키텍처는 어느 정도 백업에 의존합니다. 다음은 분석을 안내하는 데 사용할 수 있는 장애 시나리오의 예입니다. 시나리오 세분 수준, 분류 및 영향은 요구 사항 및 아키텍처에 따라 달라집니다.

	상대적 발생 위험	백업 필요	데이터 손실 가능성	예상 복구 시간
계획/제어된 유지 관리	계획			
리소스 고갈 또는 손상(높은 CPU 사용률/파일 시스템 가득 참/메모리 부족/스토리지 문제)	보통			
분산형 무상태 구성 요소 장애(예: 웹 디스패처)	보통			
분산형 상태 유지 구성 요소 장애(예: 애플리케이션 서버)	보통			
단일 장애 지점(데이터베이스/SAP 중앙 서비스)	보통			
AZ/네트워크 장애	낮음			
핵심 서비스 장애(DNS/Amazon EFS/API 호출)	낮음/보통			
손상/우발적 삭제/악의적 활동/잘못된 코드 배포	낮음			
리전 장애	매우 낮음			

제안 사항 10.3.3 – 데이터 복제가 필요한 영역을 결정

데이터 복제는 동일한 데이터의 복사본을 여러 위치에 배치하여 안정성을 개선하는 데 사용되며 RPO가 낮은 시스템의 요구 사항인 경우가 많습니다. 가용성 또는 복구를 위해 복제가 필요한지 여부를 결정할 때 서비스가 영역 단위(예: Amazon EC2 및 Amazon EBS 및 해당 서비스가 지원하는 데이터베이스) 또는 리전 단위(예: 공유 스토리지 및 Amazon S3)인지 고려합니다.

데이터베이스	복제 기술	Guidance
SAP HANA	HANA System Replication	SAP 설명서: HANA System Replication
SAP ASE	SAP Replication Server	SAP 설명서: SAP Replication Server
Oracle	Oracle Data Guard	SAP Note: 105047 - SAP 환경에서 Oracle 기능 지원 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SQL Server Always ON	<ul style="list-style-type: none"> SAP 설명서: SQL Server AlwaysOn으로 데이터베이스 고가용성 AWS 설명서: 고가용성을 위한 SQL Server 배포
SAP MaxDB	MaxDb Standby Database	SAP Note: 952783 - FAQ: SAP MaxDB 고가용성 [SAP 포털 액세스 권한 필요]
IBM Db2	HADR	SAP Note: 1612105 - DB6: FAQ on Db2 High Availability Disaster Recovery(HADR) [SAP 포털 액세스 권한 필요]

[AWS DataSync](#) 는 필요한 경우 리전 간에 [Amazon EFS](#) 및 [Amazon FSx](#) 를 모두 보호하는 데 사용할 수 있습니다.

[CloudEndure Disaster Recovery](#) 는 AWS 계정 간을 포함하여 가용 영역 또는 리전 간에 인스턴스 수준에서 지속적으로 복제합니다.

Amazon S3 복제

백업 및 기타 객체 스토리지는 Amazon S3에 저장할 수 있으며 [Amazon S3 복제](#) 를 사용하여 복제할 수 있습니다.

제안 사항 10.3.4 – 구성 데이터 및 바이너리의 일관성을 보장하는 전략을 수립

장애 발생 후 예측 가능한 동작과 테스트된 설정을 보장하기 위해 구성 데이터 및 바이너리의 일관성을 유지하는 것이 중요합니다. 여기에는 운영 체제 패키지, 애플리케이션 파라미터, 클러스터 구성이 포함될 수 있습니다. 복원력을 위해 존재하는 인스턴스(예: 추가 애플리케이션 서버, 세컨더리 데이터베이스 노드)를 포함하여 애플리케이션의 모든 인스턴스에서 일관성을 보장할 수 있는 방법을 결정합니다.

Amazon EFS, Amazon FSx 및 Amazon S3는 중앙에서 관리할 수 있는 구성 또는 공유 바이너리에 대한 고내구성 위치를 제공합니다.

버전 제어 및 구성 관리를 위한 메커니즘은 [운영 우수성] 원칙의 [모범 사례 2.1 - 버전 관리 및 구성 관리 사용](#) 을 참조하세요.

제안 사항 10.3.5 – 데이터 일관성에 대한 전체적 접근 방식을 채택

중요한 SAP 데이터의 일관성을 보장하는 접근 방식은 단일 데이터 집합에 초점을 맞출 뿐만 아니라 데이터 집합과 시스템 간의 종속성도 고려해야 합니다. 예를 들어 SAP BW 시스템을 복구해야 하지만 이 시스템이 데이터를 가져오는 소스 시스템은 복구할 필요가 없는 경우 변경 포인트에 미치는 영향은 무엇이며 일관된 복구를 보장하기 위한 메커니즘은 무엇입니까?

제안 사항 10.3.6 – 데이터를 재생 또는 재전송할 수 있는 인터페이스에 대한 전략을 수립

시스템 간 데이터 교환의 경우 통합이 소결합 방식인지 여부와 데이터를 소스 또는 대상에서 재생하거나 재전송할 수 있는지 여부를 결정합니다. 중단 중에 시나리오를 일시 중단하거나 캐시할 수 있도록 대기열 기능이 있는지 검토합니다.

제안 사항 10.3.7 – 데이터 벅커 사용을 평가

우발적 삭제 또는 악의적 행위와 같은 상황으로 인해 온라인 데이터가 불안정해지거나 사용할 수 없게 되는 장애 시나리오에는 데이터 보호 또는 복구를 보장하는 데 도움이 되는 다른 접근 방식이 필요할 수 있습니다.

네트워크 격리, 액세스 제어 등의 보안 프레임워크를 통한 예방이 최선의 방어이지만 복구 및 복원력 측면에서 영향을 고려해야 합니다.

보존 기간이 단축된 쓰기 전용 백업 계정을 사용하는 것은 드물지만 잠재적 영향이 큰 시나리오에 대한 일반적인 접근 방식입니다.

- SAP Lens [보안]: [모범 사례 8.3 - 데이터 복구 메커니즘을 위협으로부터 보호](#)

모범 사례 10.4 - 비즈니스 요구 사항에 기반한 일련의 기준에 따라 설계 검증

비즈니스 요구 사항에 따라 장애 위험, 비즈니스에 미치는 영향, 허용 가능한 절충을 균형 있게 고려하여 일련의 기준을 설정합니다. 이러한 기준을 사용하여 설계를 검증하고 필요에 따라 조정합니다.

제안 사항 10.4.1 - 중단이 비즈니스에 초래하는 비용을 평가

AWS 서비스 또는 SAP 구성 요소의 장애는 복원력 및 복구 전략에 따라 SAP 시스템에 다르게 영향을 미칩니다. 장애 유형에 따라 중단 기간(RTO) 및 잠재적 데이터 손실(RPO)이 결정됩니다.

각 장애에 대해 중단 위험과 비즈니스 비용을 평가하세요. 예를 들어 영향을 받을 수익 창출 프로세스가 있습니까? 시스템 사용 중단과 관련된 시간당 비용은 얼마입니까?

제안 사항 10.4.2 - 아키텍처 비용을 평가

SAP 환경에서 AWS 월별 청구서의 최대 요소는 일반적으로 Amazon EC2 및 스토리지 관련 서비스입니다. 안정성 요구 사항을 충족하는 최상의 아키텍처를 선택할 수 있도록 비용 영향을 이해합니다. 주요 비용 요소는 다음과 같습니다.

- 하드웨어 사용률이 극대화되지 않은 배포 패턴
- 이중화된 데이터 복제
- 운영 체제 라이선스 비용
- 클러스터링 소프트웨어 라이선스 비용
- 유지 관리, 테스트 및 숙련된 리소스와 관련된 비용

자세한 내용은 [비용 최적화]: [비용 최적화 모범 사례](#) 를 참조하세요.

제안 사항 10.4.3 - 프레임워크의 다른 원칙에 대해 설계를 평가

안정성은 단독으로 설계할 수 없고 AWS Well-Architected Framework의 나머지 원칙에 대해 평가해야 합니다. 이를 평가하기 위해 다음과 같은 질문을 할 수 있습니다.

- 운영 우수성 - 솔루션을 관리할 수 있는 경험과 기술이 있습니까?
- 보안 - 복제, 복구 등의 과정에서 데이터가 보호되고 있습니까?
- 성능 - 복제 또는 백업 작업이 사용자 성능에 영향을 줍니까?
- 비용 최적화 - 솔루션 비용이 가정된 위험과 일치합니까?

11 - 장애 탐지 및 대응

SAP 워크로드에 영향을 미치는 장애를 어떻게 탐지하고 대응합니까? SAP 워크로드의 상태 및 복원력을 보장할 수 있는 소프트웨어 또는 운영 절차를 설계합니다. 가능한 경우 예방에 초점을 맞춰 잠재적 장애 및 실제 장애를 모니터링합니다. 구성 요소가 분산되어 있는지 아니면 단일 장애 지점인지 고려하고 워크로드에 대한 영향을 최소화하는 복원성 솔루션을 설계합니다. 위험 프로필을 이해하기 위해 주기적으로 테스트하는 것 외에 복원력을 향상할 수 있는 자동화를 검토합니다.

ID	우선순위	모범 사례
□ BP 11.1	필수	SAP 애플리케이션, AWS 리소스 및 연결 장애를 모니터링
□ BP 11.2	적극 권장	가용성 유지를 위한 접근 방식 정의
□ BP 11.3	적극 권장	서비스 가용성 복원을 위한 접근 방식 정의
□ BP 11.4	적극 권장	주기적으로 복원력 테스트 수행
□ BP 11.5	권장	장애 대응을 자동화

자세한 내용은 다음을 참조하세요.

- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#) (장애 시나리오 및 아키텍처 패턴 포함)

모범 사례 11.1 - SAP 애플리케이션, AWS 리소스 및 연결 장애를 모니터링

SAP 애플리케이션, AWS 리소스 및 연결의 장애를 모니터링하면 실제 장애 또는 잠재적 장애에 적시에 대응할 수 있습니다.

제안 사항 11.1.1 – AWS Personal Health Dashboard 및 알림을 사용

[AWS Personal Health Dashboard](#) 는 애플리케이션을 구동하는 AWS 서비스의 상태에 대한 개인화된 보기를 제공하여 SAP 워크로드에 영향을 미치는 문제가 발생할 때 신속하게 확인할 수 있도록 합니다.

예를 들어 [Amazon Elastic Block Store\(Amazon EBS\)](#) 볼륨이 [Amazon EC2](#) 인스턴스 중 하나에 연결된 상태에서 손실되는 경우입니다.

이 대시보드는 또한 미래 지향적인 알림을 제공하며 이메일을 비롯한 여러 채널에서 경고를 설정할 수 있으므로 변경 일정을 계획하는 데 도움이 되는 시기적절하고 관련성 있는 정보를 받을 수 있습니다. 예를 들어 AWS 하드웨어 유지 관리 작업이 [Amazon EC2](#) 인스턴스 중 하나에 영향을 미치는 경우 변경을 계획하고 예정된 변경과 관련된 문제를 사전에 해결하는 데 도움이 되는 정보가 포함된 알림을 받게 됩니다.

제안 사항 11.1.2 – SAP 시스템의 상태를 이해하기 위한 AWS 서비스를 평가

AWS는 다수의 [관리 및 거버넌스](#) 서비스를 제공하므로 이를 평가해야 합니다. EC2 인스턴스 장애, 높은 CPU 사용률, 파일 시스템 사용률과 같은 실제 장애 또는 잠재적 장애를 나타내는 지표에 초점을 맞춥니다.

자세한 내용은 운영 우수성 원칙을 참조하세요.

- SAP Lens [운영 우수성]: [모범 사례 1.1 - SAP on AWS 모니터링을 위한 사전 조건 구현](#)
- SAP Lens [운영 우수성]: [모범 사례 1.4 - 워크로드 구성 모니터링 구현](#)

제안 사항 11.1.3 – 장애를 모니터링하는 SAP 도구의 기능을 평가

Solution Manager, Landscape Manager 같은 SAP 도구를 사용하면 애플리케이션 컨텍스트에서 모니터링 데이터를 확인할 수 있습니다. SAP에서 다음과 같은 모니터링 솔루션을 사용할 수 있습니다. 이러한 도구를 평가할 때 추가 라이선싱 비용을 검토합니다.

- SAP 설명서: [SAP Focused run](#)
- SAP 설명서: [SAP Solution Manager](#)
- SAP 설명서: [SAP Landscape Manager\(LaMa\)](#)
- SAP Note: [2574820 - Amazon Web Services\(AWS\)용 SAP Landscape Management Cloud Manager](#) [SAP 포털 액세스 권한 필요]

제안 사항 11.1.4 – AWS 및 SAP 모니터링을 위한 서드 파티 도구를 평가

AWS Marketplace에서 다음과 같은 모니터링 솔루션을 사용할 수 있습니다. 이러한 도구를 포함하여 서드 파티 도구를 평가해야 합니다.

- AWS 설명서: [AWS Marketplace의 모니터링 솔루션](#)

모범 사례 11.2 - 가용성 유지를 위한 접근 방식 정의

단일 기술 구성 요소 또는 AWS 서비스의 장애를 견딜 수 있는 복원력 있는 아키텍처를 통해 가용성을 유지합니다. 이러한 메커니즘에는 이중화된 용량, 로드 밸런싱, 소프트웨어 클러스터가 포함될 수 있습니다.

제안 사항 11.2.1 - 리소스 고갈 또는 서비스 품질 저하로 인한 장애를 방지

리소스 초과 프로비저닝, 증가에 대한 사전 모니터링 및 한도 설정을 통한 사용량 제한을 조사합니다.

운영 우수성 원칙은 SAP 애플리케이션의 상태를 이해하고 적절한 조치를 취할 수 있도록 하는 다양한 방법을 다룹니다. [운영 우수성] [1 - 상태를 이해하고 대응할 수 있도록 SAP 워크로드를 설계](#) 를 참조하세요.

성능 원칙은 용량을 적절한 규모로 설정하고 크기 조정하는 데 도움이 될 수 있습니다. [성능]: [16 - 지속적인 성능 및 최적화 옵션 이해](#) .

제안 사항 11.2.2 - 유지 관리 일정을 위한 전략을 수립

비즈니스에 예정된 중단을 최소화해야 하는 요구 사항이 있는 경우 SAP 애플리케이션, 데이터베이스, 운영 체제, AWS 등 모든 수준에서 유지 관리 전략을 개발해야 합니다. 다음 사항을 고려하세요.

- 프라이머리 노드와 세컨더리 노드를 교대로 사용하는 복제 및 클러스터 솔루션을 사용.
- 단계적 중단이 용이하게 확장 및 축소할 수 있는 초과 용량 및 메커니즘.
- 가능한 경우 운영 체제에 대한 라이브 패치 적용 접근 방식을 사용.
 - [SUSE Linux Enterprise Live Patching](#)
 - [Red Hat Reducing downtime for SAP HANA\(SAP HANA 가동 중지 시간 감소\) 백서](#)
- AWS 설명서: [AWS Systems Manager 패치 관리자 패치 그룹](#)
- SAP Note: [1913302 - HANA: 짧은 유지 관리 작업을 위해 DB 연결 일시 중단](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2077934 - HA 환경의 Rolling Kernel Switch](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [953653 - Rolling Kernel Switch](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2254173 - Linux: Pacemaker 기반 NetWeaver HA 환경의 Rolling Kernel Switch](#) [SAP 포털 액세스 권한 필요]

또한 일시적으로 성능을 향상시켜 예정된 유지 관리의 전체 가동 중지 시간을 단축할 수 있도록 AWS 서비스의 탄력적 기능을 평가해야 합니다. 예를 들어, 데이터베이스가 실행되는 Amazon EC2 인스턴

스의 크기를 확장하여 업그레이드 작업에 더 많은 CPU 및 스토리지 처리량을 제공하거나 EBS 볼륨 유형을 gp2에서 io2로 전환하여 데이터베이스 재구성 중에 스토리지 처리량을 개선합니다.

제안 사항 11.2.3 – 소프트웨어 클러스터 또는 기타 메커니즘으로 SAP 단일 장애 지점을 보호

가용 영역 간에 SAP 단일 장애 지점(SAP 중앙 서비스 및 데이터베이스) 자동 장애 조치를 위해 고가용성(HA) 클러스터링 솔루션을 사용할 수 있습니다.

여러 SAP 인증 클러스터링 솔루션이 [SAP 웹 사이트](#)에 나열되어 있습니다. SAP 클러스터링 솔루션은 SAP가 아닌 클러스터 소프트웨어 공급 업체에서 직접 지원합니다. SAP는 솔루션을 인증만 합니다. 맞춤형 솔루션은 인증되지 않으며 솔루션 빌더가 지원해야 합니다.

단일 장애 지점에 클러스터링 솔루션을 사용하지 않기로 한 경우 서비스 복원과 관련된 오류를 최소화하기 위해 스크립팅 또는 런북을 고려합니다.

제안 사항 11.2.4 – 지원되는 구성 요소에 대한 이중화된 용량 또는 자동 크기 조정

정적, 동적 또는 예약된 용량 변경이 사용량과 일치하는지 평가합니다. 최소 용량 요구 사항과 장애 및 유지 관리가 해당 요구 사항에 미치는 영향을 검토합니다. 적절한 경우 장애 복구 시간을 확보할 수 있도록 오버 프로비저닝합니다.

AZ 장애 발생 시에도 100% 용량을 유지해야 하는 경우 3개의 AZ에 걸쳐 애플리케이션 계층을 배포하는 것을 고려해야 합니다. 이때 각 AZ는 필요한 총 용량의 50%를 가져야 합니다.

여러 AZ에 SAP 애플리케이션 서버 계층을 배포하는 것 외에도 다음 SAP on AWS 블로그 게시물에 설명된 것과 같이 [Amazon EC2 Auto Scaling](#)의 기능을 활용하는 크기 조정 솔루션을 고려할 수 있습니다.

- SAP on AWS 블로그: [AWS를 사용하여 SAP Application Auto Scaling 활성화](#)
- AWS 설명서: [SAP용 Amazon EC2 인스턴스 유형](#)
- SAP Note: [1656099 - AWS의 SAP 애플리케이션: DB/OS 및 Amazon EC2 제품 지원](#) [SAP 포털 액세스 권한 필요]

제안 사항 11.2.5 – 모든 식별된 장애 시나리오에서 용량 가용성을 보장

다음은 분석을 안내하는 데 사용할 수 있는 장애 시나리오의 예입니다. 시나리오의 세분 수준 및 적용 범위, 분류, 영향은 요구 사항 및 아키텍처에 따라 달라집니다.

장애 시나리오 예	상대적 발생 위험
계획/제어된 유지 관리	계획
리소스 고갈 또는 손상(높은 CPU 사용률/파일 시스템 가득 참/메모리 부족/스토리지 문제)	보통
분산형 무상태 구성 요소 장애(예: 웹 디스패처)	보통
분산형 상태 유지 구성 요소 장애(예: 애플리케이션 서버)	보통
단일 장애 지점(데이터베이스/SAP 중앙 서비스)	보통
AZ/네트워크 장애	낮음
핵심 서비스 장애(DNS/Amazon EFS/API 호출)	낮음/보통
손상/우발적 삭제/악의적 활동/잘못된 코드 배포	낮음
리전 장애	매우 낮음

용량 예약에 대한 추가 지침은 다음에서 확인할 수 있습니다. [안정성]: [제안 사항 10.2.5 – 용량을 보장하기 위한 전략을 조사](#) 및 AWS 백서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#).

AWS 계정 내에서 사용 가능한 예약 인스턴스는 [AWS Cost Explorer RI 보고서](#) 를 사용하여 검토할 수 있습니다.

제안 사항 11.2.6 – 적용 가능한 경우 가용성이 내재된 AWS 서비스를 사용

여러 AWS 서비스는 설계에 가용성이 포함되며 고가용성을 위해 여러 가용 영역에서 실행됩니다. SAP 컨텍스트에서 사용되는 관련 서비스에는 다음이 포함됩니다.

- AWS 서비스: [Amazon EFS](#)
- AWS 서비스: [Elastic Load Balancing](#)
- AWS 서비스: [Route 53](#)
- AWS 서비스: [AWS Transit Gateway](#)
- AWS 서비스: [Amazon S3](#)

또한 배스천 호스트 또는 SAPRouter와 같은 무상태 서비스를 사용하는 구성 요소는 Auto Scaling 그룹을 사용하여 고가용성을 달성할 수 있습니다.

제안 사항 11.2.7 – 네트워크 연결을 보장하기 위한 AWS 모범 사례를 준수

사용 중인 AWS 리전에 대한 네트워크 연결의 복원력을 보장하기 위해 다음 AWS 모범 사례 중 하나 이상을 평가합니다.

- AWS 설명서: [AWS Direct Connect 복원 도구 키트](#)
- AWS 설명서: [AWS VPN CloudHub](#)

클러스터 솔루션이 오버레이 IP를 사용하는 경우 VPC 외부로부터 액세스를 활성화하려면 다음을 고려합니다.

- AWS 설명서: [오버레이 IP 주소 라우팅을 사용한 SAP on AWS 고가용성](#)

모범 사례 11.3 - 서비스 가용성 복원을 위한 접근 방식 정의

가용성 복원은 특정 장애 시나리오의 경우 일부 서비스 손실이 발생한다고 가정합니다. 복원 접근 방식에서는 서비스를 복원하는 데 필요한 시간과 가용성 목표를 달성하는 데 필요한 조치를 검토해야 합니다.

제안 사항 11.3.1 – EC2 인스턴스에 인스턴스 복구를 사용

Amazon EC2 인스턴스를 모니터링하고, 기반 하드웨어의 장애로 인해 인스턴스가 손상된 경우 인스턴스를 자동으로 복구하는 Amazon CloudWatch 경보를 생성할 수 있습니다. 이 조치는 수동 개입 필요성을 제거할 수 있지만 시작, 애플리케이션 재시작 및 로드 시간을 복구 시간 목표(RTO)에 포함해야 합니다. 하드웨어 장애로부터 보호하기 위해 클러스터링 솔루션을 사용하려는 경우 인스턴스 복구가 클러스터 솔루션과 호환되는지 평가해야 합니다.

- AWS 설명서: [Amazon EC2 인스턴스 복구](#)

제안 사항 11.3.2 – AMI 및 코드형 인프라를 사용하여 EC2 인스턴스를 다시 빌드하는 전략을 수립

코드형 인프라(IaC)의 이점은 전체 환경을 프로그래밍 방식으로 구축하고 폐기할 수 있다는 것입니다. 복원력을 위해 설계된 경우 [AWS CloudFormation](#) 템플릿 또는 [AWS Systems Manager Automation](#) 을 사용하여 몇 분 안에 환경을 구현할 수 있습니다. 자동화는 고가용성과 빠른 복구를 유지하는 데 중요합니다.

전략의 일부로 다음 AWS 서비스를 평가해야 합니다.

- AWS 서비스: [EC2 Image Builder](#)
- AWS 서비스: [AWS Launch Wizard for SAP](#)
- AWS 서비스: [AWS Cloud Development Kit](#)
- SAP on AWS 블로그: [SAP용 DevOps](#)

제안 사항 11.3.3 – Amazon EBS 장애를 이해

하나 이상의 EBS 볼륨에 장애가 발생할 경우 SAP 워크로드의 가용성 및 내구성에 영향을 줄 수 있습니다. 따라서 Amazon EBS 장애 비율, 알림 메커니즘 및 복구 옵션을 이해해야 합니다

- AWS 설명서: [Amazon EBS 내구성](#)
- AWS 설명서: [볼륨 상태 모니터링](#)
- AWS 서비스: [AWS Personal Health Dashboard](#)
- AWS 설명서: [Amazon EBS 스냅샷을 사용한 볼륨 복구](#)

제안 사항 11.3.4 – AWS Personal Health Dashboard 알림에 대응하기 위한 전략을 수립

AWS Personal Health Dashboard의 알림을 수신하고 조치를 취하기 위한 전략이 있어야 합니다. 여기에는 CloudWatch를 사용하여 Amazon SNS를 시작, [AWS Health API](#) 를 통한 ITSM 도구 통합 등이 포함될 수 있습니다.

제안 사항 11.3.5 – 가용성에 영향을 미치는 우발적 또는 악의적 이벤트로부터 보호

SAP 워크로드의 가용성에 영향을 줄 수 있는 우발적 또는 악의적 이벤트로부터 보호하려면 다음 접근 방식을 고려해야 합니다.

- 먼저 [최소 권한 원칙](#) 을 구현하고 AWS Identity and Access Management 내에서 업무 분장을 적용합니다.
- AWS 지식 센터 문서: [실수로 인한 EC2 인스턴스 종료로부터 데이터를 보호하려면 어떻게 해야 하나요?의 지침을 따릅니다.](#)
- 다음을 따릅니다. [Amazon EC2 모범 사례](#)
- [보안]: [모범 사례 8.3 - 데이터 복구 메커니즘을 위협으로부터 보호의 지침을 따릅니다.](#)

Suggestion 11.3.6 – AWS에서 SAP 워크로드를 벗어난 종속성을 식별

공유 서비스 및 지원 구성 요소 또는 시스템을 포함하여 SAP 비즈니스 프로세스의 기본 종속성을 이해합니다. 예를 들면 Active Directory, DNS, 자격 증명 공급자, SaaS 서비스, 온프레미스 시스템이 있습니다. 장애의 영향과 필요한 완화를 평가합니다.

모범 사례 11.4 - 주기적으로 복원력 테스트 수행

소프트웨어 및 절차가 예측 가능한 결과를 제공함을 입증하기 위해 중대 장애 시나리오에 대해 주기적으로 복원력을 테스트합니다. 아키텍처, 소프트웨어 또는 지원 담당자에 대한 변경 사항을 평가하여 추가 테스트가 필요한지 여부를 결정합니다.

제안 사항 11.4.1 – 비즈니스 요구 사항을 기반으로 범위 내 중대 장애 시나리오를 정의

비즈니스 요구 사항에 맞춰 테스트할 수 있는 중대 장애 시나리오를 정의해야 합니다. 다음은 분석을 안내하는 데 사용할 수 있는 장애 시나리오의 예입니다. 시나리오의 세분 수준 및 적용 범위, 분류, 영향은 요구 사항 및 아키텍처에 따라 달라집니다.

장애 시나리오 예	상대적 발생 위험
계획/제어된 유지 관리	계획
리소스 고갈 또는 손상(높은 CPU 사용률/파일 시스템 가득 참/메모리 부족/스토리지 문제)	보통
분산형 무상태 구성 요소 장애(예: 웹 디스패처)	보통
분산형 상태 유지 구성 요소 장애(예: 애플리케이션 서버)	보통
단일 장애 지점(데이터베이스/SAP 중앙 서비스)	보통
AZ/네트워크 장애	낮음
핵심 서비스 장애(DNS/Amazon EFS/API 호출)	낮음/보통
손상/우발적 삭제/악의적 활동/잘못된 코드 배포	낮음
리전 장애	매우 낮음

제안 사항 11.4.2 – 중대 장애를 시뮬레이션하기 위한 일련의 테스트 사례를 정의

SAP 워크로드에 영향을 줄 수 있는 중대 장애 시나리오를 시뮬레이션할 수 있도록 전체 세트의 테스트가 정의되어 있어야 합니다.

일부 장애 시나리오의 경우 시뮬레이션이 발생할 수 있는 실제 장애를 완전히 나타내지 않을 수 있음을 인지해야 합니다. 예를 들어 하드웨어 문제를 시뮬레이션하기 위해 EC2 인스턴스에서 장애를 유발할 수는 없지만 Nitro 기반 인스턴스의 경우 커널 패닉을 생성하여 인스턴스를 재부팅시킬 수 있습니다.

또한 [AWS Fault Injection Simulation](#) 은 AWS 리소스에서 장애를 시뮬레이션하는 데 도움이 되도록 설계되었습니다.

- AWS 설명서: [SAP on HANA용 고가용성 구성 가이드](#)
- AWS 설명서: [진단 인터럽트 전송](#)

제안 사항 11.4.3 – 각 테스트 사례의 예상 동작을 정의

테스트의 기준으로 사용할 예상 결과 세트를 문서화해야 합니다.

제안 사항 11.4.4 – 변경의 영향을 평가하기 위한 접근 방식 및 필요한 후속 테스트를 정의

변경이 환경에 미치는 영향을 평가하기 위한 접근 방식과 변경으로 인해 가용성 및 안정성에 대한 접근 방식이 무효화되지 않는지 확인하기 위해 해당 변경의 일부로 필요한 테스트가 정의되어 있어야 합니다. 이러한 변경 유형의 예로는 소프트웨어 업그레이드, 패치, 파라미터 변경이 있습니다.

제안 사항 11.4.5 – 테스트 일정을 정의

초기 구현, 변경 테스트, 주기적 환경 검증을 포함하는 테스트 일정을 수립해야 합니다.

제안 사항 11.4.6 – 테스트 결과를 검토

테스트 결과를 기반으로 테스트 사례, 구성 또는 아키텍처가 개선되었는지 식별합니다.

제안 사항 11.4.7 – 테스트 전 상태로 복귀하는 데 필요한 작업을 정의

각 테스트의 일부로 테스트 전 상태로 돌아가기 위해 필요한 작업을 정의해야 합니다. 이는 각 테스트 사례가 서로 격리되고 테스트가 프로덕션 시스템의 가용성 및 안정성에 영향을 미치지 않도록 하기 위한 것입니다.

모범 사례 11.5 - 장애 대응 자동화

장애 대응을 자동화하여 서비스에 미치는 영향을 최소화할 수 있습니다. 장애, 용량 손상 또는 연결 손실에 대응하도록 자동화를 설계합니다. 오탐을 방지하기 위해 명확한 종재 기준이 정의되어야 합니다.

제안 사항 11.5.1 – 자동화의 손상 위험을 평가

데이터 손상의 위험이 있는 구성 요소의 경우 고가용성(HA) 솔루션이 데이터 복제 방법, 스플릿 브레인 방지, 연결 안정성 및 애플리케이션 인식을 고려해야 합니다.

제안 사항 11.5.2 - 자동화를 시작하는 상태 확인 메커니즘을 평가

상태 확인은 오탐으로 인해 자동화가 시작되지 않도록 제어하도록 설계해야 합니다.

12 - 데이터 복구 계획

SAP 워크로드에 대한 논리적 데이터 관련 복구를 어떻게 계획합니까? 비즈니스 요구 사항에서 거슬러 올라가며 비즈니스 데이터를 복구 또는 재구성하는 접근 방식을 정의합니다. 복원력을 설계한 방법에 따라 이 범주에 다양한 시나리오가 포함될 수 있습니다. 최소한 백업 또는 재해 복구(DR) 태세는 우발적인 삭제, 논리적 데이터 손상 및 맬웨어로부터 사용자를 보호해야 합니다. 서비스 복구 시간과 시스템 간 종속성을 고려하여 신중하게 복원 결정을 내려야 합니다.

ID	우선순위	모범 사례
□ BP 12.1	필수	일관된 비즈니스 데이터 복구를 위한 방법 수립
□ BP 12.2	적극 권장	구성 데이터 복구를 위한 방법 수립
□ BP 12.3	적극 권장	전체 SAP 자산에 대한 복구 접근 방식 정의
□ BP 12.4	권장	주기적 테스트를 수행하여 복구 절차 검증

모범 사례 12.1 - 일관된 비즈니스 데이터 복구를 위한 방법 수립

데이터 손실 또는 손상이 발생한 경우 개별 시스템에 대한 비즈니스 데이터 일관성을 보장하는 데 도움이 되는 데이터 복구 계획을 정의합니다.

제안 사항 12.1.1 - 데이터베이스 상태를 인식하는 백업 메커니즘을 사용하여 데이터베이스 백업 일관성 보장

SAP는 데이터베이스 공급 업체의 백업 기능(예: brtools)과 통합하고 SAP 트랜잭션 또는 관리 콘솔 내에서 가시성을 제공하기 위한 메커니즘을 제공합니다. 또한 [AWS Backint Agent for SAP HANA](#) 를 포함한 서드 파티 백업 공급 또는 스토리지 솔루션과 통합할 수 있는 옵션이 있습니다. 이러한 지원되는

옵션에는 일관된 복사본을 생성하는 동안(예: 스토리지 스냅샷 사용) 데이터베이스 상태를 인식하거나, 지속적으로 변경 사항을 캡처하거나 데이터베이스를 중단(작업 일시 중지 또는 축소)하는 기능이 있습니다.

개별 데이터베이스 공급 업체용 SAP 가이드와 다음 AWS 설명서를 검토하세요.

- AWS 설명서: [AWS Backint Agent for SAP HANA](#)
- SAP 설명서: [SAP NetWeaver 및 ABAP Platform의 Guide Finder](#)
- SAP on AWS 블로그: [VSS 스냅샷을 사용하여 SAP용 Microsoft SQL Server 데이터베이스를 백업하는 방법](#)
- AWS 블로그: [Amazon EC2 인스턴스의 여러 Amazon EBS 볼륨에서 충돌 일치 스냅샷 생성](#)

제안 사항 12.1.2 – 비즈니스에 중요한 파일 기반 데이터의 내구성 및 복구 가능성을 평가

데이터베이스에 저장되지 않은 비즈니스 데이터는 별도의 백업 전략이 필요할 수 있습니다.

표준 SAP NetWeaver 시스템에는 파일 기반 인터페이스 파일, SAP 전송 디렉터리 콘텐츠, 로그(예: 배치 로그, 작업 로그, 작업 프로세스 디렉터리 로그)가 포함되는 경우가 많습니다. 비 SAP NetWeaver 시스템 및 문서 관리 솔루션과 같은 지원 시스템에는 평가해야 하는 다른 파일 기반 비즈니스 데이터가 있을 수 있습니다. [Amazon EFS](#) 또는 [Amazon FSx](#) 를 평가하여 이러한 파일 시스템의 가용성 및 내구성을 개선합니다.

파일 시스템 백업은 스냅샷, AWS Backup 또는 서드 파티 백업 솔루션을 사용하여 수행할 수 있습니다.

비즈니스 데이터는 바이너리 및 구성 데이터와 독립적으로 평가해야 하며, SAP 다운로드, 재설치 또는 코드형 인프라를 통해 다시 프로비저닝할 수 있습니다. 다음을 참조하세요.

- SAP Lens [운영 우수성]: [제안 사항 12.2.1 - 구성 생성 및 변경에 대한 코드형 인프라 접근 방식을 정의](#)
- SAP Lens [운영 우수성]: [제안 사항 12.2.2 - 루트 볼륨 등 파일 시스템 콘텐츠 백업에 대한 접근 방식을 정의](#)

제안 사항 12.1.3 – 데이터베이스 백업 및 로그의 내구성 및 위치를 평가

백업 및 로그에는 라이브 데이터 레코드가 포함되지만 그 자체로는 장애에 취약할 수 있습니다. 활성 데이터 복사본과 관련하여 백업 위치를 평가하여 장애의 영향을 최소화하는 방법을 수립합니다. 다음을 고려하는 것이 중요합니다.

- 백업을 보호하는 데 걸리는 시간 - 복구 지점에 영향
- 백업을 검색/복구하는 데 걸리는 시간 - 복구 시간에 영향

자세한 내용은 다음 설명서에서 찾을 수 있습니다.

- AWS 설명서: [HANA의 AWS Backint Agent](#)
- AWS 설명서: [FSR\(빠른 스냅샷 복원\)](#)
- AWS 설명서: [Amazon S3 복제 옵션](#)

제안 사항 12.1.4 – 특정 시점으로 복구에 대한 요구 사항을 평가

특정 시점으로 복구 요구 사항이 있는 경우 백업 설계에서 이를 허용합니까? 백업 방법이 데이터베이스를 인식하고 데이터베이스를 일관된 복구 지점으로 롤포워드할 수 있습니까? 일관성에 필요한 파일 기반 복구를 고려했습니까?

다음 사항을 고려하세요.

- 로그 간격 및 로그 보호 속도
- 복구 시간을 개선하기 위한 증분 또는 차등 백업
- 백업 카탈로그 또는 기타 메커니즘이 필요한지 여부
- 데이터베이스 또는 스토리지 옵션을 사용하여 과거 시점으로 이동할 수 있는지 여부

제안 사항 12.1.5 – 데이터 손실로 촉발되는 복구 메커니즘을 검토

데이터 손상, 삭제 또는 되돌릴 수 없는 잘못된 코드 배포와 같은 심각한 데이터 손실 상황에서 복구의 영향을 결정합니다. 데이터베이스 또는 스토리지 기반 복제 사용 시 데이터 손실의 전파를 평가하고 백업과 같은 보조 복원 메커니즘 사용 시 RTO 및 RPO 영향을 평가합니다.

제안 사항 12.1.6 – 데이터 벙커를 생성

[제안 사항 10.3.7 – 백업으로부터 복구가 필요한 장애 시나리오를 결정](#)의 지침에 따라 우발적 삭제 또는 악의적 활동으로부터 백업을 보호하기 위해 데이터 벙커를 생성합니다.

모범 사례 12.2 - 구성 데이터 복구를 위한 방법 수립

SAP 워크로드를 실행하는 데 필요한 여러 유형의 데이터는 SAP 데이터베이스에 상주하지 않습니다. 여기에는 운영 체제 구성, 필요한 AWS 리소스를 재생성하기 위한 메타데이터, 파일 시스템에 저장된

는 SAP 애플리케이션에 필요한 데이터가 포함됩니다. 데이터 손실이 발생할 경우 이 데이터를 복구 또는 재생성하는 프로세스를 정의합니다.

제안 사항 12.2.1 - 구성 생성 및 변경에 대한 코드형 인프라 접근 방식을 정의

수동으로 개별 인스턴스를 직접 변경할 경우 빠르게 시스템 간 구성 일관성이 사라져 백업을 사용하여 상태를 복구하게 될 수 있습니다. 코드형 인프라를 사용하면 애플리케이션 코드를 관리하는 것과 동일한 방식으로 SAP 시스템을 배포하고 변경 사항을 구현할 수 있습니다. 코드 파이프라인과 같은 DevOps 메커니즘은 환경 내에서 일관성과 반복성을 보장할 수 있는 추가 제어 및 테스트를 제공할 수 있습니다.

접근 방식에서 다음 AWS 서비스를 평가해야 합니다.

- AWS 서비스: [AWS Launch Wizard for SAP](#)
- AWS 서비스: [EC2 Image Builder](#)
- AWS 서비스: [AWS Cloud Development Kit](#)
- SAP on AWS 블로그: [SAP용 DevOps](#)
- AWS 설명서: [AWS 기반 DevOps 소개](#)

제안 사항 12.2.2 - 루트 볼륨 등 파일 시스템 콘텐츠 백업에 대한 접근 방식을 정의

운영 체제 패키지 및 구성, 애플리케이션 바이너리 및 파일 시스템 콘텐츠는 실행 중인 SAP 시스템에는 필수적이지만 핵심 SAP 데이터베이스 백업의 일부는 아닙니다. Amazon Machine Image(AMI), EBS 볼륨 스냅샷 및 기타 백업 옵션을 포함하여 이 데이터를 보호 및 복원하는 메커니즘을 평가합니다.

AMI, 스냅샷 및 파일 시스템 복사본의 빈도와 일관성은 물론 복구의 세분 수준 및 소요 시간도 고려해야 합니다.

시나리오에 따라 코드형 인프라를 사용하면 복원보다는 재생성에 중점을 두어 비업무용 데이터에 대한 백업 요구 사항을 줄일 수 있습니다.

- SAP 설명서: [필수 파일 시스템 및 디렉터리](#)
- AWS 설명서: [백업 및 복구 솔루션 설계](#)

제안 사항 12.2.3 – 모든 수동 설정을 문서화

데이터베이스에 포함되지 않거나 코드로 배포할 수 있거나 볼륨 백업을 사용하여 복원할 수 있는 수동 작업은 모두 기록하여 최악의 시나리오에서도 SAP 시스템을 재생성할 수 있도록 해야 합니다.

모범 사례 12.3 - 전체 SAP 자산에 대한 복구 접근 방식 정의

SAP 자산이 여러 SAP 시스템으로 구성된 경우 비즈니스 우선 순위에 따라 각 시스템이 복구되는 순서를 정의하는 세부 접근 방식을 수립해야 합니다. 데이터 손실이 시스템 및 비즈니스 운영 전반에서 일관성에 미치는 영향을 평가합니다.

제안 사항 12.3.1 – 복원 우선 순위 및 일관성 보장 계획을 포함하는 비즈니스 연속성 계획을 수립

[안정성]: [제안 사항 10.1.2 – 장애 영향을 기반으로 시스템을 분류](#) 에서 결정된 시스템 분류에 따라 각 SAP 시스템의 복원 우선 순위를 결정하는 비즈니스 연속성 계획(BCP)을 수립합니다. 이 계획은 복원 우선 순위에 대한 시스템 간 일관성 요구 사항 및 멀티 테넌트 데이터베이스 사용의 영향도 고려해야 합니다.

제안 사항 12.3.2 – 공유 서비스에 대한 종속성을 모두 평가

복구 접근 방식을 정의할 때 공유 서비스가 SAP 워크로드를 실행하기 위한 기반(예: DNS, Active Directory)의 일부인지 아니면 복원 자체를 수행하는 데 필요한 기반(예: 백업 도구)의 일부인지 고려합니다. 이러한 종속성과 관련된 위험 및 복원 전제 조건을 평가합니다.

제안 사항 12.3.3 - 재해 발생 시 수행할 런북을 작성

사전 정의된 런북은 재해 발생 시 입증된 일련의 단계를 수행하도록 하여 중요한 작업을 누락할 위험을 줄입니다.

모범 사례 12.4 - 주기적 테스트를 수행하여 복구 절차 검증

소프트웨어 및 절차가 예측 가능한 결과를 제공함을 입증하고 백업 파일의 상태를 검증하기 위해 중대 장애 시나리오로부터 복구를 주기적으로 테스트합니다. 아키텍처, 소프트웨어 또는 지원 담당자에 대한 변경 사항을 평가하여 추가 테스트가 필요한지 여부를 결정해야 합니다.

제안 사항 12.4.1 - 복구 테스트를 위한 장애 시나리오를 식별

[안정성]: [제안 사항 10.3.2 – 백업으로부터 복구가 필요한 장애 시나리오를 결정](#) 을 기반으로 복구가 필요한 장애 시나리오를 정의하고 프로세스 및 도구를 검증하는 데 필요한 적절한 수준의 테스트를 결정해야 합니다.

제안 사항 12.4.2 – 시스템 변경이 복구 접근 방식에 미치는 영향을 결정

변경의 영향을 평가하기 위한 접근 방식을 정의하고 해당 변경으로 인해 접근 방식이 무효화되지 않는지 확인하는 데 필요한 후속 복구 테스트를 정의합니다. 워크로드 복구에 영향을 줄 수 있는 변경 유형의 예로는 소프트웨어 업그레이드, 패치, 파라미터 변경이 있습니다.

관리형 서비스 파트너 또는 핵심 인력의 변경과 같이 SAP 환경을 지원하는 데 사용되는 운영 모델이 크게 변경된 경우에도 복구 테스트를 계획해야 합니다.

제안 사항 12.4.3 – 복구 테스트 계획을 정의

복구가 필요할 수 있는 중대 장애 시나리오를 시뮬레이션할 수 있도록 전체 세트의 테스트가 정의되어 있어야 합니다. 복구 테스트는 초기 구현 중 그리고 구현 이후로 주기적으로 또는 필요할 때마다 계획해야 합니다.

- SAP Lens [운영 우수성]: [모범 사례 4.3 - 정기적으로 비즈니스 연속성 계획 및 장애 복구 테스트](#).

성능 효율성

성능 효율성 원칙에서는 컴퓨팅 리소스를 효율적으로 사용하여 요구 사항을 충족하고 수요 변경 및 기술 변화에 따라 이러한 효율성을 유지하는 데 중점을 둡니다. 성능 최적화는 성능을 모니터링 및 측정하고 변화하는 요구 사항을 충족하도록 컴퓨팅 인프라를 조정하는 데이터 기반 프로세스여야 합니다.

13 – 최적의 컴퓨팅 솔루션 선택

SAP 워크로드에 최적의 컴퓨팅 솔루션을 선택하는 방법은 무엇입니까? SAP 도구 및 기존 워크로드의 지표를 사용하여 성능 요구 사항을 평가하고 추정합니다. 컴퓨팅 요구 사항을 워크로드에 가장 적합한 SAP 지원 인스턴스에 매핑합니다. 인스턴스 유형에 대한 특정 스토리지 또는 네트워크 요구 사항과 선택한 AWS 리전 및 가용 영역에서 필요한 인스턴스 유형의 가용성을 고려합니다.

ID	우선순위	모범 사례
<input type="checkbox"/> BP 13.1	필수	성능 요구 사항 평가 또는 추정
<input type="checkbox"/> BP 13.2	필수	SAP 워크로드에 적합한 EC2 인스턴스 선택
<input type="checkbox"/> BP 13.3	적극 권장	시스템 또는 구성 요소 자동 크기 조정이 가능한 아키텍처 선택
<input type="checkbox"/> BP 13.4	적극 권장	네트워크 성능 및 대기 시간을 고려하여 성능에 유리한 인스턴스 위치 선택

자세한 내용은 다음 정보를 참조하세요.

- AWS 설명서: [SAP용 Amazon EC2 인스턴스 유형](#)
- SAP 설명서: [인증 및 지원되는 SAP HANA Hardware](#)
- SAP Note: [1656099 - AWS의 SAP 애플리케이션: DB/OS 및 Amazon EC2 제품 지원](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [1656250 - SAP on AWS: Support prerequisites\(1656250 - SAP on AWS: 지원 사전 조건\)](#) [SAP 포털 액세스 권한 필요]

모범 사례 13.1 - 성능 요구 사항 평가 또는 추정

기존 SAP 시스템의 용량 및 사용 패턴을 조사하여 향후 하드웨어 요구 사항을 추정할 수 있습니다. SAP는 신규 및 기존 시스템용 하드웨어 크기 조정을 위한 여러 도구를 제공합니다. 크기 조정 추정을 추가로 검증하기 위해 개념 증명(POC) 배포 및 성능 테스트를 사용할 수 있습니다.

제안 사항 13.1.1 - 소스 하드웨어의 SAPS 성능 지표를 참조

SAP 벤치마크 하드웨어는 [SAP 애플리케이션 성능 표준\(SAPS\)](#) 을 사용하며, 이는 SAP 환경에서 시스템 구성의 성능을 설명하는 하드웨어 독립적 측정 단위입니다. 온프레미스 서버 하드웨어에 대한 SAPS 값을 얻으려면 기존 하드웨어 공급 업체 및 SAP 벤치마크 디렉터리에 문의하세요.

SAPS 기반 크기 조정은 기본 용량 요구 사항을 최소한으로 변경하는 마이그레이션(종종 리프트 앤 시프트 마이그레이션이라고 함)에 적합합니다.

제안 사항 13.1.2 - SAP EarlyWatch Alert 보고서 및 모니터링 도구에서 과거 사용량 세부 정보를 참조

[SAP EarlyWatch Alert](#) 보고서는 최대 메모리 및 CPU 사용량 같은 SAP 애플리케이션의 사용률 정보를 제공합니다. 월말 결산 및 대규모 배치 로드와 같은 여러 피크 이벤트에 걸친 이러한 보고서의 전체적 분석은 시스템 사용에 대한 귀중한 인사이트를 제공할 수 있습니다.

EarlyWatch 외에도 인프라 수준 모니터링 도구는 더 세분화된 추가 인사이트를 제공할 수 있습니다.

제안 사항 13.1.3 - SAP HANA 크기 조정 보고서를 사용하여 컴퓨팅 요구 사항을 추정

SAP HANA로 마이그레이션할 때 대상 컴퓨팅의 크기를 추정하는 데 SAP가 제공하는 도구를 사용합니다. 이러한 도구에서 생성된 출력은 SAP HANA 데이터베이스에 대한 하드웨어 크기 조정 요구 사항을 자세히 설명합니다.

- SAP 설명서: [HANA 플랫폼의 SAP HANA Administration 가이드](#)

- AWS 설명서: [SAP HANA 크기 조정](#)
- SAP Note: [1793345 – HANA의 SAP Suite 제품군 크기 조정](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [1872170 – ABAP on HANA sizing report\(S/4HANA, Suite on HANA...\)](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2296290 – SAP BW/4HANA의 새로운 크기 조정 보고서](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [1958910 - HANA 데이터베이스의 EarlyWatch Alert](#) [SAP 포털 액세스 권한 필요]

제안 사항 13.1.4 – 그린필드 구현 및 기능 변경 사항에 SAP Quick Sizer를 사용

SAP Quick Sizer는 신규 SAP 구현의 크기 조정 또는 변경 중인 SAP 구현(예: 사용자 기반 증가, 새로운 기능 또는 모듈)에 사용할 수 있습니다. 이 도구는 애플리케이션의 요구 사항을 하드웨어 사양으로 변환하는 데 도움이 됩니다. 최상의 결과를 얻으려면 기술 팀과 기능 팀이 협력하여 Quick Sizer 도구에 값을 입력해야 합니다.

복잡한 구현의 크기 조정을 검증하려면 SAP 전문가 크기 조정을 사용하는 것이 좋습니다.

SAP 도구 및 서비스에 대한 자세한 내용은 다음을 참조하세요.

- SAP 설명서: [SAP: Sizing Benchmarks](#)

제안 사항 13.1.5 – 크기 조정 정확성을 위해 개념 증명 배포를 사용

AWS 서비스의 유연성을 활용하여 SAP 워크로드를 적절한 규모로 설정하고 비즈니스 요구 사항의 변화에 따라 크기를 조정할 수 있습니다. 개념 증명(POC)을 사용하여 클라우드로의 마이그레이션을 테스트하고 성능 요구 사항을 분석합니다. 이는 비용 및 성능 모두에서 워크로드를 적절한 규모로 설정하는 데 도움이 될 수 있습니다.

모범 사례 13.2 - SAP 워크로드에 적합한 EC2 인스턴스 선택

AWS는 SAP와 협력하여 AWS 서비스가 다양한 인스턴스 유형에서 SAP 소프트웨어를 구현 및 운영하는 데 적합하도록 합니다. 관련 SAP Note 및 설명서의 지침을 사용하여 적합한 인스턴스를 식별합니다. EC2 인스턴스 패밀리는 다양한 CPU 및 메모리 비율은 물론 SAP 워크로드를 실행하는 데 적합한 스토리지 및 네트워크 처리량 특성을 제공합니다. 성능 지표, SAPS 수치 및 컴퓨팅 추정치를 사용하여 요구 사항을 적절한 인스턴스 유형에 매핑합니다. 선택한 리전 및 가용 영역에서 이러한 인스턴스의 가용성을 확인합니다.

제안 사항 13.2.1 – 지원되는 데이터베이스, 운영 체제 및 AWS 서비스에 대한 SAP 지침을 준수

AWS는 SAP 제품을 배포하는 데 사용할 수 있는 서비스를 제공합니다. SAP Note: [1656099 - AWS의 SAP 애플리케이션: DB/OS 및 Amazon EC2 제품 지원](#)에서는 현재 지원되는 SAP 제품, 데이터베이스 및 운영 체제 조합과 Amazon EC2 인스턴스 유형에 대해 설명합니다.

AWS CLI를 사용하여 [인스턴스 유형 제품을 설명](#) 하면 특정 AZ 내 개별 인스턴스 유형의 가용성을 결정할 수 있습니다.

- AWS 설명서: [SAP용 Amazon EC2 인스턴스 유형](#)
- SAP 설명서: [SAP NetWeaver benchmarks](#)

제안 사항 13.2.2 – 하드웨어 지표 및 SAPS를 사용하여 선택을 안내

각 SAP 지원 Amazon EC2 인스턴스 패밀리에는 특정 vCPU/메모리 비율을 제공합니다. 성능 프로필을 이해하려면 요구 사항에 따라 각 인스턴스 패밀리를 평가해야 합니다. 현재 세대의 Amazon EC2 인스턴스([AWS Nitro](#) 기반)는 최고의 성능을 제공하므로 배포 시나리오에서 사용 가능하고 인증된 경우 사용해야 합니다.

SAP 애플리케이션 서버는 범용(m*) 또는 메모리 최적화(r*) 인스턴스를 사용할 수 있습니다. 더 높은 vCPU/메모리 비율 요구 사항이 있는 경우 컴퓨팅 최적화(c*) 인스턴스를 사용하는 것을 고려합니다. AnyDB 데이터베이스 서버의 경우 메모리 최적화(r*) 인스턴스가 필요한 코어 대 메모리 비율에 적합하지만, 특히 배포에 CPU별 라이선싱이 적용되는 경우 추가 분석을 수행하여 크기 조정을 검증해야 합니다. 메모리에서 실행되는 SAP HANA 데이터베이스의 경우 메모리 최적화(r*, x*, u*)가 유일한 옵션입니다.

제안 사항 13.2.3 – SAP HANA 하드웨어 디렉터리 및 메모리 요구 사항을 사용하여 SAP HANA용 EC2 인스턴스를 선택

AWS는 Amazon EC2 인스턴스의 하위 집합에 대해 SAP HANA 워크로드를 실행하기 위한 SAP HANA 인증을 받았습니다. 이러한 인스턴스에 대한 자세한 내용 및 지원되는 IaaS 애플리케이션 유형(OLAP, OLTP, SAP Business One, 스케일 아웃)은 다음을 참조하세요. [인증 및 지원되는 SAP HANA Hardware](#) 및 [SAP용 Amazon EC2 인스턴스 유형](#).

데이터베이스 크기 및 실제 작업 메모리 사용량에 따라 메모리 요구 사항과 인스턴스 선택이 결정됩니다.

비프로덕션 워크로드의 경우 추가 옵션이 존재합니다. 다음 블로그를 참조하세요.

- SAP on AWS 블로그: [SAP HANA 비프로덕션 워크로드를 위한 더 작은 X1e 인스턴스](#)

제안 사항 13.2.4 – EC2 인스턴스의 기능 및 처리량 특성을 인지

Amazon EC2 인스턴스에는 다양한 기능 및 처리량 특성이 있으므로 특히 I/O 및 처리량 요구 사항이 높은 워크로드의 경우 사용 사례를 기반으로 이를 평가해야 합니다. 여기에는 [Elastic Network Adapter\(ENA\)](#) 를 통한 향상된 네트워킹, I/O 성능, Amazon EBS 최적화, 배치 그룹 적합성이 포함됩니다. 전체 기능 목록은 다음을 참조하세요.

- AWS 설명서: [범용 인스턴스](#)
- AWS 설명서: [메모리 최적화 인스턴스](#)
- AWS 설명서: [컴퓨팅 최적화 인스턴스](#)

모범 사례 13.3 – 시스템 또는 구성 요소의 독립적 크기 조정이 가능한 아키텍처 선택

SAP 시스템 및 구성 요소는 제약 없이 크기를 조정할 수 있는 유연성이 있어야 합니다. 이는 할당된 하드웨어 내에서 또는 일부 구성 요소의 수평 크기 조정을 사용하여 달성할 수 있습니다. 이러한 크기 조정이 가능한 아키텍처를 고려하고 관련된 절충을 평가합니다.

제안 사항 13.3.1 – 시스템 간 또는 구성 요소 간 성능 영향을 고려

구성 요소 간에 부정적인 성능 영향을 방지할 수 있도록 개별 시스템 또는 구성 요소를 격리합니다. 더 작은 규모의 여러 인스턴스를 배포하면 인스턴스 재사용, 워크로드 기반 크기 조정 및 온디맨드 용량에 대한 옵션을 사용할 수 있습니다. 비용 때문에 리소스 사용을 최적화하려는 경우에는 예외가 있습니다. 자세한 내용은 비용 원칙을 참조하세요.

제안 사항 13.3.2 – 최대 성능을 위해 용량 유연성을 고려

애플리케이션 서버와 같은 구성 요소의 크기 조정이 가능한 아키텍처를 선택하면 성능 요구 사항에 부합하게 용량을 조정하고 월말 처리 또는 계절성 피크를 포함한 예외적인 수요에 맞게 확장할 수 있습니다.

모범 사례 13.4 - 대기 시간이 최소화되는 리전 및 가용 영역 선택

SAP 인스턴스를 최종 사용자, 중요 인터페이스 및 시스템 내부 트래픽에 영향을 미치는 주요 비즈니스 프로세스의 대기 시간을 최소화하는 리전 및 가용 영역에 배포합니다.

제안 사항 13.4.1 – 성능이 최적화되는 리전 및 클라우드 연결을 선택

SAP 최종 사용자 및 기업 데이터 센터와의 근접성을 기반으로 리전을 선택합니다. 데이터 전송 요구 사항을 수용할 수 있도록 모든 클라우드 연결 옵션(예: Direct Connect 및 VPN)의 크기를 조정합니다.

SAP 성능 도구를 사용하여 사용자 응답 시간 분석(예: 네트워크, GUI, 애플리케이션 및 데이터베이스)을 이해하고 대기 시간 증가로 인한 네트워크 왕복 시간 변화의 영향을 평가합니다. 서로 다른 위치에 있는 시스템 간의 빈도가 높고 대기 시간이 짧은 인터페이스에 중점을 두는 것이 좋습니다.

대기 시간 증가가 특정 최종 사용자 그룹에 영향을 미치는 경우 최종 사용자 컴퓨팅 서비스 및 가속기를 사용하는 것을 고려합니다.

- AWS 설명서: [AWS Direct Connect](#)
- AWS 설명서: [AWS Global Accelerator란 무엇입니까? - AWS Global Accelerator](#)
- SAP on AWS 블로그: [Amazon AppStream 2.0에 SAP GUI 배포](#)

제안 사항 13.4.2 – 시스템 내부 대기 시간에 대한 SAP 지침을 인지

SAP는 애플리케이션과 데이터베이스 간 트래픽 및 SAP HANA 시스템 복제에 허용 가능한 네트워크 대기 시간에 대한 지침을 제공합니다.

- SAP Note: [1100926 - FAQ: 네트워크 성능](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2543171 - 애플리케이션 측 및 데이터베이스 간의 지연 시간 문제](#) [SAP 포털 액세스 권한 필요]

이러한 노트에 수록된 데이터베이스와 애플리케이션 서버 간 연결에 대한 지침은 단일 데이터 센터에서 실행되는 시스템을 기반으로 한 것으로, 다중 AZ 배포의 복원력 이점이 반영되지 않았습니다. 가용 영역은 한 AWS 리전에서 의미 있는 거리(최소 10km)로 분리되고 이중화 전원, 네트워킹 및 연결을 갖춘 하나 이상의 개별 데이터 센터입니다.

AWS의 고가용성(HA) SAP 아키텍처는 일반적으로 SAP 애플리케이션 서버 인스턴스를 포함하여 인프라를 여러 AZ에 걸쳐 배포합니다. 상당한 수의 데이터베이스 호출을 수행하는 SAP 트랜잭션 또는 배치 작업이 있는 경우 데이터베이스와 동일한 AZ에 상주하는 SAP 애플리케이션 서버에서 이러한 작업을 실행하는 것이 좋습니다. 또한 최종 사용자의 경우 SAP 로그인 그룹(트랜잭션 SMLG)을 사용하고 백그라운드 처리 작업의 경우 배치 서버 그룹(트랜잭션 SM61)을 사용합니다. 그러면 SAP 워크로드에서 대기 시간에 민감한 부분이 올바른 애플리케이션 서버에서 실행됩니다. NIPING과 같은 도구를 사용하여 대기 시간을 측정합니다.

SAP는 SYNC 모드에서 SAP HANA 동기 복제를 지원하기 위해 약 1.0ms의 대기 시간을 권장하며, 이는 가용 영역 간에 달성 가능합니다.

- SAP 설명서: [SAP HANA 네트워크 요구 사항](#)

제안 사항 13.4.3 – SAP HANA 스케일 아웃에 배치 그룹을 사용

SAP HANA 스케일 아웃 배포에서 노드 간 통신에 대한 SAP 인증을 충족하려면 클러스터 배치 그룹을 사용해야 합니다.

- AWS 설명서: [배치 그룹 - Amazon Elastic Compute Cloud](#)

14 – 최적 스토리지 솔루션 선택

SAP 워크로드에 최적인 스토리지 솔루션을 선택하는 방법은 무엇입니까? 이 스토리지를 구성하는 방법은 시스템 성능에 영향을 미칩니다. AWS는 SAP 데이터베이스, 애플리케이션 및 백업의 스토리지 요구 사항을 충족하기 위해 블록, 파일 및 객체 스토리지를 포함하는 광범위한 서비스를 제공합니다. SAP가 벤치마킹하고 인증한 지침을 따르는 것이 좋습니다. SAP HANA의 경우 매우 구체적인 지침이 있습니다. 다른 데이터베이스는 워크로드와 일치시키려면 더 많은 분석이 필요합니다.

ID	우선순위	모범 사례
□ BP 14.1	필수	기능에 부합하는 탑재 지점 및 볼륨 연결 생성
□ BP 14.2	필수	성능 요구 사항에 부합하는 Amazon EBS 유형 선택 및 구성
□ BP 14.3	권장	SAP 사용 사례에 대한 Amazon EFS 및 Amazon FSx 성능 적합성 평가
□ BP 14.4	권장	스토리지 대안으로 메모리를 고려
□ BP 14.5	권장	라이브 시스템에 대한 영향이 제한되도록 백업 성능에 적합한 백업 솔루션 및 일정 선택

모범 사례 14.1 - 기능에 부합하는 탑재 지점 및 볼륨 연결 생성

SAP 파일 시스템에는 고유한 성능 및 공유 요구 사항이 있습니다. 예를 들어 데이터베이스의 성능 프로파일은 많은 수의 읽기 I/O 작업을 지원하기 위해 데이터 파일 시스템을 요구할 수 있지만 로그 파일 시스템은 처리량의 제약을 받을 가능성이 더 높습니다. 모든 애플리케이션 서버가 로그 및 전송 파일에

액세스할 수 있도록 `sapmnt` 및 `trans` 와 같은 파일 시스템을 공유해야 합니다. 이러한 차이점을 인식하여 성능 병목 현상이 없고 액세스 요구 사항이 충족되도록 파일 시스템을 볼륨에 매핑해야 합니다.

제안 사항 14.1.1 – 각 시스템의 SAP 파일 시스템 및 디렉터리 요구 사항을 식별

SAP 파일 시스템에는 시스템 디렉터리(`root`, `boot`), 실행 파일, 페이지 또는 스왑, 애플리케이션별 요구 사항이 포함됩니다. 다음을 고려하여 각 요구 사항을 분석해야 합니다.

- 파일 시스템이 용량에 도달했을 때(100% 사용됨) 미치는 영향(특히 `root` 디렉터리)
- AMI 또는 배포 패턴에 포함되는지 여부를 포함한 빌드 일관성
- 복원력 요구 사항
- 공유 요구 사항
- 성능 프로필

핵심 SAP 파일 시스템 요구 사항은 SAP 설명서 SAP Required Filesystems and Directories(SAP에 필요한 파일 시스템 및 디렉터리)에 나열되어 있습니다. 이를 기준으로 사용하고 조직에 고유한 기타 요구 사항을 포함합니다.

제안 사항 14.1.2 – 파일 시스템 기능과 일치하도록 적절한 AWS 스토리지 서비스를 매핑

파일 시스템은 로컬 또는 공유(NFS/SMB)일 수 있습니다. 공유 파일 시스템의 경우 호스트된 NFS 서버와 비교하여 안정성 및 가용성 이점을 제공하는 Amazon EFS, Amazon FSx와 같은 AWS 서비스를 사용하는 것을 고려합니다.

Amazon EC2 인스턴스 스토어는 인스턴스에 임시 블록 수준 스토리지를 제공하는 또 다른 파일 시스템 옵션입니다. 지속성, 인스턴스 유형 간 가용성이 없고 인스턴스 복구를 사용할 수 없기 때문에 사용을 권장하지 않습니다.

제안 사항 14.1.3 – 지원되는 파일 시스템 유형을 사용

SAP 지원 Linux 배포판은 다양한 파일 시스템 유형을 권장합니다. 이후 버전은 XFS를 기반으로 표준화되고 있지만, 지원을 검토하여 운영 체제 및 데이터베이스 버전에 성능이나 기능 영향이 없는지 확인해야 합니다.

- SAP Note: [405827 - Linux: Recommended file systems](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2972496 - SAP HANA 파일 시스템 유형](#) [SAP 포털 액세스 권한 필요]

모범 사례 14.2 - 성능 요구 사항에 부합하는 Amazon EBS 유형 선택 및 구성

각 파일 시스템 기능 및 스토리지 서비스에 대해 스토리지 레이아웃 지침과 튜닝 옵션을 평가하여 IOPS 및 처리량 성능이 최적화되었는지 확인합니다.

제안 사항 14.2.1 – EBS 볼륨 유형에 대한 스토리지 특성 및 옵션을 평가

AWS에는 고유한 특성을 가진 다양한 볼륨 유형이 있어 SAP 워크로드의 다양한 성능 요구 사항을 충족할 수 있습니다. 기록 데이터 또는 크기 조정을 사용하여 IOPS 및 처리량 요구 사항을 평가합니다. 성능, 내구성, 유연성 및 비용을 고려하여 볼륨 유형을 선택합니다.

볼륨 유형 gp3, io1 및 io2 의 IOPS 및 처리량은 볼륨 크기와 독립적입니다.

볼륨 유형 gp2 의 IOPS 및 처리량은 볼륨 크기에 따라 다릅니다. 필요한 IOPS 및 처리량을 사용할 수 있으려면 볼륨을 더 크게 지정해야 할 수 있습니다.

- AWS 설명서: [Amazon EBS 볼륨 유형](#)

제안 사항 14.2.2 – LVM 스트라이핑 메커니즘을 사용하여 선형으로 크기 조정

단일 EBS 볼륨으로 성능 요구 사항을 충족할 수 없는 경우 논리적 볼륨 관리(LVM)를 사용한 스트라이핑을 고려합니다. 예를 들어 단일 볼륨의 처리량이 250MiB/s인 경우 4개 볼륨에 걸쳐 스트라이프 세트가 있으면 1,000MiB/s의 처리량을 제공할 수 있습니다.

볼륨은 크기 및 성능 특성이 동일해야 합니다.

SAP HANA 벤치마크 테스트에서 데이터 볼륨에 256KB 스트라이프 크기를 사용하고 로그 볼륨에 64KB 스트라이프 크기를 사용하여 최상의 성능을 얻었습니다.

처리량, I/O 및 연결된 볼륨 수에 대한 인스턴스 제한에 유의해야 합니다.

- AWS 설명서: [EBS 볼륨에 LVM 논리 볼륨 생성](#)
- SAP Note: [2931808 - Usage of Logical Volume Manager\(LVM\) with SAP HANA](#) [SAP 포털 액세스 권한 필요]
- AWS 설명서: [운영 체제 및 스토리지 구성 - SAP HANA on AWS](#)

제안 사항 14.2.3 – SAP HANA 성능을 보장하도록 AWS 제공 스토리지 지침을 준수

AWS는 SAP와 협력하여 정의된 성능 벤치마크에 따라 SAP HANA 워크로드용 스토리지를 인증합니다. AWS가 제공하는 구성에는 SAP TDI 5 Storage KPI의 프레임워크 내에서 성능, 비용, 내구성이 균

형 있게 반영되어 있습니다. 호환 스토리지 레이아웃은 설명서에 자세히 설명되어 있으며 시작 마법사 및 빠른 시작 배포에 사용됩니다.

- AWS 설명서: [SAP HANA용 스토리지 구성 - SAP HANA on AWS](#)

AWS 구성과 다른 경우 하드웨어 검사 도구를 실행하는 것이 좋습니다.

- SAP Note: [1943937 - 하드웨어 구성 검사 도구 - Central Note](#) [SAP 포털 액세스 권한 필요]

범용 SSD와 프로비저닝된 IOPS SSD 중에서 선택할 때 범용 SSD가 SAP KPI를 충족한다는 점을 이해하고 있어야 합니다. SAP HANA와 같은 인 메모리 데이터베이스는 데이터베이스 시작 시 디스크에서 메모리로 데이터를 로드해야 합니다. 성능이 우수한 스토리지 솔루션 및 설계는 시작 시간을 크게 단축하고 스토리지 성능에 의존하는 백업 및 복원과 같은 작업의 속도를 향상할 수 있습니다.

대규모 시스템 또는 가동 시간 요구 사항이 매우 높은 시스템은 프로비저닝된 IOPS가 유리할 수 있습니다. 최상의 배포 패턴에 대한 추가 지침은 AWS 팀에 문의하세요.

제안 사항 14.2.4 – 성능이 우수한 로컬 백업을 저렴한 비용을 사용하기 위해 **st1** 스토리지 사용

SAP 솔루션에 백업 저장을 위한 로컬 스토리지가 필요한 경우 저렴한 비용으로 높은 처리량을 제공하는 st1 인스턴스 유형을 사용하는 것을 고려합니다. st1은 자주 액세스하는 처리량 집약적 워크로드를 위해 설계된 저비용 블록 스토리지 유형입니다.

SAP HANA의 경우 2단계 백업의 성능 및 비용 영향을 피할 수 있도록 AWS Backint Agent for SAP HANA를 사용하는 것을 고려합니다.

모범 사례 14.3 - SAP 사용 사례에 대한 Amazon EFS 및 Amazon FSx 성능 적합성 평가

Amazon EFS(Linux) 및 Amazon FSx(Windows)는 여러 가용 영역에 걸쳐 배치할 수 있는 고내구성 및고가용성 파일 시스템을 제공합니다. 두 솔루션 모두 고성능을 제공하도록 설계되었지만 네트워크 파일 시스템 사용을 선택할 때는 액세스 패턴을 고려해야 합니다. 예를 들어, 많은 수의 소용량 파일, 고도의 병렬 쓰기 또는 높은 쓰기/읽기 비율은 적합하지 않을 수 있습니다. SAP 워크로드의 경우 SAP HANA XSA, Java 실행 파일 또는 많은 수의 작업 및 스펴 로그에 적용될 수 있습니다.

제안 사항 14.3.1 – 크기 조정 및 성능 옵션을 평가

Amazon EFS에는 범용 및 최대 I/O라는 두 가지 성능 모드와 버스팅 모드 및 프로비저닝된 모드라는 두 가지 성능 모드가 있습니다. SAP 애플리케이션의 경우 범용 성능 모드가 일반적으로 충분한 I/O를 제공합니다. 파일 시스템의 데이터 양이 처리량 요구에 비해 적은 경우와 같이 프로비저닝된 처리량을 고려해야 하는 시나리오가 있을 수 있습니다.

- AWS 설명서: [Amazon Elastic File System\(EFS\) | FAQ - 크기 조정 및 성능](#)
- AWS 설명서: [Amazon FSx for Windows File Server 기능 | 크기 조정 및 성능](#)

제안 사항 14.3.2 - 단기 요구 사항을 위해 임시 프로비저닝을 고려

마이그레이션 또는 일회성 작업과 관련된 사용 사례에는 이벤트 기간 동안 성능 특성을 조정할 수 있는 임시 파일 시스템이 유용할 수 있습니다.

모범 사례 14.4 - 스토리지 대안으로 메모리를 고려

지원되는 시나리오에 대해 데이터베이스 또는 애플리케이션 계층에서 메모리를 사용할 때의 성능 이점을 고려합니다. SAP HANA는 기본적으로 메모리를 사용하지만 로드를 최적화하거나 정적 데이터를 오프로드하는 옵션의 이점을 누릴 수 있습니다. 관계형 데이터베이스는 캐싱을 활용해야 하며 애플리케이션 서버는 스왑이 요구 사항인지 고려해야 합니다.

제안 사항 14.4.1 - SAP HANA에 대해 메모리 사용을 최적화

SAP HANA 메모리 요구 사항과 운영 체제 메모리 지표 간의 상관 관계를 이해하여 메모리 병목 현상이 성능에 영향을 미치지 않도록 해야 합니다.

- SAP 문서: [SAP HANA 메모리 사용량 및 운영 체제](#)
- SAP Note: [1999997 - FAQ: SAP HANA 메모리](#) [SAP 포털 액세스 권한 필요]

호스트 재시작을 포함하지 않는 시나리오에서 데이터베이스 시작 성능을 향상하려면 SAP HANA Fast Restart 옵션을 사용하는 것을 고려합니다. SAP HANA Fast Restart 옵션은 RAM의 일부를 운영 체제가 재시작할 때까지 영구 메모리로 취급되는 임시 파일 시스템(tempfs)으로 할당하고 컬럼 스토어의 주요 부분을 해당 tempfs에 배치하도록 허용합니다. 이 부분은 인덱스 서버 재시작 또는 크래시에도 유지됩니다. 그러므로 스토리지로부터 다시 로드(I/O를 사용)가 필요하지 않습니다.

- SAP 문서: [HANA 빠른 재시작 문서](#)

제안 사항 14.4.2 - 관계형 데이터베이스에 데이터베이스 캐싱을 사용

읽기 IOP 요구 사항이 높은 관계형 데이터베이스의 경우 데이터베이스 캐싱을 사용하면 처리량 및 데이터 검색 대기 시간을 크게 개선할 수 있습니다. 캐시는 데이터베이스에 대한 인접 데이터 액세스 계층 역할을 하여 읽기 성능이 향상됩니다.

다음 설명서에서는 캐싱 사용 사례에 대한 정보를 제공하지만 이 세부 정보는 대부분 AWS 데이터베이스와 관련되므로 관계형 데이터베이스 구성과 관련된 정보는 SAP Note를 참조하세요.

- AWS 설명서: [캐싱 \(데이터베이스 캐싱 포함\)](#)

제안 사항 14.4.3 – SAP 애플리케이션의 스왑 공간 요구 사항을 평가

물리적 메모리 리소스가 고갈되면 SAP는 스왑을 사용하여 비활성 페이지를 전용 디스크 기반 저장 영역으로 이동합니다. 스왑이 있으면 메모리 부족으로 인해 애플리케이션이 크래시하는 것을 방지할 수 있지만 스왑이 자주 사용되지 않도록 구성 파라미터와 메모리 크기 조정을 적용하는 것이 좋습니다.

스왑 사용이 예상되는 경우 추가 성능 문제를 방지하기 위해 할당된 볼륨의 특성을 평가합니다. 스왑은 호스트에서 물리적 메모리가 고갈될 때 SAP 애플리케이션에서 메모리 부족 상황이 발생하는 것을 방지할 수 있습니다.

- SAP Note: [153641 - R/3 64비트 커널의 스왑 공간 요구 사항](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2999334 - SWAP Utilization](#) (HANA 관련) [SAP 포털 액세스 권한 필요]
- SAP Note: [2488097 - FAQ: Windows ABAP 서버의 메모리 사용량](#) [SAP 포털 액세스 권한 필요]

모범 사례 14.5 – 적절한 백업 솔루션 및 일정 선택

백업 방법에 따라 스토리지에서 읽기 및 쓰기 작업이 모두 크게 증가하여 애플리케이션 성능에 부정적인 영향을 미칠 수 있습니다. 볼륨이 크고 기간이 길 수 있는 데이터베이스 수준 백업은 특히 그렇습니다.

제안 사항 14.5.1 – 적절한 백업 기간을 결정

비즈니스 요구 사항에 따라 백업 작업을 실행하는 데 가장 적절한 기간을 정의합니다. 야간 배치 일정, 허용 가능한 런타임과 같은 주요 종속성을 고려합니다.

제안 사항 14.5.2 – 백업의 성능 영향을 최소화하는 옵션을 고려

스토리지 또는 네트워크 제약 조건을 분석하고 백업의 영향을 최소화하는 옵션을 평가합니다. 여기에는 데이터베이스 또는 스토리지 수준에서 델타 변경 백업을 사용하여 기간을 단축하는 것이 포함될 수 있습니다. 안정성 원칙을 참조하여 이로 인해 백업의 일관성 또는 전체 복원 시간에 부정적인 영향이 미치지 않도록 하세요.

- SAP Lens [안정성]: [모범 사례 12.1 - 일관된 비즈니스 데이터 복구를 위한 방법 수립](#)

15 - 운영 체제, 데이터베이스 및 SAP 애플리케이션 계층에 대한 튜닝 옵션 평가

다양한 튜닝 옵션이 SAP 시스템 성능에 미치는 영향을 어떻게 이해하고 계산합니까? SAP 소프트웨어 제품, 지원되는 운영 체제 및 데이터베이스, 버전의 다양한 조합에 따라 성능 권장 사항의 차이가 크므로 단일 문서에 성능 우수성 권장 사항의 전체 목록이 포함되지 않습니다. 이를 감안하여 다음 지침을 대부분의 SAP 사용 사례에 적용해야 하며, 해당되는 경우 특정 초점 영역이 언급될 것입니다.

ID	우선순위	모범 사례
<input type="checkbox"/> BP 15.1	필수	SAP 성능에 대한 운영 체제 지침을 준수
<input type="checkbox"/> BP 15.2	적극 권장	하드웨어 선택에 맞춰 데이터베이스 파라미터 수정
<input type="checkbox"/> BP 15.3	적극 권장	하드웨어 선택에 맞춰 SAP 파라미터 수정
<input type="checkbox"/> BP 15.4	권장	복구 및 가용성을 위해 튜닝

모범 사례 15.1 - SAP 성능에 대한 운영 체제 지침을 준수

SAP는 배포하는 SAP 소프트웨어에 지원되는 각 운영 체제에서 최적의 성능을 보장하기 위해 튜닝하는 방법에 대한 구체적인 지침을 제공합니다. 관련 튜닝 파라미터를 이해하고 운영 체제별 옵션을 활용하여 성능 튜닝을 보다 용이하고 보다 동적으로 수행하려면 배포하는 운영 체제에 대한 모든 관련 SAP 설명서를 읽어야 합니다.

제안 사항 15.1.1 – 설치, 버전 업데이트 또는 인프라 변경 전에 운영 체제 관련 SAP Note를 검토

운영 체제를 빌드 또는 업데이트할 때(자동화를 통해 또는 수동으로) SAP 소프트웨어와 운영 체제 버전의 조합에 적절한 성능 설정이 적용되었는지 확인합니다.

제안 사항 15.1.2 – 운영 체제 공급 업체가 제공하는 SAP 튜닝을 평가

Red Hat 및 SUSE는 SAP 실행에 최적화된 도구와 구성이 포함된 이미지 및 리포지토리를 제공합니다. 이들은 AWS Marketplace에서 또는 기존 보유 구독 사용(BYOS) 모델을 통해 사용할 수 있습니다.

공급 업체는 운영 체제가 SAP 애플리케이션에 최적화되도록 노력하고 있습니다. 공급 업체 제공 튜닝 도구(예: saptune 또는 Red Hat Enterprise Linux용 (Ansible) 시스템 역할)를 사용하면 알려진 성능 튜닝 기준을 정의하는 데 도움이 될 수 있습니다. 특정 SAP 워크로드를 가장 잘 수용하도록 운영 체제를 튜닝하는 작업은 여전히 필요하지만 이러한 도구를 사용하면 가장 일반적인 요구 사항을 조사, 계산 및 적용하는 데 들어가는 작업량을 줄일 수 있습니다. 또한 tuned 데몬과 연결된 구성을 CPU 수 및 가용 메모리를 포함하여 시스템에서 수집한 정보를 사용하여 동적으로 조정할 수도 있습니다.

운영 체제	Guidance
SUSE Linux Enterprise Server	SAP Note: 1275776 - Linux: SAP 환경용 SLES 준비 [SAP 포털 액세스 권한 필요]
Red Hat Enterprise Linux	SAP Note: 2777782 - SAP HANA DB: RHEL 8의 권장 OS 설정 [SAP 포털 액세스 권한 필요]
Microsoft Windows	(지침은 SAP 또는 공급 업체 설명서 참조)
Oracle Enterprise Linux	SAP Note: 2478541 - Oracle 데이터베이스의 운영 체제 요구 사항 [SAP 포털 액세스 권한 필요]

제안 사항 15.1.3 – 운영 체제에 관련 네트워크 파라미터를 적용

SAP 시스템 성능은 특히 SAP HANA 스케일 아웃 데이터베이스 설계에서 또한 시스템 환경의 여러 애플리케이션 서버 인스턴스와 데이터베이스 인스턴스 간의 통신에서 잘못된 네트워크 구성으로 인해 심각한 영향을 받을 수 있습니다. AWS에서 대부분의 경우 인스턴스의 최대 네트워크 처리량은 인스턴스 패밀리 및 크기에 따라 결정되지만 운영 체제 수준 및 SAP 소프트웨어 자체의 네트워크 설정 조정이 영향을 미칠 수 있습니다.

다음 AWS 및 SAP 권장 사항을 참조하세요.

- AWS 설명서: [동일한 Amazon VPC의 Amazon EC2 Linux 인스턴스 간에 네트워크 처리량 벤치마킹](#)
- AWS 설명서: [Elastic Network Adapter – Amazon EC2용 고성능 네트워크 인터페이스](#)
- AWS 설명서: [클러스터 배치 그룹](#)
- SAP Note: [2198693 - Key Monitoring Metrics for SAP on Amazon Web Services\(AWS\)](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [1612283 - 하드웨어 구성 기준 및 지침](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2081065 - SAP HANA 네트워크 문제 해결](#) [SAP 포털 액세스 권한 필요]

- SAP Note: [1100926 - FAQ: 네트워크 성능](#) [SAP 포털 액세스 권한 필요]

모범 사례 15.2 - 하드웨어 선택에 맞춰 데이터베이스 파라미터 수정

SAP는 기본 데이터베이스의 특정 파라미터를 수정하여 SAP 시스템의 성능을 최적화하기 위한 구체적인 지침을 제공합니다. 이러한 파라미터는 데이터베이스 유형에 고유하며 분석 또는 트랜잭션 유형 애플리케이션을 지원하는지 여부에 따라 달라질 수 있습니다.

제안 사항 15.2.1 – SAP HANA 관련 튜닝 파라미터를 검토(해당되는 경우)

운영 체제 및 SAP HANA 데이터베이스 파라미터는 성능에 큰 영향을 미칠 수 있습니다. 운영 체제 및 스토리지 구성에 대한 SAP on AWS 권장 사항을 따르세요.

- AWS 설명서: [SAP HANA on AWS – 운영 체제 및 스토리지 구성](#)

메모리 할당 등 SAP HANA 파라미터에 대한 지침은 SAP Note 및 설명서를 참조하세요.

- SAP Note: [2000000 - FAQ: SAP HANA 성능 최적화](#) [SAP 포털 액세스 권한 필요]
- SAP 설명서: [HANA Parameter: global_allocation_limit](#)
- SAP Note: [1999997 - FAQ: SAP HANA 메모리](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [2926166 - 전반적인 SAP HANA 메모리 할당을 제한하는 방법](#) [SAP 포털 액세스 권한 필요]

제안 사항 15.2.2 – 비 SAP HANA 데이터베이스에 대한 데이터베이스 튜닝 가이드를 검토

SAP 시스템의 기본 데이터베이스에 관계없이 시스템 성능은 부분적으로 데이터베이스를 튜닝하는 방법에 따라 달라집니다. 각 데이터베이스에는 사용 가능한 컴퓨팅, 메모리 및 디스크 스토리지를 기반으로 튜닝에 대한 특정 권장 사항이 있습니다. 특정 데이터베이스 파라미터는 선택한 기본 EC2 인스턴스 크기에 따라 다릅니다. 예를 들어 사용 가능한 물리적 메모리는 Oracle 데이터베이스의 db_cache_size 를 제한합니다.

사용하는 데이터베이스와 관련된 정보는 다음을 참조하세요.

데이터베이스	Guidance
SAP ASE	SAP Note: 2473646 - ASE -SAP ASE의 성능 및 튜닝 정보 [SAP 포털 액세스 권한 필요]

데이터베이스	Guidance
IBM Db2	SAP Note: 2751102 – DB6: DB2 11.5 표준 파라미터 설정 [SAP 포털 액세스 권한 필요]
Oracle	SAP Note: 2470718 – Oracle 데이터베이스 파라미터 12.2 / 18c / 19c [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 2779607 – SQL Server 2019의 구성 파라미터 [SAP 포털 액세스 권한 필요], SAP Note: 2729848 – SQL Server 2019의 SAP 설치 미디어 및 SQL4SAP [SAP 포털 액세스 권한 필요]
SAP MaxDB	SAP Note: 819641 – FAQ: SAP MaxDB 성능 [SAP 포털 액세스 권한 필요]

모범 사례 15.3 - 하드웨어 선택에 맞춰 SAP 파라미터 수정

SAP 애플리케이션 파라미터를 조정하면 애플리케이션 성능을 개선하는 데 도움이 될 수 있습니다. 이러한 파라미터는 기본 하드웨어 구성 및 운영 체제 유형에 따라 달라지는 경우가 많습니다.

제안 사항 15.3.1 – SAP가 **PHYS_MEMSIZE# ## ## ##### ##**

커널 릴리스 7.40 이상을 사용하는 최신 버전의 SAP 소프트웨어에서는 특정 파라미터의 자체 튜닝이 가능하며 권장됩니다. 예를 들어 많은 파라미터가 인스턴스(PHYS_MEMSIZE)에서 사용 가능한 기본 메모리와 관련된 공식을 통해 도출됩니다. 그러므로 변화하는 성능 요구 사항을 충족하기 위해 SAP 소프트웨어의 기반이 되는 EC2 인스턴스의 크기를 조정할 때 메모리 파라미터가 자동으로 조정될 수 있습니다.

- SAP 설명서: [SAP 메모리 관리: 파라미터 참조](#)
- SAP Note: [2085980 – Kernel 릴리스 7.40의 메모리 관리 새로운 기능](#) [SAP 포털 액세스 권한 필요]

제안 사항 15.3.2 – SAP 스왑 공간 및 최대 메모리 사용량을 검토

SAP on AWS를 실행할 때 디스크의 스왑 공간을 과도하게 사용하면 Amazon EBS에서 I/O 크레딧이 고갈되어 성능이 저하될 수 있습니다. AWS에서 사용 가능한 다양한 [EBS 스토리지 옵션](#) 을 평가하고 성능 요구 사항을 충족하도록 스왑 공간을 구성합니다.

- SAP Note: [1597355 - Linux의 스왑 공간 권장 사항](#) [SAP 포털 액세스 권한 필요]

- SAP 설명서: [스왑 공간 요구 사항](#)

모범 사례 15.4 – 복구 및 가용성 옵션에 대한 성능 튜닝을 고려

Well-Architected 안정성 및 운영 우수성 원칙을 참고하여 선택한 복구 및 복원력 요구 사항에 따라 SAP 시스템 튜닝을 평가하여 성능 영향을 최소화해야 합니다. 백업 중 시스템 성능, 선택한 데이터베이스의 클러스터링 옵션(예: 동기식 및 비동기식 SAP HANA 시스템 복제), 여러 SAP 애플리케이션 서버 인스턴스로 로드 분산과 같은 항목을 고려합니다.

제안 사항 15.4.1 – 백업 및 복구 솔루션에 대한 성능 권장 사항을 검토

지원되는 각 데이터베이스마다 백업 및 복구 작업 성능을 최적화하기 위한 다양한 권장 사항이 있으며, 이러한 권장 사항은 서드 파티 제품을 포함하여 백업 및 복원 관리를 위해 선택한 소프트웨어 솔루션과 연동하는 경우가 많습니다. AWS의 예에는 AWS Backint Agent for SAP HANA를 사용할 때 EBS 볼륨 및 동시성 파라미터 설정의 최대 IOPS 및 처리량 구성이 포함됩니다.

일반적으로 EC2 인스턴스와 백업 스토리지 대상(예: EBS 볼륨, S3 버킷, EFS 파일 시스템) 간의 처리량 향상을 위한 지침을 따르면 백업 및 복구 성능을 향상할 수 있습니다. 예를 들어 Amazon S3를 백업 용 리포지토리로 사용하는 경우 Amazon S3용 AWS Command Line Interface(CLI)를 사용하면 최대 동시 요청 수 또는 멀티파트 청크 크기와 같은 [구성 파라미터](#)를 변경하여 성능을 향상할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- AWS 설명서: [AWS Backint Agent for SAP HANA](#)
- AWS 설명서: [SAP NetWeaver on AWS – 백업 및 복구](#)
- SAP on AWS 블로그: [가용성 및 안정성을 위한 구축](#)

데이터베이스	Guidance
SAP HANA	<ul style="list-style-type: none"> • AWS 설명서: SAP HANA on AWS – SAP HANA용 스토리지 구성 [SAP 포털 액세스 권한 필요] • SAP Note: 1842096 - HANA 백업 및 복원 성능 [SAP 포털 액세스 권한 필요] • SAP Note: 2945518 - 데이터 백업 실행 중 HANA에서 발생한 성능 문제 [SAP 포털 액세스 권한 필요]
SAP ASE	(지침은 SAP 또는 공급 업체 설명서 참조)

데이터베이스	Guidance
IBM Db2	(지침은 SAP 또는 공급 업체 설명서 참조)
Oracle	SAP Note: 2084077 - Oracle 데이터베이스의 백업 주기를 계획하는 방법 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 1420452 - FAQ: MS SQL Server로 복원 및 복구 [SAP 포털 액세스 권한 필요]
SAP MaxDB	SAP Note: 1377148 - FAQ: SAP MaxDB 백업 / 복구 [SAP 포털 액세스 권한 필요]

제안 사항 15.4.2 – 클러스터링 파라미터의 구성을 검토

SAP HANA 및 기타 데이터베이스에 대한 클러스터링 옵션은 기본 인스턴스와 장애 조치 인스턴스 간의 클러스터에서 확인된 연결(즉, 하트비트)에 의존하는 경우가 많습니다. SAP 관리자는 시스템에서 작업이 발생할 수 있는 속도와 통신 중단이 오탐되는 경우 발생할 수 있는 장애 조치 부작용의 가능성을 균형 있게 고려해야 합니다. 시간 초과 파라미터 및 관련 설정에 대한 권장 사항을 따르세요.

- AWS 설명서: [SAP HANA on AWS: SLES 및 RHEL용 고가용성 구성 가이드](#)
- AWS 설명서: [SAP HANA on AWS 운영 가이드: 네트워킹](#)
- AWS 설명서: [SAP on AWS – 페이스메이커를 사용한 IBM Db2 HADR](#)
- SAP Note: 1612105 - [DB6: FAQ on Db2 High Availability Disaster Recovery\(HADR\)](#) [SAP 포털 액세스 권한 필요]
- 운영 체제별 설명서: [SUSE Linux SAP HSR 크기 조정 성능 최적화 시나리오](#)
- 운영 체제별 설명서: [페이스메이커 클러스터의 크기 조정에서 자동화된 SAP HANA 시스템 복제](#)

16 - 지속적인 성능 및 최적화 옵션 이해

성능 변화와 최적화 기회를 측정하기 위해 어떤 프로세스 및 절차를 사용하고 있습니까? 과거 모니터링 데이터에서 애플리케이션 성능 요구 사항의 기준을 식별하고 관련 경고를 설정하여 편차가 발생하면 시스템 관리자에게 알립니다. 시스템 관리자가 수동 또는 자동 작업으로 이러한 문제를 해결할 수 있는 절차를 수립합니다.

ID	우선순위	모범 사례
□ BP 16.1	필수	성능 평가를 위한 데이터 확보
□ BP 16.2	필수	기준 성능 요구 사항 설정
□ BP 16.3	적극 권장	데이터를 사용하여 성능 추세 식별
□ BP 16.4	적극 권장	성능 문제 식별 및 해결
□ BP 16.5	적극 권장	동적 크기 조정을 통해 성능 요구 충족
□ BP 16.6	권장	분석을 위해 프로덕션 로드 시뮬레이션 메커니즘 개발
□ BP 16.7	권장	성능 데이터를 기반으로 크기 조정 및 구성을 지속적으로 최적화

모범 사례 16.1 – 성능 평가를 위한 데이터 확보

SAP 시스템의 성능을 평가하고 최적 성능이 아닌 경우 조치를 취하려면 리소스 모니터링에 관한 Well-Architected Framework 성능 우수성 지침에 설명된 대로 컴퓨팅, 메모리, 스토리지 및 네트워킹에 대한 모니터링 데이터를 수집해야 합니다. Well-Architected Framework 운영 우수성 원칙에 명시된 대로 시스템의 현재 상태를 이해하고, 핵심 성과 지표를 설정하고, 진단을 위해 적시에 지표를 수집하는 것이 성능 문제를 조사하는 데 중요합니다.

- Well-Architected Framework [성능 효율성]: [리소스를 모니터링하여 예상 성능을 제공하는지 확인](#)
- Well-Architected Framework [운영 우수성]: [워크로드 상태 파악](#)

제안 사항 16.1.1 – 성능 지표와 관련된 데이터를 수집 및 저장

관련 SAP 모니터링 데이터를 수집하고 확인하려면 SAP용 AWS Data Provider를 설치 및 구성하고 SAP 워크로드를 지원하는 특정 모니터링 도구에서 지표를 설정해야 합니다. 모니터링 및 추가 권장 사항에 대한 자세한 내용은 운영 우수성 원칙에서 확인할 수 있습니다.

- AWS 설명서: [AWS Data Provider for SAP\(SAP용 AWS Data Provider\)](#)
- SAP Lens [운영 우수성]: [모범 사례 1.1 - SAP on AWS 모니터링을 위한 사전 조건 구현](#)
- SAP Lens [운영 우수성]: [모범 사례 1.2 - SAP에 대한 인프라 모니터링 구현](#)
- SAP Lens [운영 우수성]: [모범 사례 1.3 - SAP에 대한 개별 애플리케이션 모니터링 구현](#)

모범 사례 16.2 - 기존 성능 요구 사항 설정

모든 SAP 애플리케이션에는 고유한 성능 요구 사항이 있습니다. 과거 모니터링 데이터를 사용하면 SAP 관리 팀이 이러한 애플리케이션의 기존 성능을 파악하여 성능 변화의 범위를 식별 및 이해할 수 있습니다. 의도하지 않은 CPU 스파이크, 스토리지 처리량 델타, 메모리 사용 증가, 보다 복잡한 성능 저하와 같은 이상 현상을 감지하기 위해 관련 경고를 설정할 수 있습니다. 이 모니터링 데이터를 사용하여 성능을 추가로 미세 튜닝할 수 있습니다.

제안 사항 16.2.1 – SAP 관련 KPI를 반영하는 데이터를 수집 및 평가

이 제안 사항은 Well-Architected Framework 성능 효율성 원칙의 [리소스 모니터링](#)에 관한 추가 제안 사항과 밀접한 관련이 있습니다.

이 일반 지침 외에도 SAP 관련 KPI에는 대화 응답 시간, 버퍼 스왑, 사용된 메모리가 포함됩니다. 이러한 KPI는 실행 중인 SAP 소프트웨어 유형 및 버전에 따라 다를 수 있습니다. KPI 및 모니터링 권장 사항에 대한 자세한 내용은 이 문서의 운영 우수성 원칙에 나와 있습니다.

- SAP Lens [운영 우수성]: [모범 사례 1.2 - SAP에 대한 인프라 모니터링 구현](#)
- SAP Lens [운영 우수성]: [모범 사례 1.3 - SAP에 대한 개별 애플리케이션 모니터링 구현](#)

모범 사례 16.3 - 데이터를 사용하여 성능 추세 식별

성능 기준이 설정된 후에는 시스템 관리자가 시간에 따른 추세를 모니터링하여 KPI가 원하는 기준 내에서 안정적으로 유지되는지 확인해야 합니다. 성능 데이터가 허용할 수 없는 KPI 값을 향하는 추세를 보이는 경우 시스템 관리자는 성능 영향을 방지 또는 완화하기 위한 조치를 취할 수 있습니다.

제안 사항 16.3.1 – 주기적으로 SAP 시스템 성능 검토를 수행

시스템 관리자가 KPI를 정기적으로 검토하면 성능 관련 데이터의 추세를 식별하고 어떤 경고가 가장 유용한지 결정하는 데 도움이 될 수 있습니다. 그런 다음 이러한 경고를 사용하여 추세가 지속되는 경우

알림을 자동화하고 잠재적인 성능 문제를 해결하기 위한 자동 수정 조치(예: 성능 지표에 대한 응답으로 SAP 파라미터를 동적으로 변경)를 설정할 수 있습니다. KPI 및 관련 추세에는 SAP EarlyWatch Alert 보고서에서 확인할 수 있으며, 경우에 따라 유용한 추가 지표를 사용하여 사용자 지정할 수 있습니다. SAP 서비스 수준 보고는 SAP 워크로드에 대한 서비스 수준 계약(SLA)이 있는 경우에도 유용할 수 있습니다.

- SAP 설명서: [Service Level Reporting](#)
- SAP Note: [1040343 - SAP EarlyWatch Alert](#) [SAP 포털 액세스 권한 필요]
- SAP Note: [1829914 - EWA Reports 사용자 지정](#) [SAP 포털 액세스 권한 필요]

제안 사항 16.3.2 – 추세 식별을 위해 과거 데이터를 보존

시스템 동작의 추세를 이해하려면 미리 결정된 기간 동안 성능 데이터 및 관련 로그를 보존해야 합니다. 모든 SAP 시스템의 성능 튜닝은 일, 주, 월 단위의 과거 기간 동안 성능 추세 또는 주기적 성능 이벤트를 구성하는 요소를 이해하는 능력에 좌우됩니다. 성능 영향을 관찰하기 위해 데이터를 보존해야 하는 일반적인 이벤트는 다음과 같습니다.

- 월말 및 연말 재무 처리
- 비즈니스 이정표 부근에서 보고 요구 사항 증가(예: 대규모 반기 세일 시작 후)
- 비즈니스 내에서 대규모로 신규 SAP 사용자 온보딩
- 인프라 크기 조정, 데이터베이스 패치, 운영 체제 버전 업데이트 또는 SAP 소프트웨어 업그레이드와 같은 기술 변경

모범 사례 16.4 - 성능 문제 식별 및 해결

주요 지표가 성능 저하를 나타내는 경우 근본 원인을 해결하기 위한 프로세스를 수립합니다. 자동화(동적 크기 조정에 대한 다음 모범 사례 참조)를 사용하면 수동 개입의 필요성을 줄일 수 있습니다. 그러나 이것이 불가능한 경우 관리자를 위한 자동화된 경고 프로세스가 필수적입니다.

제안 사항 16.4.1 – 성능 경고를 적절히 구성

Well-Architected Framework 성능 효율성 원칙에 언급된 모니터링 및 경고에 관한 지침을 따르고 추가 기능을 제공하는 SAP 경고 기능을 활용합니다. [운영 우수성] [1 - 상태를 이해하고 대응할 수 있도록 SAP 워크로드를 설계](#) 에서도 추가 세부 정보를 확인할 수 있습니다.

- Well-Architected Framework [성능 효율성]: [모니터링](#)
- SAP 설명서: [SAP NetWeaver Alert Monitor](#)

제안 사항 16.4.2 – 성능 인시던트의 자동 수정

성능 인시던트 관리에는 Well-Architected Framework 운영 우수성 원칙에 자세히 설명된 운영 관련 모범 사례가 포함되지만 잠재적인 성능 저하를 사전에 감지하고 자동으로 수정하면 성능 문제 악화를 방지하고 최종 사용자 경험을 개선할 수 있습니다. 성능 문제를 완화하기 위한 자동화된 프로세스가 불가능한 경우 운영 팀이 성능 문제에 대응하는 방법을 자세히 규정한 런북을 작성하면 성능 인시던트에 대한 대응을 가속화할 수 있습니다.

- SAP Lens [운영 우수성]: [모범 사례 1.8 - 자동 응답 및 복구 기술을 사용하여 모니터링 경고에 대응](#)
- Well-Architected Framework [운영 우수성]: [모범 사례: 운영](#)

모범 사례 16.5 - 크기 조정을 통해 성능 요구 충족

AWS에서 워크로드를 운영하는 주요 이점 중 하나는 사용 사례에 요구되는 성능에 맞게 컴퓨팅 용량을 늘리거나 줄일 수 있고 스토리지 성능 특성을 변경할 수 있다는 것입니다. SAP 워크로드의 경우 성능 병목 현상을 방지하기 위해 해당되는 경우 동적 크기 조정을 사용합니다. SAP HANA 데이터베이스 클러스터 확장과 같이 동적 확장이 불가능한 시나리오에서는 수동 배포 프로세스를 사용합니다.

제안 사항 16.5.1 – 사후 대응식으로 SAP 워크로드 크기를 조정

워크로드 성능 요구 사항의 동적 변화에 대응하여 적절히 SAP 리소스의 크기를 조정합니다. 가능한 경우 자동화를 사용하여 확장 또는 축소하되, 이것이 가능하지 않은 경우(예: 데이터베이스 인스턴스 확장) 수동으로 수행할 수 있는 프로세스를 수립합니다. 고려 사항:

- 요구를 충족하기 위해 필요에 따라 애플리케이션 서버 용량 추가/제거 또는 인스턴스 크기 변경
- 프로그래밍 방식으로 가상 리소스를 재배포하도록 SAP 파라미터를 변경
- [해당되는 경우 AWS에서 스토리지 유형을 수정하여](#) (예: Amazon EBS gp3 을 io2 로 또는 그 반대로) 스토리지 성능을 최적화

제안 사항 16.5.2 – SAP 워크로드를 예측 가능하도록 크기 조정을 예약

자동 방식이든 수동 방식이든 예측 가능한 성능 패턴을 기반으로 SAP 워크로드를 확장 또는 축소하는 것이 좋습니다. 예를 들어 SAP ECC 시스템에서 월말 재무 처리로 인해 애플리케이션 서버 인스턴스의 처리 요구 사항이 예측 가능한 수준으로 20% 증가하는 경우 시스템 관리자는 사전에 애플리케이션 서버의 수 또는 크기를 늘렸다가 예측 가능한 수준으로 사용량이 감소하면 인스턴스를 축소할 수 있습니다.

모범 사례 16.6 - 분석을 위해 프로덕션 로드 시뮬레이션 메커니즘 개발

테스트 시스템에 프로덕션 데이터를 복제하면 시스템 관리자는 프로덕션 SAP 워크로드를 시뮬레이션하고 스트레스 및 볼륨 테스트와 같은 중요한 성능 테스트를 수행할 수 있습니다. 이러한 유형의 테스트는 잠재적인 성능 병목 현상을 식별하고 실제 프로덕션 환경에서 발생하는 성능 문제를 방지하는 데 도움이 될 수 있습니다.

제안 사항 16.6.1 – SAP 시스템에서 자동화된 스트레스 및 볼륨 테스트를 수행

AWS에서 실행하는 프로덕션 데이터를 테스트 환경에 복사하는 것은 비교적 쉽습니다(예를 들어 [프로덕션 환경의 EBS 스냅샷](#) 을 사용하여 새 테스트 인스턴스를 생성). 그러나 수동 또는 자동 복사 후 단계를 올바르게 수행하려면 주의가 필요합니다. 이러한 복사 후 단계에는 트랜잭션 BDLS를 통한 논리적 시스템 이름 변경, 민감한 프로덕션 데이터 스크램블링 또는 삭제, 관련 테스트 시스템에 대한 통합 설정이 포함될 수 있습니다. 또 다른 추가 이점은 이러한 격리된 성능 테스트 시스템이 영구적일 필요가 없다는 것입니다. 필요에 따라 인스턴스를 프로비저닝, 구성 및 종료할 수 있기 때문입니다.

그런 다음 여러 방법으로 테스트 시스템에 로드를 부과할 수 있습니다.

- AWS에서는 [분산 로드 테스트](#) 솔루션이 자동화된 로드 테스트를 위한 유용한 옵션일 수 있습니다.
- SAP 소프트웨어에서 [eCATT\(Extended Computer Aided Test Tool\)](#)를 통해 [스크립트 생성 및 자동화](#)
- 서드 파티 자동 테스트 솔루션을 사용
- 운영 체제 수준에서 스크립트를 작성하여 SAP 시스템 내에서 적절한 프로그램을 대규모로 시작

모범 사례 16.7 - 성능 데이터를 기반으로 크기 조정 및 구성을 지속적으로 최적화

사고 대응 프로세스 외부에서 정기적으로 성과 지표를 검토합니다. 이렇게 하면 너무 작거나, 너무 크거나, 더 이상 사용되지 않는 시스템 구성 요소를 찾을 수 있습니다. 실제 사용자 로드에서 적절하게 시스템 구성 요소의 크기를 조정하는 데 중점을 두고 SAP 워크로드에 대한 성능 최적화 주기를 설정해야 합니다. 이 활동은 사용자 경험을 개선하고 아키텍처에서 불필요한 부분을 제거하며 워크로드의 비용 효율성 및 복원력을 모두 개선하는 데 도움이 됩니다.

제안 사항 16.7.1 – 과거 성능 지표를 가이드로 사용하여 정기적으로 아키텍처 크기를 적절하게 조정

구성 요소의 규모를 적절하게 조정할 수 있는 기회를 위해 정기적으로 SAP 워크로드를 검토합니다. 비즈니스 성능 요구 사항에 더 잘 부합하도록 스토리지, 컴퓨팅, 네트워크 및 지원 서비스를 확장 또는 축소해야 하는지 여부를 고려합니다.

자세한 내용은 다음 리소스를 참조하세요.

- SAP Lens [비용 최적화]: [모범 사례 20.5 - 최적화 기회를 위해 사용량을 검토](#)
- SAP Lens [운영 우수성]: [모범 사례 4.4 - 주기적 워크로드 검토를 수행하여 복원력, 성능, 민첩성 및 비용 최적화](#)
- AWS 설명서: [적절한 규모 결정](#)

비용 최적화

비용 최적화 원칙에는 전체 수명 주기 동안 시스템을 개선하고 구체화하는 지속적인 프로세스가 포함됩니다. 이 최적화는 최초 개념 증명 설계부터 프로덕션 워크로드 운영까지 지속되어야 합니다. 올바른 솔루션 및 가격 책정 모델을 선택한 다음 비즈니스 성과를 달성하고 비용을 최소화할 수 있는 비용 인식 시스템을 구축합니다. 시간이 지남에 따라 비용 최적화를 실현하려면 삭제 또는 축소할 수 있는 데이터, 인프라 리소스 또는 분석 작업을 식별해야 합니다.

17 – SAP 아키텍처 패턴에서 비용 효율성 평가

SAP 아키텍처 패턴 평가에 비용 고려 사항을 어떻게 통합합니까? 아키텍처에 대한 결정을 내릴 때 설계 고려 사항의 일부로 비용 영향을 완전히 이해해야 합니다.

ID	우선순위	모범 사례
□ BP 17.1	필수	SAP 관리형 서비스 제품 사용 평가
□ BP 17.2	필수	SAP 애플리케이션 아키텍처 패턴의 비용 특성 평가
□ BP 17.3	필수	환경별로 비용 최적화된 설계 결정을 내리기 위한 비즈니스 요구 사항 이해
□ BP 17.4	적극 권장	SAP 구성 요소에 대한 크기, 세분 수준 및 사용 가능한 최신 EC2 인스턴스 선택 검토
□ BP 17.5	적극 권장	비용 효율성을 개선하기 위해 온디맨드 용량 사용을 고려
□ BP 17.6	권장	공유 서비스 및 솔루션의 비용 이점과 영향 평가

ID	우선순위	모범 사례
□ BP 17.7	권장	자동화의 비용 이점 평가

모범 사례 17.1 - SAP 관리형 서비스 제품 사용 평가

AWS 공동 책임 모델에 따라 SAP on AWS 워크로드를 관리할 책임은 고객에게 있습니다. 선택적으로 서비스 공급 업체를 사용하여 SAP on AWS 워크로드를 관리할 수 있습니다. 서비스 공급 업체를 평가할 때 선행 및 지속적인 비용 관리에 대한 책임이 적절히 위임되어야 하고 지속적인 프로세스로 처리되어야 합니다.

여러 AWS 파트너가 SAP 환경 배포 및 운영을 위한 서비스를 제공합니다. 제공하는 서비스의 범위 및 성숙도는 파트너에 따라 다릅니다. 이러한 유형의 서비스는 예를 들어 중앙 집중식 지원 또는 자동화된 배포 서비스와 같이 효율성을 제공할 수 있습니다. 이러한 서비스는 전체 비용을 절감할 수 있으며 특정 비즈니스 요구 사항에 따라 평가해야 합니다. 파트너에 대해 [SAP 컨설팅 컴피턴시](#) 및 AWS 파트너 네트워크(APN) 등 AWS 컴피턴시를 평가합니다.

제안 사항 17.1.1 – 비용 관리와 관련된 역할 및 책임을 이해

관리형 서비스 제품마다 인프라, 라이선싱 및 서비스 비용 모델이 다릅니다. 비용 관리 책임이 어디에 있는지 결정합니다. 이 과정에서 다음과 같은 질문을 할 수 있습니다.

- 공급 업체 비용이
 - 인프라 지출의 백분율을 기준으로 합니까?
 - 합의된 총 소유 비용(TCO)을 기준으로 합니까?
- 크게 3단계(소규모, 중규모, 대규모)로 구분됩니까? 비용을 제어하고 이해할 수 있도록 적절한 변경 제어 프로세스가 마련되어 있습니까?
- 인프라 비용의 가시성 및 투명성이 충분합니까?
- 비용 거버넌스가 혁신과 유연성을 제한합니까?

제안 사항 17.1.2 – 모든 당사자와 비용 관리 및 최적화 접근 방식에 동의

사용 가능한 다양한 관리형 서비스 제품을 평가할 때 관리형 서비스 파트너의 비용 관리 접근 방식을 이해합니다. 조직의 지속적인 비용 최적화를 위해 어떻게 협력할 수 있습니까?

이 평가에는 주기적 검토 프로세스가 포함되어야 합니다. 또한 양쪽 당사자가 모두 재정적 이익을 얻을 수 있도록 파트너가 소유권을 갖도록 장려하는 공유 보상 모델과 같은 인센티브의 혜택을 받을 수 있습니다.

모범 사례 17.2 - SAP 애플리케이션 아키텍처 패턴의 비용 특성 평가

SAP 환경의 아키텍처를 개발할 때 인프라 구성 요소의 크기 및 위치 외에 구성 요소 수에 따른 비용도 고려합니다. 솔루션의 비즈니스 요구 사항을 설정하고, 위험 및 최적화 기회를 인식함으로써 상당한 비용 절감을 실현할 수 있습니다.

제안 사항 17.2.1 – 선택한 SAP 설치 패턴을 검토

각 SAP 애플리케이션에 대해 독립 실행형, 분산형 또는 고가용성(HA)과 같은 배포 패턴을 정의합니다. 비즈니스 요구 사항을 충족하기 위해 비용 및 안정성 특성이 최적의 균형을 이룬 아키텍처 패턴을 선택합니다. 유용한 접근 방식 하나는 비즈니스 중단 비용을 수량화한 후 거슬러 올라가며 작업하는 것입니다. 가용성에 영향을 미치는 개별 장애의 위험과 해당 위험을 축소하는 비용의 균형을 맞춥니다.

또한 아키텍처에 적절한 크기 조정이 가능한 유연성이 있는지 확인합니다. 운영 체제 라이선싱, 스토리지, 단일 호스트에서 여러 애플리케이션 서버 관리를 통해 비용을 절감할 수 있습니다. 애플리케이션 계층의 경우 지원되는 인스턴스 패밀리에서 CPU 및 메모리를 미세 단위로 지정한(가격은 거의 정비례) 인스턴스 크기를 사용할 수 있습니다. 더 작은 규모의 여러 인스턴스를 배포하면 인스턴스 재사용 및 워크로드 기반 크기 조정에 대한 옵션을 사용할 수 있습니다.

논리적 그룹화를 평가하고 구성 요소, 시스템(SID) 또는 환경을 결합하는 효과를 고려합니다. 이러한 활동으로 인해 운영 복잡성이 증가하고 안정성이 감소합니까?

- AWS 설명서: [Architecture Guidance for Availability and Reliability of SAP on AWS\(SAP on AWS의 가용성 및 안정성을 위한 아키텍처 지침\)](#)
- SAP Lens [안정성]: [안정성 설계 원칙](#)
- AWS Well-Architected Framework [안정성]: [안정성 원칙](#)

제안 사항 17.2.2 – 멀티 테넌시 사용 또는 단일 호스트에서 다중 데이터베이스 호스팅에 대한 예외를 평가

대부분의 데이터베이스에서 각 시스템의 크기를 독립적으로 조정하고 해당 시스템의 요구 사항에 맞게 유연한 인스턴스 크기 조정을 활용합니다. 경우에 따라 해당 권장 사항에서 벗어나는 것이 비용 측면에서 합리적일 수 있습니다. 예를 들면 다음과 같습니다.

- HANA 기반 구성 요소에 사용 가능한 최소 EC2 인스턴스 크기보다 적은 메모리가 필요한 경우 [SAP HANA 멀티 테넌트 데이터베이스 컨테이너](#)를 사용하는 것을 고려합니다. 컴퓨팅 리소스를 다른 구성 요소와 함께 호스트하면 효율적으로 사용할 수 있습니다.
- Oracle 및 SQL Server를 포함한 관계형 데이터베이스용 코어 기반 데이터베이스 라이선싱 모델
- 가동 시간 요구 사항 및 버전 종속성을 위해 밀결합되었거나 밀결합될 수 있는 애플리케이션. 여기에는 관리 도구(예: Solution Manager 및 SAP HANA Cockpit)와 일부 SAP NetWeaver Gateway 배포 옵션(Fiori 및 ECC)이 포함됩니다.

제안 사항 17.2.3 – 복원력 및 확장성이 필요하지 않은 시스템에 대한 단일 호스트 설치 패턴의 사용을 평가

개별 애플리케이션 또는 환경의 경우 단일 호스트 모델의 장점을 고려해야 합니다. 이를 통해 운영 체제 비용, 스토리지 복제, 소프트웨어 라이선스 비용 및 관리 서비스 비용을 절감할 수 있습니다. 특히 비프로덕션 환경에 대한 일반적인 아키텍처 옵션은 다음과 같습니다.

- 데이터베이스, 애플리케이션 및 SAP 중앙 서비스를 공동 호스팅
- 데이터베이스를 분리(데이터베이스 라이선싱을 최소화하기 위해). 자세한 내용은 [비용 최적화]: [모범 사례 18.3 - 라이선싱 영향 및 최적화 옵션 평가](#)를 참조하세요.
- 애플리케이션과 SAP 중앙 서비스를 결합

제안 사항 17.2.4 – 가장 비용 효율적으로 요구 사항을 충족하는 리전을 선택

SAP 리전의 주요 선택 기준은 근접성, 데이터 상주 및 서비스 가용성입니다. 리전을 선택할 수 있는 배포의 경우 각 AWS 리전은 현지 시장 상황에 따라 가격이 책정되며, 따라서 AWS 서비스 가격이 리전마다 다르다는 점을 인식해야 합니다. 가격 차이와 잠재적 영향을 검토합니다.

제안 사항 17.2.5 – 장애 발생 시 크기를 조정할 수 있는 아키텍처를 사용

클라우드에서는 복구 메커니즘과 탄력성 덕분에 이중화 리소스를 활성화할 필요 없이 100% 용량으로 설계가 가능합니다. 비즈니스 요구 사항에 따라 보다 유연한 RTO 또는 RPO가 허용되는 경우 다음을 고려합니다.

데이터베이스:

- 복구 지점 목표에서 허용하는 경우 프라이머리 데이터베이스 노드의 변경 사항을 적용하기 위해 동등한 컴퓨팅 용량이 필요하지 않은 세컨더리 또는 스탠바이 데이터베이스 노드를 고려합니다. 복구 시간 영향을 감안하여, 세컨더리 데이터베이스에 더 작거나 공유된 인스턴스를 배포하고 필요할 때

만 확장할 경우의 비용 이점을 고려합니다. 더 작은 인스턴스를 사용하면 기본 시스템 인스턴스와 보조 시스템 인스턴스 간에 1:1 관계가 유지됩니다. 공유 인스턴스 아키텍처는 복제되지 않는 시스템 데이터베이스가 있는 세컨더리 데이터베이스를 단일 인스턴스로 풀링합니다. 장애 발생 시 복제되지 않는 시스템을 중지해야 전환이 가능합니다. 그러면 RTO가 증가합니다.

- 세컨더리 SAP HANA 데이터베이스에 더 작은 인스턴스를 사용하는 경우 스탠바이의 더 작은 메모리 공간을 수용하고 비용을 절감하기 위해 메모리 미리 로드를 끕니다. SAP 도움말 문서 [Secondary System Usage\(보조 시스템 사용량\)](#)에 메모리 요구 사항이 추정되어 있습니다.
 - SUSE 설명서: [SAP HANA 시스템 복제 크기 조정 - 성능 최적화 시나리오 | SUSE](#)
- 복구 시간 목표 및 복원력 요구 사항에서 허용하는 경우 다중 AZ 스토리지(예: Amazon FSx, Amazon EFS 또는 Amazon S3)를 사용하는 데이터 및 로그 백업 접근 방식을 고려합니다. 이러한 접근 방식을 사용하면 이중화 보조 리소스 없이 데이터를 지리적으로 보호할 수 있습니다. 장애가 발생한 경우 온디맨드로 보조 리소스를 생성하고 교차 위치 백업 및 로그 스토리지에서 신속하게 복원할 수 있습니다.
 - SAP on AWS 블로그: [스냅샷을 사용하여 SAP ASE 데이터베이스용 자동 복구 절차를 생성하는 방법](#)

애플리케이션:

- [AWS 인스턴스 복구](#) 는 CloudWatch 경보를 사용하여 Amazon EC2 인스턴스를 모니터링합니다. 기본 하드웨어 장애로 인해 인스턴스가 손상된 경우 자동으로 인스턴스를 복구합니다. 해당 장애 시나리오가 충분한 보호를 제공하는지 평가합니다.
- 애플리케이션 서버를 신속하게 재생성해야 하는 시나리오의 경우 옵션으로는 프로비저닝되었지만 실행되지 않는 EC2 인스턴스, 템플릿 AMI, 공통 스테이징 서버를 사용하는 스토리지 복제, 코드형 인프라(IaC) 등이 있습니다.

제안 사항 17.2.6 – 장애 발생 시 컴퓨팅 용량 최소 비용을 고려

여러 가용 영역에 SAP 구성 요소를 분산하면 장애 발생 시 용량 예약에 발생하는 비용을 절감할 수 있습니다. 여러 가용 영역에 구성 요소를 분산하면 워크로드의 일부가 이미 지리적으로 분산되어 있으므로 초과 용량이 필요하지 않습니다. 이는 AZ 장애 발생 시 영향 범위를 최소화합니다.

예를 들어 가용 영역 손실이 포함된 장애 시나리오에 대한 가용성 요구 사항이 100% 용량인 경우 두 개의 가용 영역에 200% 용량을 프로비저닝하는 대신 세 개의 가용 영역에 150% 용량을 프로비저닝합니다.

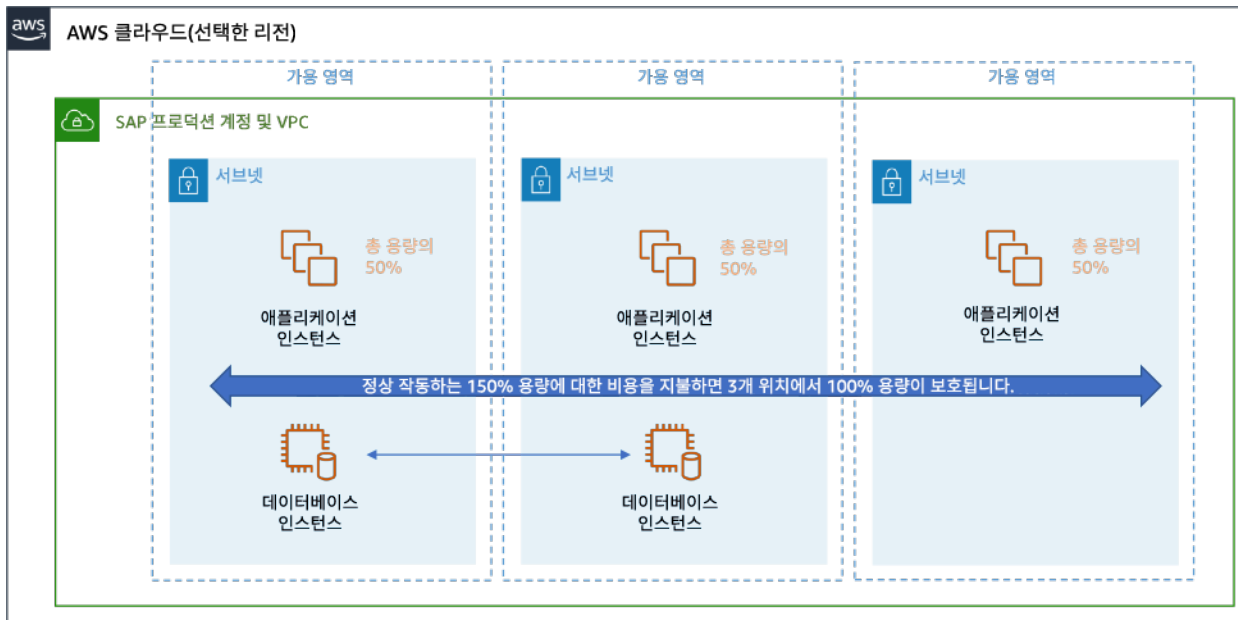


그림: 정상 작동 중인 150% 용량의 3개 가용 영역 아키텍처의 예

제안 사항 17.2.7 – 스토리지만 기반으로 하는 복구 옵션 사용을 평가

일반적으로 AWS에서는 가장 광범위한 장애 시나리오로부터 보호하기 위해 스토리지 복제보다 데이터베이스 복제를 권장합니다. 애플리케이션 계층 또는 덜 중요한 인스턴스의 경우 컴퓨팅 필요 없이 스토리지 복제를 사용하는 DR 솔루션을 사용하면 비용을 절감할 수 있습니다. 또한 변경 사항 관리와 관련된 복잡성도 최소화됩니다.

- AWS 설명서: [CloudEndure 재해 복구 - Amazon Web Services](#)
- SAP 설명서: [SAP 애플리케이션의 CloudEndure Disaster Recovery](#)
- AWS 설명서: [자동 백업을 다른 AWS 리전에 복제 - Amazon Relational Database Service\(Amazon RDS\)](#)

제안 사항 17.2.8 – 네트워킹 관련 비용을 이해

SAP 고객은 온프레미스 네트워크와 Amazon VPC 간의 보안 연결이 필요한 경우가 많습니다. 적절한 크기로 조정된 Direct Connect, VPN 연결 또는 둘 다를 사용하면 비용을 최소화하면서 성능 및 안정성 요구 사항을 충족할 수 있습니다.

데이터 전송 비용은 리전, VPC 및 가용 영역 설계의 영향을 받습니다. 안정성 저하 없이 SAP 구성 요소의 배포 및 복제를 최적화할 수 있는 방법을 평가합니다.

예를 들어 대량의 데이터를 전송하는 두 시스템이 서로 다른 위치에 있는 경우 데이터 전송 비용에 미치는 영향을 고려해야 합니다.

- AWS 설명서: [EC2 온디맨드 인스턴스 요금 – Amazon Web Services](#)
- AWS 설명서: [아키텍처 패턴 - 일반 SAP 가이드](#)

추가 지침은 Well-Architected Framework 검토의 비용 원칙에서 찾을 수 있습니다 ([Plan for Data Transfer - Cost Optimization Pillar\(데이터 전송 계획 - 비용 최적화 원칙\) 참조](#)).

모범 사례 17.3 - 환경별로 비용 최적화된 설계 결정을 내리기 위한 비즈니스 요구 사항 이해

각 시스템 또는 환경의 비용을 각기 다른 특성에 따라 개별적으로 최적화합니다. 비즈니스 요구 사항에 부합하는 용량, 성능, 안정성 및 운영 시간을 고려합니다. 최종 사용자의 경험이나 비즈니스 프로세스에 덜 중요한 환경 또는 애플리케이션의 경우 스토리지, 컴퓨팅 및 운영 시간을 최소화하여 비용을 절감합니다. 구성 축소에 따른 비용 절감과 테스트 또는 지원을 위한 운영 요구 사항 간의 균형을 유지합니다.

제안 사항 17.3.1 – 비프로덕션 환경에 프로덕션 데이터의 전체 복사본이 필요한지 평가

비프로덕션에 프로덕션 데이터의 전체 복사본을 유지하면 스토리지 및 컴퓨팅 비용에 큰 영향을 미칩니다. 테스트 요구 사항을 계속 충족하면서 프로덕션 데이터의 복사본 수를 최소화하는 것을 고려합니다. 비프로덕션 환경 데이터 스토리지의 비용을 최소화하기 위한 옵션은 다음과 같습니다.

- 개발 및 테스트 시스템에 더 적은 스토리지 용량을 사용합니다.
- 데이터 슬라이싱 도구를 사용하여 비프로덕션 시스템에서 테스트 데이터를 더 작은 하위 집합으로 분할합니다.
- 임시 프로덕션 사본의 사용을 고려합니다. 이러한 복사본은 온디맨드로 생성한 다음 비즈니스 요구 사항 또는 테스트가 통과한 후 신속하게 폐기 또는 아카이브할 수 있습니다.
- 비프로덕션 시스템에서 SAP HANA 데이터베이스에 대한 SAP 권장 사항인 50% 작업 메모리가 필요한지 평가합니다.

제안 사항 17.3.2 – 비프로덕션 환경에 항상 프로덕션 환경과 동일한 성능이 필요한지 평가

비프로덕션 시스템 및 일부 지원 시스템은 사용자 집합이 작거나, 훨씬 적은 트랜잭션 볼륨을 처리하거나, 유연한 응답 시간 요구 사항이 있을 수 있습니다. 다음 사항을 고려하세요.

- 더 작은 EC2 인스턴스 유형을 사용하여 워크로드에 대한 SAP 애플리케이션 성능 표준(SAPS)을 낮춥니다.
- 더 적은 수의 애플리케이션 서버를 사용합니다.

- 더 저렴한 Amazon EBS 스토리지 유형을 사용합니다(예: io2 대신 gp3).
- 비프로덕션 시스템 볼륨에 감소된 성능 특성을 사용합니다(예: 10,000 IOPS 대신 3,000 IOPS).
- 클라우드의 탄력성 덕분에 로드 또는 크기 조정 테스트와 같이 프로덕션과 유사한 성능이 필요한 비프로덕션 테스트 리소스를 확장할 수 있습니다.

제안 사항 17.3.3 – 비프로덕션 환경에 프로덕션 환경과 동일한 운영 시간이 필요한지 평가

테스트, 교육 및 샌드박스 시스템과 같은 비프로덕션 환경은 프로덕션에 비해 운영 시간이 짧을 수 있습니다. 표준 시간대와 지원 팀 근무 시간을 고려하여 모든 시스템이 연중무휴 24시간 필요한지 여부를 결정합니다. 이 정보를 사용하여 가장 저렴한 가격 모델을 선택합니다.

예를 들어 온디맨드 요금 모델(약 23% 가동 시간)을 사용하여 주당 40시간 동안 SAP 교육 시스템을 실행하는 것이 3년 예약 인스턴스 또는 Savings Plan을 사용하여 100%로 상시 실행하는 것보다 저렴합니다.

제안 사항 17.3.4 – 비프로덕션 환경에 프로덕션 환경과 동일한 안정성이 일관되게 필요한지 평가

각 시스템의 개별 안정성 요구 사항에 부합하는 가장 비용 효율적인 아키텍처를 선택합니다. [안정성]: [모범 사례 10.1 - 비즈니스 요구 사항에 부합하는 SAP 워크로드 가용성 목표에 합의](#) 를 참조하세요. 추가 지침은 AWS Well-Architected Framework의 [안정성 원칙](#) 에서 찾을 수 있습니다.

프로덕션 환경과 유사한 아키텍처가 테스트 전용으로 존재하는 경우 프로덕션을 미러링해야 하는 빈도를 고려합니다. 비프로덕션 환경에서 안정성 또는 성능 테스트를 위해 데이터베이스 고가용성이 필요한 경우 이러한 테스트 기간 외에 보조 인스턴스를 종료하거나 축소하여 비용을 절감할 수 있습니다.

자동화를 사용하고 항상 프로덕션과 같은 성능이 필요하지 않은 환경에 대해 온디맨드 요금을 사용하여 비용 이점을 실현할 수 있습니다.

제안 사항 17.3.5 – 지원 및 레거시 시스템을 포함한 비핵심 시스템의 비즈니스 요구 사항을 평가

환경이 참조용으로만 존재하거나 비즈니스 역할이 덜 중요한 경우 핵심 프로덕션 시스템과 비교하여 필요한 가동 시간, 성능 및 안정성 요구 사항을 평가합니다.

예를 들어 레거시 ERP 시스템은 이전 애플리케이션 전환 또는 비즈니스 구조 조정에서 참조용으로 유지해야 할 수 있습니다. 이 시스템의 비용은 필요할 때만 EC2 인스턴스를 실행하고 Amazon EBS 스토리지에 대해서만 비용을 지불하여 최적화할 수 있습니다. 보다 비용 효율적인 솔루션은 Amazon S3 및 Amazon S3 Glacier로 백업을 통해 시스템을 아카이브하는 것입니다.

모범 사례 17.4 - SAP 구성 요소에 대한 크기, 세분 수준 및 사용 가능한 최신 EC2 인스턴스 검토

더 작은 EC2 인스턴스가 SAP 워크로드에서 비용 유연성이 더 큽니다. 컴퓨팅을 사용하지 않을 때 종료하거나 피크 로드 중에만 확장할 수 있는 수평 확장 옵션을 제공하기 때문입니다. 애플리케이션 계층에서 일관된 EC2 인스턴스 크기를 채택하면 모든 워크로드에서 예약 인스턴스 및 Savings Plans 약정의 이점을 극대화하는 데 도움이 됩니다. 사용 가능한 최신 AWS SAP 인증 인스턴스를 고려합니다. 각 구성 요소에 대한 운영 영향, 라이선스 비용, 지원, 공유 및 재사용 가능성도 평가해야 합니다.

제안 사항 17.4.1 – 유연성을 제공하기 위해 더 작은 애플리케이션 서버를 여러 개 배포하는 경우의 비용 이점을 평가

많은 SAP 워크로드의 경우 애플리케이션 서버를 변경할 수 없도록 설계할 수 있습니다. 기본 유닛을 복제하여 수평으로 확장되는 표준 애플리케이션 서버 구성이 있으면 일관된 반복 가능한 유닛에 대한 옵션이 확보됩니다. 장점에는 재사용 가능성, 컴퓨팅 사용률, 예약 및 자동화가 있습니다. 운영 체제 라이선싱, 스토리지 복제 및 관리 비용과 같은 유닛별 요구 사항을 평가에 고려해야 합니다.

다음 사항을 고려하세요.

- SAP on AWS 블로그: [DevOps for SAP – Driving Innovation and Lowering Costs\(SAP용 DevOps - 혁신을 촉진하고 비용을 절감\)](#).
- SAP on AWS 블로그: [AWS를 사용하여 SAP Application Auto Scaling 활성화](#)

제안 사항 17.4.2 - 지원되는 경우 SAP HANA 스케일 아웃 구성의 비용 이점을 평가

SAP OLAP 워크로드는 [스케일 업 및 스케일 아웃](#) 구성 모두에서 배포할 수 있습니다. SAP는 운영 복잡성을 줄이기 위해 스케일 아웃 전에 스케일 업할 것을 권장합니다. 하지만 스케일 아웃 구현은 상당한 컴퓨팅(SAPS)이 필요한 대규모 분석 또는 네이티브 SAP HANA 워크로드에 적용될 수 있습니다.

일부 경우에는 S/4HANA가 스케일 아웃 구성도 지원하지만 제한 사항이 있습니다. 다음 SAP Note를 참조하세요. [2408419 - SAP S/4HANA - Multi-Node Support](#) [SAP 포털 액세스 권한 필요].

스케일 업과 스케일 아웃을 비교할 때 다음을 고려하세요.

- [인증 EC2 인스턴스 크기](#) (스케일 업 및 스케일 아웃에 사용 가능)
- 각 인스턴스 패밀리의 EC2 메모리 GiB당 비용. 큰 EC2 인스턴스는 일반적으로 작은 인스턴스보다 GiB당 비용이 더 높습니다.
- 스케일 아웃 배포에서 가중되는 데이터 배포 관리의 복잡성 및 운영 오버헤드. 다음 SAP Note를 참조하세요. [2081591 - FAQ: SAP HANA Table Distribution](#) [SAP 포털 액세스 권한 필요]

모범 사례 17.5 - 비용 효율성을 개선하기 위해 온디맨드 용량 사용을 고려

온디맨드 요금 모델은 단축된 운영 시간, 단기 프로젝트, 실험 또는 단기간의 용량 확장(예: 성능 테스트)이 필요한 SAP 워크로드에 적합합니다. SAP 아키텍처에서 온디맨드 요금을 사용할 수 있는 영역을 결정합니다.

제안 사항 17.5.1 – 연중무휴 24시간 운영 시간이 필요하지 않은 SAP 시스템에 온디맨드 사용을 평가

온디맨드 요금 모델과 다른 요금 모델 간의 손익분기점을 기반으로 ([안정성]: [모범 사례 18.1 - Amazon EC2에 사용할 수 있는 결제 및 약정 옵션 이해](#) 참조) 온디맨드가 최저 비용을 제공하는지 평가합니다. 이 평가의 일환으로 전체 Savings Plan 약정을 고려합니다.

일반적인 사용 사례에는 시험 업그레이드 및 개념 증명(POC)과 같이 연장된 업무 시간 또는 단기 비즈니스 실험 외에는 필요하지 않은 비프로덕션 시스템이 포함됩니다.

- SAP on AWS 블로그: [AWS Systems Manager를 사용하여 분산 SAP HANA 시스템 자동 시작 또는 중지](#)

제안 사항 17.5.2 - 피크 로드와 대한 예약 또는 동적 크기 조정 옵션을 평가

온디맨드 용량은 SAP 워크로드에서 일반적으로 짧은 기간 동안 용량 요구 사항이 급증하는 피크에 사용됩니다. 다음 사항을 고려하세요.

- 기간, 월말, 연말 또는 계절성 피크와 같은 알려진 사용량 패턴 피크에 대해 일정 기반 SAP 애플리케이션 서버 크기 조정을 사용합니다.
- 피크가 확실하지 않고 실시간 사용자 로드를 기반으로 크기를 조정해야 하는 경우 애플리케이션 계층 동적 크기 조정을 사용합니다. SAP를 인식하고 필요한 거버넌스 및 제어를 제공하는 메커니즘을 탐색합니다.

참고: 애플리케이션 계층 동적 크기 조정을 평가할 때 SAP 구성 요소의 상태 유지 특성으로 인해 SAP 애플리케이션 서버가 종료되는 경우 사용자 연결 및 배치 작업에 미치는 영향을 고려하세요. AWS, SAP 및 APN 파트너 개발 도구가 이 요구 사항을 해결하는 데 도움이 될 수 있습니다.

- AWS 설명서: [Systems Manager Automation 작업 참조](#)
- SAP 설명서: [SAP Landscape Management](#)
- SAP on AWS 블로그: [AWS를 사용하여 SAP Application Auto Scaling 활성화](#)

모범 사례 17.6 - 공유 서비스 및 솔루션의 비용 이점과 영향 평가

여러 SAP 시스템에 동일한 기능이 필요한 경우 기존 솔루션을 사용하거나, 구성 요소를 공유하거나, 둘 다 사용하여 관리 및 비용을 중앙 집중화하는 것이 비용 효율적 옵션이 될 수 있습니다. 모니터링, 백업 및 연결은 AWS 계정 경계 내에서 또는 전용 계정에서 관리할 수 있는 일반적인 기능입니다. 표준화, 중복 감소, 복잡성 감소는 비용을 낮춥니다.

비용 절감을 위해 리소스를 공유하면서도 적절한 격리를 유지하고 운영에 영향을 미칠 수 있는 종속성이 부과되지 않는 적절한 방법을 모색합니다.

제안 사항 17.6.1 – 각 공유 서비스에 대해 일대일 설정과 일대다 설정의 비용 이점을 비교

SAP 환경의 표준 패턴은 다중 계정 전략의 일부로 비프로덕션 워크로드와 프로덕션 워크로드를 별도의 계정으로 분리하는 것입니다. 이것은 일부 서비스에서 논리적 경계가 될 수 있습니다. 세분화를 적용하는 관리 경계 및 리전, AZ, VPC 또는 계정 간의 데이터 전송 비용 영향을 포함하여 각 시나리오의 복잡성과 운영 비용을 고려합니다.

다중 계정 설계에서 일부 AWS 서비스는 비용을 절감하기 위해 중앙에서 호스트하고 허브 앤 스포크 설계의 여러 애플리케이션 및 계정에서 액세스할 수 있습니다. 이러한 서비스에는 다음이 포함됩니다.

- 스포크 VPC의 모든 아웃바운드 트래픽에 대한 NAT 게이트웨이 포함 전용 VPC
- 로드 밸런서 및 웹 디스패처를 위한 중앙 집중식 모델
- 전송 및 기타 파일 공유 필요를 충족하기 위한 공유 Amazon EFS 또는 Amazon FSx

제안 사항 17.6.2 – 기존 서비스를 재사용하여 비용을 절감할 수 있는 영역을 평가

이 제안 사항은 여러 수준에 해당됩니다.

- AWS가 서비스를 제공하는 경우 이러한 서비스는 종종 오버헤드를 최소화하며 사용량 기반 요금제를 사용합니다. 예를 들면 Amazon EFS, AWS Backup for SAP HANA, AWS Backup이 있습니다.
- 비즈니스에는 운영 일관성 및 규모의 경제를 위해 사용해야 하는 일부 기능(예: 엔터프라이즈 백업)에 대한 전사적 표준이 있을 수 있습니다.
- APN 파트너 솔루션은 특정 비즈니스 요구 사항에 따라 AWS Marketplace 또는 BYOL(기존 보유 라이선스 사용)을 통해 제공될 수 있습니다.
- 라이선스 포함 AWS Marketplace 머신 이미지는 선결제 비용을 줄이는 데 도움이 될 수 있습니다. 이 시나리오에서는 라이선스 제한을 고려해야 합니다. 다른 인스턴스 유형으로의 이식성을 제한하여 솔루션 유연성에 영향을 줄 수 있기 때문입니다.

제안 사항 17.6.3 – 자체 구축, 구매 및 오픈 소스 접근 방식 사용의 영향을 이해

AWS 솔루션이든 APN 파트너 솔루션이든 자체 구축, 오픈 소스, 기성품은 정도의 차이가 있습니다. 예로는 백업 솔루션,고가용성(HA) 솔루션 및 공유 스토리지 솔루션이 있습니다.

자체 구축 접근 방식 또는 오픈 소스 솔루션 사용을 고려할 때 다음 사항을 고려해야 합니다.

- 서비스 수준 계약
- 구축 및 유지 관리에 필요한 기술
- 서비스 중단이 비즈니스에 미치는 영향

또한 특정 비즈니스 요구 사항과 각 솔루션이 제공하는 기능을 기반으로 구매하려는 솔루션에 사용 가능한 상용 모델을 평가해야 합니다. 예를 들어 사용 권한 대 사용 건당 요금 지불, 그러한 요금이 계산되는 방식과 같은 상용 모델의 조건을 고려합니다.

모범 사례 17.7 - 자동화의 비용 이점 평가

AWS에서 자동화를 도입함으로써 얻을 수 있는 이점에는 효율성 및 생산성 향상이 포함될 수 있으며, 이는 조직의 비용 절감으로 이어질 수 있습니다.

제안 사항 17.7.1 – 빌드 자동화 효율을 평가

코드형 인프라를 사용한 빌드 프로세스 자동화는 출시 시간 및 생산성을 향상시킬 수 있는 비용 효율성이 있습니다. DevOps 모범 사례가 제공할 수 있는 품질, 일관성, 반복성 및 복구 가능성의 이점은 자동화 개발에 필요한 더 높은 선행 투자와 비교해야 합니다.

AWS Professional Services 또는 AWS 파트너와 협력하면 전문가의 경험을 활용하여 전반적인 노력을 줄일 수 있습니다.

AWS Launch Wizard for SAP는 자동화를 통해 SAP 배포를 가속화할 수 있습니다. SAP 모범 사례에 따라 AWS 기반 SAP HANA 애플리케이션의 크기 조정, 구성 및 배포를 안내하는 서비스입니다. 이 서비스는 무료이고 AWS가 지원을 제공합니다.

- AWS 설명서: [코드형 인프라](#)
- AWS 설명서: [AWS CloudFormation](#)
- SAP on AWS 블로그: [AWS for SAP DevOps](#)

제안 사항 17.7.2 – 운영에 대한 자동화 효율을 평가

AWS 및 서드 파티 도구를 사용하여 운영 실행 및 모니터링을 자동화할 수 있는 방법을 조사하여 반복 가능한 작업의 비용과 수동 작업을 줄입니다. 다음 사항을 고려하세요.

- AWS 서비스: [AWS Systems Manager](#)

추가 지침은 [운영 우수성] [모범 사례 3.6 - 자동화를 사용하여 SAP 환경 작업 수행](#) 을 참조하세요.

18 – 비용 효율성을 위한 SAP 컴퓨팅 리소스 평가

SAP 워크로드에 대한 컴퓨팅 및 스토리지 옵션을 어떻게 평가합니까? SAP를 구현하거나 AWS로 마이그레이션할 때 비용 목표를 충족하기 위해 SAP 워크로드에 대한 비용 효율적인 EC2 인스턴스 및 스토리지 솔루션을 선택해야 합니다.

ID	우선순위	모범 사례
□ BP 18.1	필수	Amazon EC2에 사용할 수 있는 결제 및 약정 옵션 이해
□ BP 18.2	필수	EC2 인스턴스 선택을 위한 주요 고려 사항으로 비용을 사용
□ BP 18.3	적극 권장	라이선싱 영향 및 최적화 옵션 평가
□ BP 18.4	적극 권장	필요한 특성을 기반으로 스토리지 옵션의 비용 영향 평가

모범 사례 18.1 - Amazon EC2에 사용할 수 있는 결제 및 약정 옵션 이해

온디맨드 요금과 비교하여 상당한 할인을 제공하는 예약 인스턴스 및 Savings Plans 사용을 고려합니다. 1년 및 3년 약정 기간과 전체 선결제, 부분 선결제, 선결제 없음의 세 가지 결제 옵션으로 사용할 수 있습니다.

제안 사항 18.1.1 – 요금 모델 간 손익분기점을 이해

[예약 인스턴스](#) 는 표준 예약 인스턴스(온디맨드 요금에서 최대 72% 할인)와 컨버터블 예약 인스턴스(온디맨드 요금에서 최대 54% 할인)로 구분됩니다. [Savings Plans](#) 는 Compute Savings Plans(온디맨드 요금에서 최대 66% 할인)과 EC2 Instance Savings Plans(온디맨드 요금에서 최대 72% 할인)으로 구분됩니다.

Amazon EC2 온디맨드 시간당 요금 대비 실현할 수 있는 할인율은 다음 요인에 따라 달라집니다.

- 선택한 약정 기간
- 선택한 결제 옵션
- 선택한 예약 인스턴스 또는 Savings Plan 유형
- 인스턴스 패밀리

메모리 최적화 인스턴스 패밀리(예: X1 및 X1e)는 약정에 따른 절감 효과가 더 크므로 SAP, 특히 SAP HANA 워크로드의 경우 요금 옵션을 이해하는 것이 중요합니다.

AWS 요금 계산기의 고급 옵션을 사용하여 손익분기점을 계산합니다. 이 계산기에서 사용되는 가정을 알고 있어야 합니다. 이를 설명하기 위해 다음 공식을 사용하여 각 인스턴스 패밀리에 대해 예약 인스턴스 또는 Savings Plan을 사용하는 것이 온디맨드를 사용하는 것보다 낮은 TCO를 제공하는 지점을 계산하는 예를 알아보겠습니다.

$(\text{약정의 유효 시간당 요금} / \text{온디맨드의 시간당 요금}) * 730\text{시간}$

각 [RI 약정 기간과 유형](#) 및 각 [Savings Plan 약정 기간과 유형](#)에 대한 유효 시간당 요금을 참조하세요. 다양한 손익분기점을 보여주는 다음 예를 비교합니다.

예 1: 버지니아 북부(us-east-1)에서 M5 패밀리의 경우 선결제 없는 3년 표준 예약 인스턴스 또는 EC2 Savings Plan이 더 낮은 TCO를 제공하는 손익분기점은 월 315시간(월요일부터 금요일까지 하루 약 16시간)입니다.

예 2: 버지니아 북부(us-east-1)에서 X1 인스턴스 패밀리의 경우 선결제 없는 3년 표준 예약 인스턴스 또는 EC2 Savings Plan이 더 낮은 TCO를 제공하는 손익분기점은 월 235시간(월요일부터 금요일까지 하루 약 12시간)입니다.

포괄적인 지침([비용 관리](#) 및 Well-Architected Framework [비용 최적화 원칙](#))을 사용합니다. 다음 [SAP on AWS 요금 가이드](#)에서도 AWS에서 실행되는 SAP 워크로드와 관련된 지침을 제공합니다. 비용을 분석할 때 모든 AWS 요금(AWS 중국 리전 제외)은 미국 달러(USD)로 표시되지만 지불 시 대체 통화를 선택할 수 있습니다. 다음을 참조하세요. [현재 AWS에서 지원되는 통화](#).

- AWS 설명서: [Savings Plans - Compute Savings Plans 및 예약 인스턴스](#)
- AWS 설명서: [Savings Plans - 플랜 유형](#)
- AWS 설명서: [예약 인스턴스의 유형](#)

제안 사항 18.1.2 – SAP와 관련된 각 요금 모델의 고려 사항을 이해

시간당 요금 할인 외에도 예약 인스턴스 및 Savings Plans의 다른 이점도 고려해야 합니다. 이 AWS 설명서: [Savings Plans 및 RI 비교표](#) 에는 예약 인스턴스와 Savings Plans가 비교되어 있습니다.

[영역 단위 예약 인스턴스](#) 는 특정 가용 영역 내에서 용량 예약을 제공하는 데 사용할 수 있습니다. Savings Plans는 용량 예약을 제공하지 않지만 [온디맨드 용량 예약](#) 과 결합하여 영역 단위 예약 인스턴스와 동일한 기능을 제공할 수 있습니다. 용량 전략에 대한 자세한 내용은 [안정성]: [모범 사례 10.2 - 가용성 및 용량 요구 사항에 적합한 아키텍처 선택](#) 을 참조하세요.

[Amazon EC2 스팟 인스턴스](#) 를 사용하면 AWS 클라우드에서 사용하지 않는 EC2 용량을 활용할 수 있습니다. 스팟 인스턴스는 온디맨드 인스턴스 가격 대비 최대 90% 할인된 가격으로 이용할 수 있습니다. AWS는 AWS에 용량이 필요할 경우 2분 전에 통지하여 스팟 인스턴스를 회수할 수 있습니다. 그러므로 스팟 인스턴스는 일반적으로 SAP 워크로드를 실행하는 데 적합하지 않습니다.

또한 [온디맨드 인스턴스](#) 를 사용하는 경우 시스템이 시작될 때마다 애플리케이션 성능에 미치는 영향 외에도 필요한 운영 시간을 기반으로 SAP 시스템 및 기본 EC2 인스턴스를 중지 및 시작하는 경우 이것이 미치는 추가적인 운영상의 영향을 고려해야 합니다.

제안 사항 18.1.3 – 예약 인스턴스 및 Savings Plans 약정의 통합 청구 및 공유를 위한 기업 전략을 평가

[통합 결제](#) 를 사용하면 예약 인스턴스 및 Savings Plans가 AWS 조직 내 모든 계정의 사용량에 적용됩니다. 조직의 관리 계정은 관리 계정을 포함하여 해당 조직의 모든 계정에 대해 예약 인스턴스 할인 및 Savings Plans 할인 공유를 해제할 수 있습니다. 즉, 예약 인스턴스 및 Savings Plans 할인은 공유가 해제된 계정 간에 공유되지 않습니다. 예약 인스턴스 또는 Savings Plans 할인을 공유하려면 두 계정 모두 공유가 설정되어 있어야 합니다. 이 기본 설정은 영구적이 아니며 언제든지 변경할 수 있습니다.

- AWS 설명서: [AWS Organizations 통합 결제](#)
- AWS 설명서: [예약 인스턴스 및 Savings Plans 할인 공유 해제](#)

약정 공유 전략을 결정하는 핵심 요소는 조직에서 채택한 전반적인 [AWS 계정 전략](#) 입니다. SAP 워크로드가 자체 전용 AWS 계정에서 실행되는지 아니면 AWS에서 호스트되는 다른 워크로드와 함께 실행되는지도 고려해야 합니다. 예약 인스턴스 및 Savings Plans 할인이 조직의 통합 결제에 어떻게 적용되는지 이해하려면 다음을 참조하세요.

- AWS 설명서: [통합 결제 이해](#)

SAP Note: [1656250 - SAP on AWS: Support prerequisites\(1656250 - SAP on AWS: 지원 사전 조건\)](#) [SAP 포털 액세스 권한 필요]에 자세히 설명된 대로 SAP on AWS는 유료 [AWS Support 계약](#) (예:

Business Support 또는 Enterprise Support)이 체결된 경우에만 지원됩니다. 비용 및 요구 사항에 따라 적절한 Support 플랜을 결정합니다.

- AWS 설명서: [AWS Support 플랜 비교](#)

AWS는 조직 내의 각 멤버 계정에 대해 독립적으로 Support 비용을 계산합니다.

모범 사례 18.2 - EC2 인스턴스 선택을 위한 주요 고려 사항으로 비용을 사용

워크로드에 적합한 SAP 인증 EC2 인스턴스를 선택하면 비용을 최적화할 수 있습니다. 가능한 경우 데이터에 기반한 의사 결정을 내릴 수 있도록 각 시스템에 대한 철저한 분석을 수행합니다. 일반 지침은 Well-Architected Framework [Cost Optimization Pillar - Cost-Effective Resources\(비용 최적화 원칙 - 비용 효율적 리소스\)](#)에서 찾을 수 있습니다.

제안 사항 18.2.1 – 리전에서 사용 가능한 최신 세대 인스턴스를 선택

최신 세대의 Amazon EC2 인스턴스는 최저의 비용으로 더 나은 성능을 제공하는 경우가 많으므로 배포 시나리오에 대해 사용 가능하고 인증된 경우 사용해야 합니다.

- AWS 설명서: [SAP용 Amazon EC2 인스턴스 유형](#)
- AWS 설명서: [리전별 인스턴스 유형 가용성](#)

Note

일부 Amazon EC2 인스턴스 패밀리(예: X1 및 고용량 메모리)는 리전 내의 일부 가용 영역에서 사용하지 못할 수 있습니다. 계획 단계에서 SAP 워크로드에 필요한 인스턴스 유형이 대상 가용 영역에서 사용 가능한지 확인해야 합니다.

제안 사항 18.2.2 – 비용과 성능 요구 사항을 균형 있게 고려

각 SAP 지원 Amazon EC2 인스턴스 패밀리는 [SAPS](#)로 측정된 특정 성능을 제공합니다. 성능 요구 사항에 따라 각 인스턴스 패밀리를 평가해야 합니다. SAPS당 비용 및 GiB당 비용 비율을 이해하는 것이 좋습니다.

컴퓨팅 최적화(C*)	범용(M*)	메모리 최적화(R*)
1 vCPU: 2GiB	1 vCPU: 4GiB	1 vCPU: 8GiB

워크로드 구성 요소에 [SAPS](#) (CPU)보다 메모리가 더 필요한 경우 메모리 1GiB당 비용이 가장 낮은 인스턴스 패밀리를 선택해야 합니다. 구성 요소에 메모리보다 SAPS(CPU)가 더 필요한 경우 SAPS당 가장 낮은 비용을 제공하는 인스턴스 패밀리를 선택해야 합니다.

AMD 프로세서로 구동되는 SAP 인증 인스턴스 패밀리는 일반적으로 유사한 Intel 기반 EC2에 비해 10%의 비용 절감 효과를 제공합니다. 예를 들면 동일한 성능 KPI에 대해 C5a는 C5 패밀리보다 10% 저렴합니다.

비프로덕션 SAP HANA 워크로드의 경우 SAP Note: [2271345 - 비프로덕션 사용을 위해 비용 최적화된 SAP HANA 하드웨어](#) [SAP 포털 액세스 권한 필요]에 자세히 설명된 요구 사항을 충족하는 인스턴스 패밀리 중 하나를 사용하는 것을 고려합니다.

제안 사항 18.2.3 – 증가 프로파일 및 최대 용량 요구 사항의 예측 가능성을 검토

기존의 AWS 기반 SAP 환경 또는 동종 마이그레이션은 새로운 그린필드 환경 구현 또는 이종 마이그레이션보다 예측 가능한 증가 및 사용 패턴을 보일 가능성이 높습니다.

과거 증가 데이터가 부족한 시스템의 경우 단기 또는 중기 증가에 충분한 EC2 인스턴스 크기를 선택할 때의 비용 이점을 고려해야 합니다. 요구 사항이 변화함에 따라 인스턴스 크기를 조정하도록 계획합니다. 리소스 소비가 변화함에 따라 아키텍처 설계가 서로 다른 EC2 인스턴스 패밀리 간에 이동할 수 있는 유연성을 제공하는지 확인해야 합니다.

마찬가지로, 최대 용량에 대한 변경이 고려되었는지 평가해야 합니다.

SAP HANA 환경의 크기를 조정할 때 데이터베이스 크기뿐만 아니라 작업 메모리 요구 사항도 고려합니다. SAP HANA 크기 조정 보고서 및 도구를 참조하여 크기와 사용량을 추정하세요.

제안 사항 18.2.4 – 인스턴스 약정 유연성을 고려

약정 기간 도중 구성 요소(예: SAP HANA 데이터베이스)가 확장되어야 하는 경우 이로 인해 다른 인스턴스 패밀리로 이동해야 하는지 평가합니다. 이는 요금 모델 선택에 영향을 미칩니다.

- AWS 설명서: [Amazon EC2 인스턴스 유형](#)

모범 사례 18.3 - 라이선싱 영향 및 최적화 옵션 평가

SAP 워크로드를 AWS로 이동할 때 SAP 워크로드에 필요한 소프트웨어 라이선스에 상업적 영향이 있을 수 있습니다. 이러한 영향과 사용 가능한 옵션을 이해해야 합니다.

제안 사항 18.3.1 – 소프트웨어 라이선스에 대한 CPU 및 메모리의 영향을 이해

라이선스 비용을 최적화하기 위해 지원되는 SAP용 [Amazon EC2 인스턴스 유형](#) 에서 사용 가능한 다양한 vCPU/메모리 비율을 평가합니다.

- SAP 설명서: [vCPU 또는 메모리로 라이선스가 부여된 SAP 구성 요소](#)
- SAP 설명서: [SAP HANA 할당 메모리 풀 및 할당 제한](#)

Oracle 기반 환경의 경우 다음을 검토하세요.

- [Oracle License Considerations, Licensing Oracle Software in the Cloud Computing Environment](#)
- Oracle Premium Support requirements, SAP Note: [2069760 - Oracle Linux 7.x SAP 설치 및 업그레이드](#) [SAP 포털 액세스 권한 필요]

Microsoft Windows 및 SQL Server 환경의 경우 다음을 검토하세요.

- AWS 설명서: [AWS 기반 Microsoft 라이선스](#)
- SAP Note: [2139358 - SQL Server의 라이선스 약관 변경 영향](#) [SAP 포털 액세스 권한 필요]

IBM Db2 환경의 경우 다음을 검토하세요.

- [Eligible Public Cloud BYOSL Policy](#)
- AWS 설명서: [AWS License Manager를 사용하여 IBM 라이선스 사용 추적](#)

CPU 또는 메모리가 ISV 및 서드 파티 제품 라이선스에 미치는 영향을 이해합니다.

- 라이선스 비용을 최적화하기 위해 [Optimize CPU](#) 기능을 사용하는 것을 고려합니다.
- 소프트웨어 라이선스 및 관련 비용을 관리하기 위해 [AWS License Manager](#) 를 사용하는 것을 고려합니다.
- AWS 설명서: [Amazon EC2 인스턴스 유형별 물리적 코어](#)

제안 사항 18.3.2 – 운영 체제 구매 옵션을 이해

각 SAP 지원 운영 체제에서 일련의 구매 옵션을 사용할 수 있습니다.

1. Amazon EC2 제공 라이선스
2. AWS Marketplace 제공 라이선스
3. 기존 보유 라이선스 사용(BYOL)

운영 체제에 따라 사용할 수 없는 옵션도 있습니다. 가장 비용 효율적인 옵션을 결정하려면 요구 사항과 라이선스 계약을 평가해야 합니다. 다음 운영 체제 비용을 Amazon EC2 비용의 일부로 포함할 수 있습니다.

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

AWS Marketplace를 통해 다음 운영 체제를 구매할 수 있습니다.

- Red Hat Enterprise Linux for SAP(Red Hat Enterprise Linux 기반 EC2 비용에 기초)
- SUSE Linux Enterprise Server for SAP(Amazon Linux 기반 EC2 비용에 기초)

다음 운영 체제에 기존 보유 라이선스(BYOL)를 사용할 수 있습니다.

- Windows Server
- Red Hat Enterprise Linux¹
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux for SAP²
- SUSE Linux Enterprise Server for SAP²
- Oracle Enterprise Linux(Oracle Premium Support 요구 사항은 SAP Note: [2069760 - Oracle Linux 7.x SAP 설치 및 업그레이드](#) 에 자세히 설명되어 있음) [SAP 포털 액세스 권한 필요]

¹ SAP Note: [2871484 - Red Hat Enterprise Linux의 SAP 지원 변형](#) [SAP 포털 액세스 권한 필요]를 참조하세요. SAP는 RHEL 8부터 SAP 워크로드에 표준 Red Hat Enterprise Linux를 더 이상 지원하지 않습니다.

² 이러한 제품은 장기 지원을 제공하여 업그레이드에 대한 운영 비용을 절감할 수 있습니다. 자세한 내용은 SUSE 설명서: [SUSE Enterprise Support Policy](#) 및 Red Hat 설명서: [Red Hat Enterprise Support Policy](#) 를 참조하세요.

제안 사항 18.3.3 – 라이선싱 제한을 완화하기 위해 Amazon EC2 전용 호스트 사용을 고려

Amazon EC2는 고객이 전용 하드웨어에 액세스할 수 있는 전용 호스트를 제공합니다. 전용 인프라에서 [이미 라이선스를 보유한 소프트웨어](#) 를 사용할 수 있습니다. Amazon EC2 전용 호스트는 Windows

Server 및 SQL Server 라이선스를 포함하여 소프트웨어 라이선스를 관리하는 데 도움이 되는 서비스인 [AWS License Manager](#) 와 통합됩니다.

제안 사항 18.3.4 – 기가바이트당 또는 코어당 라이선스 모델에서 전환할 때의 비용 이점을 평가

클라우드로 마이그레이션의 일부로 SAP Runtime 데이터베이스 라이선스 모델을 사용하는 것을 고려합니다.

SAP는 고객이 Runtime 데이터베이스 라이선스 모델에 따라 SAP HANA, SAP ASE 및 서드 파티 데이터베이스의 라이선스를 사용할 수 있는 기능을 제공합니다. SAP로부터 라이선스를 부여받은 Runtime 데이터베이스는 SAP로부터 라이선스를 부여받은 소프트웨어 및 SAP 지정 사용자를 지원하기 위한 용도로만 사용됩니다. SAP의 Runtime 데이터베이스는 일반적으로 SAP Application Value(SAV)라고 하는 SAP 소프트웨어 요금의 백분율로 라이선스가 부여됩니다.

Runtime 라이선스는 기가바이트의 메모리 또는 CPU 코어 수를 기반으로 하지 않습니다. SAP Runtime 데이터베이스 라이선스는 SAP 라이선스 계약에 포함되는 모든 환경에 적용되므로 특히 비프로덕션 시스템이 여러 개 있는 경우 기가바이트 또는 코어당 라이선스 모델에 비해 비용 이점을 제공할 수 있습니다.

SAP 라이선스 계약 내에서 SAP HANA Database Runtime 라이선스를 사용할 수 있는 권한이 이미 있는 경우 SAP HANA를 기본 데이터베이스로 사용할 수 없는 SAP 구성 요소에 대해 SAP ASE Database Runtime 라이선스를 추가로 사용할 수 있는 권한이 있는지 또는 해당 구성 요소에 SAP HANA를 사용하는 것과 관련된 인프라 비용을 절감할 수 있는지 확인해야 합니다.

- SAP 설명서: [SAP Licensing Guide](#) 를 참조하거나 SAP 계정 팀에 문의하세요.

모범 사례 18.4 - 필요한 특성을 기반으로 스토리지 옵션의 비용 영향 평가

SAP 시스템을 호스트, 아카이브, 보호하기 위한 서비스로 객체 스토리지, 파일 스토리지 및 블록 스토리지 서비스 중에서 선택합니다. 비용을 절감하고 민첩성을 향상하도록 스토리지를 설계합니다.

제안 사항 18.4.1 – 워크로드의 I/O 및 처리량 요구 사항에 부합하게 설계하는 가장 비용 효율적인 방법을 평가

대부분의 SAP 요구 사항에서는 EBS 볼륨에 SSD(솔리드 스테이트 디스크)를 사용하는 것이 좋습니다. 비용 효율적인 선택을 위해 대부분의 SAP 워크로드에 적합한 범용 Amazon EBS 유형으로 시작하는 것이 좋습니다. 시간이 지남에 따라 CloudWatch 지표 및 애플리케이션/데이터베이스 모니터링을 사용하여 사용량을 검토합니다. 더 높은 I/O 또는 처리량이 필요한 경우 일반적으로 프로비저닝된 IOPS Amazon EBS 유형으로 충족할 수 있습니다.

- AWS 설명서: [Amazon EBS 볼륨 유형](#)

비용과 성능을 균형 있게 고려하려면 SAP HANA 데이터 및 로그 볼륨에 사용되는 스토리지 구성이 SAP 스토리지 KPI를 충족해야 합니다. 다음 문서에 설명된 스토리지 레이아웃은 SAP TDI 지침에 대해 테스트되었습니다. [SAP HANA Tailored Data Center Integration](#)

- AWS 설명서: [SAP HANA용 스토리지 구성](#)

제안 사항 18.4.2 – 스토리지 크기 및 구성에 대한 동적 변경을 계획

데이터 사용량 또는 IOPS 요구 사항에 따라 스토리지를 적절한 크기로 조정하여 스토리지 비용을 최적화합니다.

필요에 따라 동적으로 볼륨 크기를 확장합니다. 애플리케이션 업그레이드와 같이 향상된 성능이 필요한 작업 중에 볼륨 유형을 변경하는 옵션을 평가합니다.

- AWS 설명서: [볼륨 수정 요청](#)

비용 관리를 보장하기 위해 모든 분리된 또는 사용되지 않는 볼륨을 정기적으로 검토합니다.

- AWS 설명서: [Amazon EBS 볼륨 또는 스냅샷 정보 나열](#)

제안 사항 18.4.3 – 객체 스토리지의 비용 이점을 평가

SAP 시스템의 핵심 데이터는 데이터베이스 내에 포함되며 Amazon EBS에 상주합니다. Amazon S3는 백업 또는 아카이브와 같은 보조 데이터와 이미지 또는 문서와 같은 대형 객체를 위한 저렴한 객체 스토리지를 제공할 수 있습니다. 보존 및 내구성 요구 사항에 적합한 [스토리지 유형](#) 을 선택하여 비용을 추가로 최적화할 수 있습니다.

제안 사항 18.4.4 – 공유 파일 시스템의 비용 이점을 평가

Amazon Elastic File System(Amazon EFS)은 스토리지를 프로비저닝 또는 관리하지 않고도 파일 데이터를 공유할 수 있는, 한 번 설정으로 완료되고 탄력적인 서버리스 파일 시스템입니다. 성능 및 가용성 요구 사항에 따라 적절한 스토리지 클래스를 선택하여 비용을 추가로 최적화할 수 있습니다.

Amazon FSx는 Windows Server에 구축된 완전관리형 파일 스토리지 솔루션으로, 가용성 및 내구성이 뛰어납니다. 데이터 중복 제거 기능이 중복 데이터를 제거하여 추가로 비용을 최적화할 수 있습니다.

Amazon EFS 또는 Amazon FSx의 일반적인 SAP 사용 사례에는 sapmnt, 전송, 인터페이스 파일, 백업 저장, 소프트웨어가 있습니다. Amazon EFS 또는 Amazon FSx를 사용하면 자체 고가용성 NFS 솔루션을 배포하는 것보다 비용 이점이 있습니다.

- AWS 설명서: [Amazon EFS](#)
- AWS 설명서: [Amazon FSx](#)

19 - 스토리지 비용 효율성을 위해 SAP 데이터 사용 최적화

스토리지 및 메모리 관련 비용을 최소화하기 위해 SAP 데이터 사용을 최적화하는 방법은 무엇입니까? 비용을 고려하여 데이터베이스 스토리지, 백업 및 지원 파일 시스템을 설계하고 정기적으로 위치, 보존 및 하우스키핑 전략을 평가합니다.

ID	우선순위	모범 사례
□ BP 19.1	필수	액세스 및 보존 요구 사항 이해
□ BP 19.2	적극 권장	정기적인 하우스키핑을 통해 불필요한 데이터 삭제
□ BP 19.3	권장	압축, 재구성 및 회수 전략 사용
□ BP 19.4	적극 권장	개선을 위해 백업 전략 검토
□ BP 19.5	권장	라이브 데이터에 계층화 옵션 고려
□ BP 19.6	권장	아카이빙 및 오프로딩 옵션 평가

모범 사례 19.1 - 액세스 및 보존 요구 사항 이해

데이터에 액세스하고 보존하는 방법을 이해합니다. 활성 데이터, 문서 관리 시스템 및 백업을 고려합니다.

제안 사항 19.1.1 – SAP 시스템에서 다양한 유형의 비즈니스 데이터를 분류

비즈니스 관점에서 다양한 데이터 유형 및 데이터 액세스 빈도(데이터 온도)를 분류함으로써 SAP 시스템에서 데이터를 아카이브 또는 오프로드할 기회를 식별하여 비용을 최적화할 수 있습니다.

다음은 SAP 시스템에서 볼 수 있는 몇 가지 일반적인 데이터 유형입니다.

- 참조 - 값이 자주 변경되지 않는 데이터. 예: 도시, 국가 및 환율
- SAP 마스터 데이터 - 값이 거의 변경되지 않는 데이터. 예: SAP Customer Master, 제품
- 감사 - 감사 목적으로 보관되는 데이터. 예: 변경 로그
- 트랜잭션 - 일상적인 비즈니스 운영의 일부로 생성된 데이터. 예: 판매 주문
- 분석 - 분석 및 의사 결정을 지원하기 위해 생성된 데이터. 예: 월별 매출 보고

다음과 같이 데이터 온도를 분류합니다.

- 핫 - 자주 액세스하는 데이터
- 웜 - 자주 액세스하지 않는 데이터
- 콜드 - 산발적으로만 액세스하는 데이터

다음과 같이 보존 요구 사항을 분류합니다.

- 재해 복구(DR) 목적으로 보존
- 참조 목적으로 보존
- 규정 준수 또는 감사 목적으로 보존

모범 사례 19.2 - 정기적인 하우스키팅을 통해 불필요한 데이터 삭제

비용을 절감하기 위해 정기적인 하우스키팅 및 재구성 작업을 통해 데이터베이스 크기 및 기타 파일 시스템 사용을 최소화하여 데이터 공간을 축소합니다.

제안 사항 19.2.1 – SAP 기술 테이블에서 크기 조정을 검토하고 정기적으로 하우스키팅을 수행

SAP는 기술 테이블의 데이터 관리에 대한 포괄적인 지침을 제공합니다. 이러한 테이블의 증가를 식별하고 해결함으로써 스토리지 및 컴퓨팅 비용을 절감할 수 있습니다. 이는 데이터베이스 크기와 메모리 요구 사항 간의 직접적인 관계 때문에 SAP HANA 인스턴스와 특히 관련이 있습니다.

- SAP Note: [2388483](#) - 방법: [기술 표의 데이터 관리](#) [SAP 포털 액세스 권한 필요]

테이블(특히 기본 테이블로 표시된 항목)의 상대적 크기를 얻으려면 참조되는 'largest table' SQL 문을 사용하세요. 기존 SAP 고객에서 빈번한 예는 삭제 또는 아카이브할 수 있는 완료된 SAP 워크플로 항목의 수가 많다는 것입니다. 마이그레이션 전에 하우스키핑을 수행하면 일정 및 성능도 향상될 수 있습니다. SAP HANA를 사용하는 경우 보고서 '/SDF/HDB_SIZING'이 정리 세부 정보 및 예상 디스크 요구 사항을 제공할 수 있습니다.

제안 사항 19.2.2 – 로그, 추적, 인터페이스 파일 및 백업의 자동 또는 정기적 정리를 통해 파일 시스템 증가를 제어

스토리지 비용은 사용량에 따라 결정되므로 장애 분석에 더 이상 유용하지 않은 파일의 복사본 및 백업의 승수 효과 외에도 기존 사용량을 최적화할 수 있는 기회가 있습니다.

- SAP Note: [2399996](#) - 방법: [SAP HANACleaner로 자동 SAP HANA Cleanup 구성](#) [SAP 포털 액세스 권한 필요]

모범 사례 19.3 - 압축, 재구성 및 회수 전략 사용

SAP에서 지원하는 모든 데이터베이스는 공간 회수 메커니즘을 제공합니다. 이러한 메커니즘은 메모리 또는 EBS 볼륨 확장과 관련된 비용 증가를 최소화하기 위한 정기적인 유지 관리 활동의 일부여야 합니다.

제안 사항 19.3.1 – 데이터베이스 압축을 사용

압축은 SAP HANA의 기본 특징입니다. 다른 데이터베이스에서 압축을 사용하려면 추가 라이선스가 필요할 수 있지만 비용 및 성능 이점을 위해 조사해야 합니다. 다음 노트는 다양한 데이터베이스의 출발점을 제공하지만 추가 정보는 SAP 및 데이터베이스 설명서를 참조하세요.

데이터베이스	SAP 설명서 또는 SAP Note
SAP HANA	SAP Note: 2112604 - FAQ: SAP HANA 압축 [SAP 포털 액세스 권한 필요]
SAP ASE	(지침은 SAP 또는 공급 업체 설명서 참조)
IBM Db2	SAP Note: 1555903 - DB6: 지원되는 IBM Db2 데이터베이스 기능 [SAP 포털 액세스 권한 필요]

데이터베이스	SAP 설명서 또는 SAP Note
Oracle	SAP Note: 1289494 - FAQ: Oracle 압축 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 1488135 - SQL Server의 데이터베이스 압축 [SAP 포털 액세스 권한 필요]
SAP MaxDB	(지침은 SAP 또는 공급 업체 설명서 참조)

제안 사항 19.3.2 – 데이터베이스 재구성 및 회수 작업을 사용

유기적 사용 또는 대상 지정 아카이브 및 정리 작업으로 인해 데이터베이스 내에서 사용되지 않은 공간은 공간 절약을 실현하기 위해 재구성 또는 회수 작업이 필요할 수 있습니다. 공간을 정기적으로 회수함으로써 전반적인 증가와 스토리지 또는 메모리 추가 요구 사항을 줄일 수 있습니다. 다음 노트는 다양한 데이터베이스의 출발점을 제공하지만 SAP 및 데이터베이스 설명서를 참조하세요.

데이터베이스	SAP 설명서 또는 SAP Note
SAP HANA	SAP Note: 2499913 - SAP HANA 데이터 볼륨 크기를 축소하는 방법 [SAP 포털 액세스 권한 필요]
SAP ASE	SAP Note: 2543407 - 온라인에서 재구성 및 재구축 - SAP ASE for Business Suite [SAP 포털 액세스 권한 필요]
IBM Db2	SAP Note: 1942183 - DB6: 테이블 또는 인덱스 재구성을 고려할 시기 [SAP 포털 액세스 권한 필요]
Oracle	SAP Note: 541538 - FAQ: 재구성 [SAP 포털 액세스 권한 필요]
Microsoft SQL Server	SAP Note: 1721843 - MSSQL: 아카이빙, 삭제 또는 압축 이후 단계 [SAP 포털 액세스 권한 필요]

데이터베이스	SAP 설명서 또는 SAP Note
SAP MaxDB	(지침은 SAP 또는 공급 업체 설명서 참조)

모범 사례 19.4 - 개선을 위해 백업 전략 검토

SAP on AWS를 실행할 때 백업 및 보존에 대한 접근 방식을 평가하여 위치, 보존 및 복구와 관련된 비용을 최적화해야 합니다.

제안 사항 19.4.1 - 백업 위치를 평가

Amazon S3는 저렴한 비용, 내구성, 스토리지 클래스 옵션 때문에 SAP 시스템 백업용으로 제안되는 장기 스토리지 솔루션입니다. Amazon EBS 볼륨의 데이터를 Amazon S3로 복사하려면 특정 시점 스냅샷, 통합 데이터베이스 도구 또는 직접 API 호출을 사용하여 데이터를 전송할 수 있습니다.

스냅샷은 증분 백업입니다. 즉, 가장 최근 스냅샷 이후에 변경된 디바이스의 블록만 저장됩니다. 이렇게 하면 스냅샷을 생성하는 데 필요한 시간이 최소화되고 데이터를 복제하지 않아 스토리지 비용이 절약됩니다.

데이터베이스 백업 솔루션은 일관성을 보장하기 위해 데이터베이스 상태를 인식해야 합니다. AWS는 Amazon S3와 직접 통합되는 SAP HANA 백업 솔루션(AWS Backint for SAP HANA)을 추가 비용 없이 제공합니다. 다른 SAP 지원 데이터베이스의 경우 Amazon S3로의 직접 백업을 지원하는 데이터베이스 공급 업체 또는 서드 파티 제공 백업 도구를 사용할 수 있습니다.

- SAP 설명서: [Featured backup solutions](#)

임시 요구 사항 또는 스테이징 영역의 경우 먼저 Amazon EBS로 백업해야 할 수 있습니다. 이러한 사용 사례의 경우 ST1 볼륨 유형은 백업에 적합한 처리량 및 성능 특성을 제공하는 저렴한 HDD 볼륨입니다. SAP 데이터베이스를 디스크에 백업해야 하는 경우 ST1 을 선택하면 전체 스토리지 비용을 절감할 수 있습니다.

- AWS 설명서: [Amazon EBS 볼륨 유형](#)

백업에 Amazon EFS를 사용하는 경우 EFS-Infrequent Access를 고려합니다. 이 스토리지 클래스는 일상적으로 액세스하지 않는 파일의 스토리지 비용을 줄여줍니다. Amazon EFS One Zone-Infrequent Access는 데이터가 하나의 가용 영역에만 상주하므로 백업에 권장되지 않습니다.

제안 사항 19.4.2 - 표준 백업에 대한 보존 정책을 검토 및 구현

비용을 관리하기 위해 비즈니스 요구 사항에 부합하는 보존 정책을 구현해야 합니다. Amazon S3는 GB당 비용, 최소 저장 기간 요금, 검색 요금(해당되는 경우)과 같은 특성으로 다양한 사용 사례에 맞게 설계된 여러 스토리지 클래스를 제공합니다. 백업에 대한 보존 및 액세스 요구 사항을 이해하면 요구 사항에 가장 적합한 스토리지 클래스를 결정하는 데 도움이 됩니다.

S3 수명 주기 정책을 사용하면 애플리케이션을 변경하지 않고 자동으로 다른 스토리지 클래스로 전송할 수 있습니다. 예를 들어 보존 기간이 더 짧은 백업은 이러한 클래스와 관련된 최소 저장 기간 요금 및 검색 요금으로 인해 S3-IA 또는 Amazon S3 Glacier보다 S3 Standard에 더 적합할 수 있습니다. 감사 목적의 월별 백업과 같이 보존 기간이 더 긴 백업은 필요한 보존 기간에 따라 S3-IA 또는 Amazon S3 Glacier에 더 적합합니다.

- AWS 설명서: [Amazon S3 저장소 클래스](#)
- AWS 서비스: [Amazon Data Lifecycle Manager](#)
- AWS 설명서: [Amazon EFS 수명 주기 관리](#)
- AWS 서비스: [AWS Backup](#)

제안 사항 19.4.3 – 임시 백업에 대한 전략을 수립

시스템 또는 연결된 파일 시스템의 임시 백업이 요구 사항일 수 있습니다. 이러한 백업은 변경 전에 또는 특정 시점의 시스템 상태에 대한 참조로 필요할 수 있습니다. 이러한 백업은 표준 보존 기간과 다를 수 있으므로 삭제를 포함한 스토리지 사용 및 수명 주기 정책이 해당 백업의 개별 요구 사항에 가장 비용 효율적이 되도록 별도의 일정 또는 프로세스를 채택해야 합니다.

제안 사항 19.4.4 – 복구 접근 방식에 따라 백업 설정을 검토

백업은 시스템을 이전 시점으로 되돌리고 장애 시나리오로부터 방어하는 데 사용됩니다. 강력하지만 과도하지 않은 백업 스토리지 사용을 통해 비용 효율성을 보장하려면 복구 접근 방식을 검토해야 합니다. 더 세분화되고 오래된 백업의 요구 사항에 대한 가정을 재검토합니다. 복구 시 이러한 이전 백업이 필요한지 여부를 결정합니다.

예를 들어 데이터베이스 백업과 파일 시스템 백업을 모두 사용하는 것이 유효한 전략입니다. 그러나 기본 복구 메커니즘이 데이터베이스 복원 도구를 사용하는 경우 보존을 축소하거나 일부 볼륨의 스냅샷 백업을 삭제하여 비용을 최적화할 수 있는 기회가 있을 수 있습니다.

- AWS 설명서: [Amazon EBS 스냅샷](#)
- AWS 설명서: [AWS Trusted Advisor 모범 사례 점검 항목](#)

모범 사례 19.5 - 라이브 데이터에 계층화 옵션 고려

SAP HANA 관련 컴퓨팅 비용의 주요 요소는 필요한 메모리 용량입니다. 그러므로 데이터 오프로드 및 계층화 옵션을 사용하면 컴퓨팅 비용을 절감할 수 있습니다. 다른 데이터베이스에는 계층화 옵션이 있을 수 있지만 여기서는 강조되지 않았습니다. 사용 가능한 옵션을 파악하려면 데이터베이스 공급 업체에 문의하세요.

제안 사항 19.5.1 – SAP HANA OLAP 기반 워크로드에 대해 동적 계층화, 확장 노드 및 NLS(Near-Line Storage)를 평가

SAP HANA 동적 계층화는 기록 데이터를 관리하기 위한 SAP HANA 데이터베이스의 선택적 추가 기능입니다. 동적 계층화의 목적은 자주 액세스하지 않는 데이터를 관리하기 위해 (SAP HANA의 인 메모리 스토어와 반대로) 디스크 중심 열 기반 스토어로 SAP HANA 메모리를 확장하는 것입니다. 동적 계층화는 네이티브 SAP HANA 사용 사례에만 사용할 수 있으며 HANA의 BW(Business Warehouse) 또는 BW/4 HANA 사용 사례에는 사용할 수 없습니다.

SAP HANA 확장 노드는 워 데이터를 저장하기 위해 특별히 설정되고 예약된 특수 목적 SAP HANA 작업자 노드입니다. SAP HANA 확장 노드를 사용하면 SAP BW(Business Warehouse) 또는 네이티브 SAP HANA 분석 사용 사례의 워 데이터를 저장할 수 있습니다. SAP HANA 확장 노드에 저장할 수 있는 전체 데이터 양은 확장 노드의 총 메모리 양의 1배에서 2배 사이입니다.

SAP IQ가 포함된 SAP BW NLS(Near-Line Storage)를 사용하면 BW 외부의 콜드 데이터를 HANA 또는 BW/4 HANA 데이터베이스에 저장할 수 있습니다. NLS는 콜드 데이터를 HANA 데이터베이스에서 이동하여 SAP IQ 서버의 스토리지에 저장합니다.

- AWS 설명서: [SAP 데이터 계층화](#)

제안 사항 19.5.2 – OLTP 기반 워크로드에 대해 데이터 에이징 및 SAP HANA NSE(Native Storage Extension)를 평가

데이터 에이징은 디스크 영역에 자주 액세스하지 않는 데이터를 저장하여 SAP HANA 메모리를 확보합니다.

- AWS 설명서: [SAP 데이터 계층화](#)

제안 사항 19.5.3 – 대규모 분석 데이터에 데이터 레이크 사용을 고려

SAP 및 비 SAP 데이터를 분석할 때 S3 기반 데이터 레이크는 비용 효율적인 데이터 스토리지 옵션을 제공합니다.

- SAP on AWS 블로그: [SAP on AWS를 사용하여 데이터 레이크 구축](#)

모범 사례 19.6 - 아카이빙 및 오프로딩 옵션 평가

자주 액세스하지 않는 데이터를 아카이브하거나 대형 객체를 니어라인 스토리지로 오프로드하는 옵션을 고려하면 인프라 및 백업 비용을 절감할 수 있습니다.

제안 사항 19.6.1 – 자주 액세스하지 않는 데이터가 있는 대규모 테이블에 대한 아카이빙을 구현

특히 SAP HANA 데이터베이스의 경우 아카이빙 전략을 사용하여 데이터베이스 증가를 관리하면 비용 이점이 있습니다.

- SAP 설명서: [데이터 아카이빙](#)

제안 사항 19.6.2 – Amazon S3를 대상으로 지원하는 아카이빙 도구를 평가

Amazon S3는 뛰어난 가용성 및 내구성으로 설계되었으며 다양한 비용 효율적인 스토리지 클래스를 제공합니다. 따라서 가장 낮은 총 소유 비용(TCO)으로 SAP 아카이브 데이터를 저장하는 데 이상적입니다.

- AWS 설명서: [Amazon S3 저장소 클래스](#)
- SAP 설명서: [SAP Certified Archiving Solutions](#)

제안 사항 19.6.3 – 대형 객체에 데이터 관리 시스템을 사용

송장 및 이미지와 같은 대형 객체에 대해 SAP 데이터베이스 외부에서 데이터를 오프로드하고 관리하기 위한 옵션과 비용 이점을 이해합니다. 데이터 액세스에 대한 비즈니스 요구 사항, 구현 노력 및 지속적인 관리의 복잡성을 고려합니다.

대형 객체는 데이터베이스 크기를 증가시켜 리소스 및 백업 비용을 높입니다. 데이터 관리 시스템 옵션은 더 저렴한 스토리지 솔루션을 제공할 수 있습니다.

- SAP 설명서: [SAP Document Management](#)
- SAP 설명서: [Search for Certified ILM Solutions](#)

20 – 가시성, 계획 및 거버넌스로 비용 관리

비용 최적화 및 인식을 보장하기 위해 클라우드 재무 관리(CFM)를 어떻게 실행합니까? 시작부터 운영에 이르기까지 어떻게 SAP 클라우드 인프라 예산 관리를 설정하고 비즈니스 요구 사항에 맞춰 지속적으로 사용량을 최적화합니까?

ID	우선순위	모범 사례
□ BP 20.1	필수	프로젝트 단계에서 소비 모델 및 환경 사용량 계획
□ BP 20.2	필수	다양한 가격 책정 방식을 활용하는 다년 계획 비용 모델 설정
□ BP 20.3	적극 권장	이상 탐지를 포함하여 비용 할당 및 추적을 위한 예산 및 메커니즘 수립
□ BP 20.4	권장	비용 관련 승인 절차 및 제어 설정
□ BP 20.5	권장	최적화 기회를 위해 사용량을 검토

모범 사례 20.1 - 프로젝트 단계에서 소비 모델 및 환경 사용량 계획

마이그레이션 또는 구현 프로젝트 등 프로젝트 중에 단계적 접근 방식으로 시스템을 배포하는 경우가 많습니다. 또한 크기 조정 및 사용 프로필을 설정하는 안정화 기간도 있습니다. 이 기간 동안 유연성과 온디맨드 인스턴스 기능을 활용하여 비용을 최소화합니다.

제안 사항 20.1.1 – 필요한 경우에만 시스템을 배포하도록 계획

리드 타임을 단축하려면 필요한 경우에만 시스템을 배포할 수 있는 옵션을 제공해야 합니다. 단기 프로젝트 시스템의 경우 온디맨드 인스턴스를 사용하여 필요한 기간 동안 프로젝트 시스템을 구축합니다.

제안 사항 20.1.2 – 예상 기간 및 사용 프로필에 따라 요금 옵션을 평가

프로젝트 기간과 업무 시간은 요금 모델에 영향을 미칩니다. 온디맨드 요금 모델이 프로젝트 시작 시 기본적으로 선택되는 경우가 많습니다. 적절한 경우 더 저렴한 옵션으로 조정할 수 있도록 예산을 정의하고 평가합니다.

제안 사항 20.1.3 – 사용하지 않는 시스템을 일시 중단 또는 폐기하도록 계획

프로젝트가 더 이상 활성 상태가 아니거나 목적을 달성한 경우 인스턴스 종료에 따른 비용 절감과 폐기에 따른 스토리지 절감을 고려합니다. 일반적으로 프로젝트는 마이그레이션 중에 시스템의 복사본을 여러 개 생성합니다. 사용되지 않는 시스템은 종료해야 합니다.

모범 사례 20.2 - 다양한 가격 책정 방식을 활용하는 다년 계획 비용 모델 설정

요금 모델을 최대한 활용하여 AWS에서 제공하는 할인을 극대화할 수 있도록 용량 요구 사항에 대한 다년 계획을 수립합니다. 비용 기준을 설정하고 비용을 추적합니다. 클라우드 요금 모델은 변화하는 비즈니스 요구 사항에 대응하여 탄력적으로 인프라를 조정할 수 있는 유연성을 제공합니다. 장기 Savings Plan 또는 예약 인스턴스를 약정하기 전에 최소 3년간 예상되는 SAP 시스템 사용량을 이해하고 계획합니다. 테스트, SAP Quick Sizer 출력 및 증가 예측을 사용하여 데이터를 기반으로 약정 계획을 수립하고 워크로드에 대한 최대 할인을 활용합니다.

제안 사항 20.2.1 – 주요 비즈니스 이벤트를 이해하여 용량 추정치를 설정

SAP 워크로드는 일반적으로 사용 패턴 및 운영 시간이 알려져 있어 안정적입니다. SAP 시스템에 대해 잘 파악된 안정 상태 용량 기준을 설정합니다. 이 작업은 배포 초기 몇 주 동안 성능 테스트 및 프로덕션 환경 모니터링을 통해 수행할 수 있습니다.

다음은 고려하여 안정 상태 용량 추정치를 최소 3년 범위로 확장합니다.

- 인수, 합병, 매각과 같은 주요 비즈니스 이벤트
- 데이터 스토리지 요구 사항 또는 비즈니스 프로세스 빈도에 영향을 줄 수 있는 규정 변경
- 정상적인 비즈니스 운영으로 인한 데이터 증가(데이터가 스토리지 크기 외에 컴퓨팅 크기에도 영향을 미치므로 SAP HANA와 같은 인 메모리 데이터베이스에 특히 중요)
- 주요 시스템 업그레이드, 시스템 교체 또는 폐기

제안 사항 20.2.2 – 1년 또는 3년 약정이 적절한지 평가

용량 추정치를 사용하여 3년 약정 컴퓨팅을 활용할 때 가능한 할인을 극대화할 수 있는 SAP 워크로드의 양을 평가합니다. 다음 사항을 고려하세요.

- SAP 워크로드의 모든 컴퓨팅 요구 사항에 3년 약정을 고려할 수 있습니까?
- 변화하지 않을 것이라고 확신하는 일부 요구 사항에 3년 약정을 고려할 수 있습니까? 예: SAP 기본 애플리케이션 서버 또는 프라이머리 데이터베이스.
- SAP 워크로드가 향후 SAP 용량 요구 사항의 변화로 인해 컴퓨팅 요구 사항이 감소할 때 초과 컴퓨팅 약정을 사용할 수 있는 보다 광범위한 AWS 조직의 일부입니까?

- SAP 워크로드가 보다 광범위한 AWS 조직의 일부이며 연중무휴 24시간 운영할 필요가 없는 비프로덕션 환경에 대한 컴퓨팅 약정을 공유할 수 있습니까?
- 중기 용량 변화의 경우 3년 컴퓨팅 계획을 약정하는 이점이 초과 또는 미사용 용량 낭비보다 더 클까(예: 단기 약정 대비 손익분기점이 20개월)?
- 단기적으로 주요 비즈니스 변경 또는 교체의 영향을 받을 가능성이 있는 애플리케이션에 대해 단기 약정(1년)을 고려할 수 있습니까?
- 환율 변동이 고려해야 할 문제입니까? AWS 요금은 미국 달러(USD)입니다(AWS 중국 제외). 고정 환율이 바람직한 경우 가능하면 전체 선결제 요금 모델을 고려할 수 있습니다.

할인을 극대화하기 위해 워크로드 용량 요구 사항을 약정 기간과 일치시키는 계획을 수립합니다.

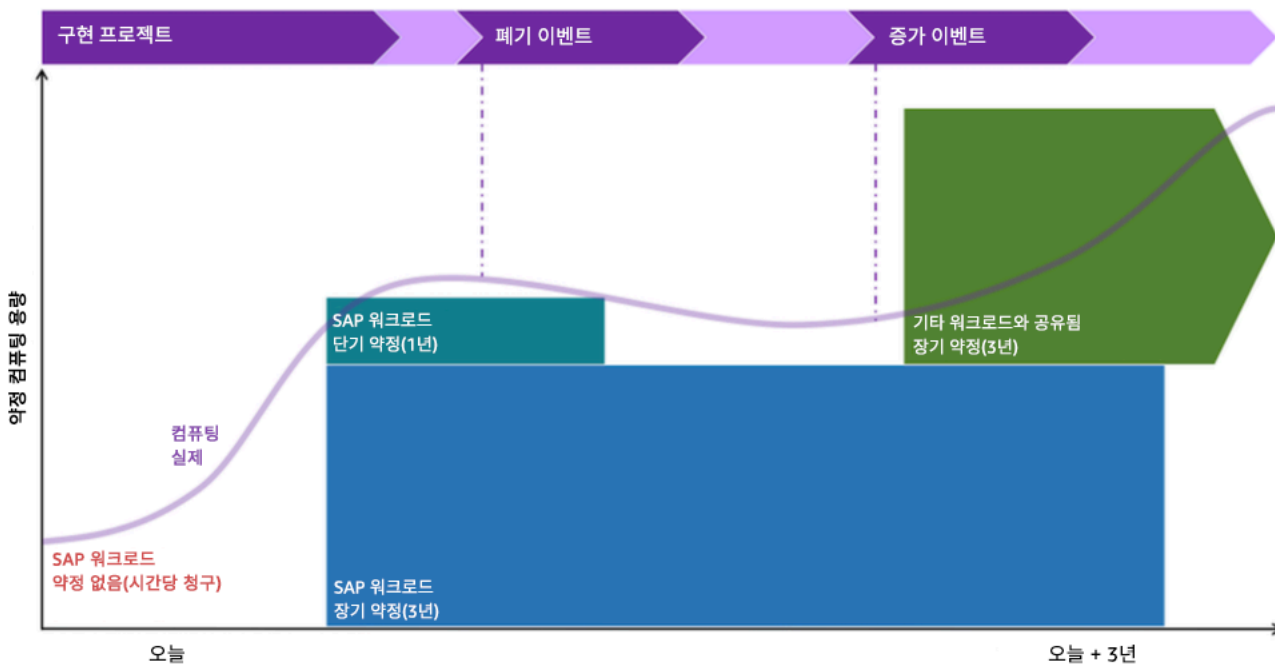


그림: SAP on AWS 컴퓨팅 약정의 타임라인 예

제안 사항 20.2.3 – 할인폭을 늘리기 위해 컴퓨팅 유형을 고정하는 것이 적절한지 평가

SAP 워크로드는 일반적으로 제한된 세트의 AWS 컴퓨팅 유형만 사용하므로 할인을 극대화하기 위해 특정 컴퓨팅 패밀리 또는 특정 인스턴스 유형을 약정하는 것이 워크로드에 적합한지 고려해야 합니다. 컴퓨팅에 대한 가장 할인이 높은 두 요금 모델은 EC2 Instance Savings Plans 및 표준 예약 인스턴스입니다.

다음 사항을 고려하세요.

- 환경에서 자주 사용되는 컴퓨팅 유형을 식별하여 이에 대한 특정 EC2 Instance Savings Plans 또는 표준 예약 인스턴스를 구매하는 것을 고려합니다. 예를 들어 여러 SAP 애플리케이션을 위한 애플리케이션 서버에 m5.xlarge 를 사용 중인 경우입니다. 항상 이 약정을 사용할 가능성이 높기 때문에 이는 EC2 전용 Savings Plan 또는 표준 예약 인스턴스를 구매하기에 좋은 후보입니다.
- 워크로드 증가 또는 비즈니스 이벤트로 인해 EC2 패밀리를 변경할 가능성이 높은 컴퓨팅 구성 요소를 식별합니다. 이러한 항목에는 보다 일반적인 Compute Savings Plans 또는 컨버터블 예약 인스턴스를 구매하는 것이 좋습니다. 예를 들어 SAP HANA 데이터베이스가 6개월 만에 크기 증가로 인해 EC2 r5 에서 x1e 컴퓨팅 패밀리로 이동해야 하는 경우입니다. 이는 단기 컨버터블 예약 인스턴스 또는 Compute Savings Plans에 적합한 후보입니다.
- 일반 컴퓨팅 가격과 특정 컴퓨팅 가격의 손익분기점을 식별하고 약정 유형을 선택할 때 이를 고려합니다. 예를 들어 3년 차에 크기 조정 변경이 있는 경우 3년 컨버터블 예약 인스턴스를 약정하는 것보다 3년 동안 표준 예약 인스턴스를 구매하는 것이 더 저렴할 수 있습니다. AWS 예약 인스턴스 Marketplace에서 잔여 예약 인스턴스 가치를 판매하는 것도 고려할 수 있습니다.
- 인스턴스 유형을 변경하기 전에 AWS Marketplace 판매자 비공개 제안 또는 연간 구독 소프트웨어의 사용을 식별합니다. 이렇게 하면 추가 소프트웨어 비용이 발생하지 않습니다. 두 플랜 모두 지정된 기간 동안 한 Amazon EC2 인스턴스에서 소프트웨어 제품을 실행하도록 약정함으로써 비용을 절감할 수 있습니다. 예를 들어 r4.xlarge 인스턴스에서 실행할 소프트웨어에 대한 연간 구독을 구매했습니다. 인스턴스 유형을 r5.xlarge 로 변경하기로 결정했습니다. 연간 구독은 더 이상 인스턴스에 연결되지 않지만 여전히 활성 상태입니다. 그 결과 r5.xlarge 에서 소프트웨어에 대한 추가 온디맨드 요금이 설정됩니다. 인스턴스 크기를 변경하기 전에 연간 구독이 만료될 때까지 기다리는 것이 좋습니다.

제안 사항 20.2.4 – Savings Plans, 예약 인스턴스 또는 둘 다 더 적합한지 평가

SAP 워크로드에 적합한 경우 Savings Plans와 예약 인스턴스를 혼합하여 다양한 모델의 이점을 확보합니다. 약정 기간 및 컴퓨팅 요구 사항을 전체적으로 계산한 다음 요금 모델을 선택합니다.

Savings Plans와 예약 인스턴스의 차이점에 대한 자세한 내용은 [비용 최적화]: [모범 사례 18.1 - Amazon EC2에 사용할 수 있는 결제 및 약정 옵션 이해](#) 및 [Compute Savings Plans 및 예약 인스턴스에서 찾을 수 있습니다.](#)

[안정성]: [모범 사례 10.2 - 가용성 및 용량 요구 사항에 적합한 아키텍처 선택](#) 을 고려하세요. 여기서는 Savings Plans와 예약 인스턴스 간의 용량 예약 기능 차이점과 절충에 대해 설명합니다.

제안 사항 20.2.5 – 예산 및 추적 목적을 위해 용량 계획을 비용 모델로 변환

Savings Plans, 예약 인스턴스 선택, 온디맨드 예산을 최소 3년간의 SAP 환경에 대한 AWS 지출을 추정하는 비용 계획으로 전환합니다. 컴퓨팅 추정치를 다른 AWS 비용과 결합하여 예산 책정 및 추적 목적으로 SAP 워크로드 비용 모델을 완성합니다.

SAP 비용을 추정할 때 다음 항목을 포함해야 합니다.

- 컴퓨팅 연결 스토리지 비용(예: Amazon EBS 볼륨)
- 공유 파일 스토리지 비용(예: Amazon EFS 및 Amazon FSx)
- 백업 스토리지 비용(예: Amazon S3 및 Amazon S3 Glacier)
- 네트워크 및 VPC 비용(예: Elastic Load Balancer, NAT 게이트웨이, Transit Gateway, 네트워크 아웃바운드 비용, Direct Connect 및 VPN)
- 관리 및 거버넌스 서비스 비용(예: CloudWatch 세부 지표, AWS CloudTrail 및 AWS Config)
- 보안 서비스 비용(예: AWS WAF, Amazon GuardDuty 및 AWS Shield)
- AWS Support 비용(Business 또는 Enterprise)
- 자격이 있는 기업 할인 프로그램 또는 대량 구매 할인을 고려합니다(자세한 내용은 AWS 계정 관리자에게 문의).
- 통화: AWS 요금은 미국 달러(USD)입니다. 청구 통화를 선택할 수 있으며 청구서는 USD로 계산되며 경쟁력 있는 환율로 원하는 통화로 환산됩니다.

모범 사례 20.3 - 이상 탐지를 포함하여 비용 할당 및 추적을 위한 예산 및 메커니즘 수립

Well-Architected Framework에는 재무 관리를 구현하기 위한 [지침](#) 이 있습니다. 비즈니스 요구 사항에 따라 연간, 분기별, 월별 또는 일일 예산으로 클라우드 비용 예상치를 설정합니다. 정기적으로 사용량에 따라 예측을 조정하고 패턴 및 이상을 식별합니다. 계정 및 태깅 전략을 사용하여 비용 할당 메커니즘을 설정합니다.

제안 사항 20.3.1 - 비용 및 결제 도구를 사용하여 지출 가시성을 확보

SAP 시스템은 사용 패턴이 정적인 경우가 많습니다. 영구적으로 또는 프로젝트 단계에서 온디맨드 요금 모델을 사용하는 경우 Amazon EC2 비용이 변동할 수 있습니다. 데이터 볼륨 관리 전략이 수립되지 않으면 Amazon EBS 및 Amazon S3 비용이 예상보다 높을 수 있습니다.

적은 설정 작업으로 지출 가시성을 확보할 수 있는 도구는 [AWS Cost Anomaly Detection](#) 입니다. 고급 기계 학습(ML) 기술을 사용하여 비정상적인 지출 및 근본 원인을 식별하므로 조치를 취할 수 있습니다. [AWS Budgets](#) 를 사용하여 예상 비용 및 사용량을 기반으로 맞춤 예산을 설정합니다. 임계값을 초과할 경우 알리도록 예산 경고를 구성합니다.

[AWS Cost Explorer](#) 및 [AWS 결제 및 비용 관리](#) 는 가시성 및 분석을 위한 도구를 제공합니다.

추가 지침은 Well-Architected Framework [비용 최적화]: [지출 및 사용량 인식](#) 에서 찾을 수 있습니다.

제안 사항 20.3.2 – 태그를 사용하여 지출을 분석 및 할당

개별 계정, 리소스, 사업부 및 SAP 환경을 기반으로 AWS 리소스 요금을 식별하는 데 도움이 되는 [비용 할당 태그](#) 를 생성할 수 있습니다. 이러한 태그는 AWS 결제 보고서에 표시되며 Cost Explorer를 사용하여 분석할 수 있습니다. 비용 할당 태그를 사용하여 개별 SAP 환경과 관련된 비용을 결정할 수 있습니다. 더 이상 필요하지 않은 임시 환경 또는 프로젝트 환경과 같은 특정 환경과 관련된 비용을 축소하거나 제거하기 위해 조치를 취해야 하는지 여부를 알리는 데 도움이 됩니다. 비용 할당 태그가 연결되지 않은 리소스를 식별하는 프로세스가 있어야 합니다. 이러한 리소스에 비용 할당 태그를 추가하는 데 필요한 작업을 구현합니다.

- SAP on AWS 블로그: [SAP on AWS 태깅 권장 사항](#)

모범 사례 20.4 - 비용 관련 승인 절차 및 제어 설정

클라우드 준비를 위해 기존 비용 평가 프로세스를 조정해야 할 수도 있습니다. 올바른 재무 관행 및 정책을 구현하는 방법을 숙지하기 위해 [AWS 클라우드 금융 관리 안내서](#) 를 검토합니다.

제안 사항 20.4.1 – 관리자에게 비용 영향을 교육

책임을 할당하고 비용 최적화에 대한 인센티브를 제공하는 메커니즘을 도입합니다.

제안 사항 20.4.2 – IAM 제어를 사용하여 특정 사용자만 인스턴스를 프로비저닝할 수 있도록 허용

비용 관리를 보장하기 위해 계정 경계 내에서 리소스 유형 및 직무에 부합하는 IAM 정책을 사용합니다. 예를 들어 샌드박스 계정의 소규모 시스템은 프로젝트 팀 내에서 제어하도록 허용하지만 프로덕션 계정의 대규모 인스턴스에는 추가 승인 프로세스 및 액세스 제한이 있을 수 있습니다.

모범 사례 20.5 - 최적화 기회를 위해 사용량을 검토

정기적으로 SAP 워크로드를 검토하여 비용 최적화 기회를 식별합니다. 정기 검토는 다음 사항에 중점을 두어야 합니다. AWS 청구서와 SAP 워크로드 예산 간에 발견되는 차이 및 이상을 최소화, 모든 SAP 클라우드 리소스의 크기가 적절하고 과도하게 프로비저닝되지 않았는지 확인, SAP 워크로드의 비용 효율성을 향상시킬 수 있는 새로운 AWS 서비스 릴리스 또는 비용 절감을 이해.

제안 사항 20.5.1 – 초기 계획보다 사용량이 많은 경우 추가 비용을 최소화

계획되지 않은 비즈니스 이벤트 또는 추가로 필요한 성능으로 인해 클라우드 사용량이 예상 비용 모델을 초과하여 증가할 수 있습니다. 새로운 비용을 최적화하기 위해 이러한 변경 사항을 분석합니다. 변경 사항이 지속적인 경우 추가 Savings Plan 약정 또는 예약 인스턴스를 고려합니다.

단기간만 추가 용량이 필요한 경우 추가 비용을 최소화하기 위해 자동 크기 조정 또는 예약된 온디맨드 인스턴스 용량을 사용하는 수평적 확장 메커니즘(예: 추가 SAP 애플리케이션 서버)을 고려합니다.

제안 사항 20.5.2 – SAP 워크로드 사용량 지표를 검토하고 가능한 경우 추가로 적절히 크기 조정

SAP 시스템을 지원하는 구성 요소를 정기적으로 검토하여 적절한 크기인지 확인합니다. CloudWatch 지표를 사용하여 다음을 고려합니다.

- SAP EC2 컴퓨팅이 적절한 크기입니까? CPU 또는 메모리 사용률이 낮습니까? 더 작은 EC2 인스턴스 크기로 이동할 수 있습니까?
- SAP 스토리지가 적절한 크기입니까? 프로비저닝되었지만 사용되지 않은 초과 공간이 있습니까? 볼륨 크기를 줄일 수 있습니까?
- SAP 스토리지의 성능이 적절합니까? 줄일 수 있는 초과 IOPS 또는 MBps가 프로비저닝되었습니까?
- 백업 및 스냅샷이 적절하게 관리되고 있습니까? Amazon S3 Infrequently Accessed 또는 Amazon S3 Glacier에 아카이브할 수 있는 백업 복사본이 S3 Standard에 너무 많습니까?
- 최적화를 위한 추가 영역을 식별하려면 [AWS Compute Optimizer](#) 및 [AWS Trusted Advisor](#) 와 같은 도구를 사용합니다. SAP Note: [1656099 - AWS의 SAP 애플리케이션: DB/OS 및 Amazon EC2 제품 지원](#) [SAP 포털 액세스 권한 필요]에 따라 SAP 특정 컴퓨팅 및 스토리지 제한 사항을 인식합니다.

조사 결과를 사용하여 정기적으로 SAP 워크로드 구성 요소를 계속 적절한 크기로 조정하고 Savings Plans 및 예약 인스턴스 사용을 극대화합니다.

제안 사항 20.5.3 – 새로운 AWS 서비스를 이해하고 추가 비용 최적화를 달성할 수 있는 경우 구현을 계획

AWS는 정기적으로 새로운 서비스를 출시하고 주기적으로 가격을 인하합니다. 새로운 SAP on AWS 서비스 발표를 검토하고 최소 12개월마다 아키텍처에서 이를 활용할 계획을 수립합니다. AWS와의 Enterprise Support 계약의 일부로 테크니컬 어카운 관리자(TAM)가 있는 경우 정기 신규 서비스 브리핑 및 최적화 논의에서 도움을 받을 수 있습니다.

최신 발표 및 뉴스를 위해 [SAP on AWS 블로그](#) 및 [새로운 소식](#) 피드를 구독합니다.

SAP 워크로드의 지속적인 최적화에 대한 자세한 내용은 [운영 우수성]: [모범 사례 4.4 - 주기적 워크로드 검토를 수행하여 복원력, 성능, 민첩성 및 비용 최적화](#) 를 참조하세요.

결론

이 렌즈는 AWS에서 안정적이고 안전하며 효율적이면서 경제적인 SAP 워크로드를 설계, 구축, 운영하기 위한 아키텍처 관련 지침을 제공했습니다. 일반적인 패턴, 학습한 교훈, 포괄적인 SAP 설계 권장 사항을 살펴보았습니다.

이 프레임워크를 워크로드에 적용하면 견고하고 안정적이며 효율적인 시스템을 구축하는 데 큰 도움이 되므로, SAP 워크로드에서 높은 가치의 운영 작업에 집중하고 전문 영역의 한계를 넓히는 데 더욱 집중할 수 있습니다.

SAP 에코시스템은 애플리케이션, 도구 및 프로세스가 성장하고 성숙함에 따라 계속 진화합니다. AWS에서는 이러한 발전이 진행됨에 따라 이 글을 꾸준히 업데이트하여 SAP 애플리케이션이 Well-Architected가 되도록 돕고자 합니다.

도움 주신 분들

다음은 본 문서를 작성하는 데 도움을 준 개인 및 조직입니다.

- John Studdert: Amazon Web Services EMEA SAP 전문가 SA 관리자
- Peter Perbellini: Amazon Web Services APJ SAP 전문가 SA 선임 관리자
- Adam Hill: Amazon Web Services 수석 SAP 전문가 SA
- Nerys Olver: Amazon Web Services 선임 SAP 컨설턴트
- Wilson Puvvula: Amazon Web Services 선임 글로벌 어카운트 SA
- Christopher Spruell: Amazon Web Services 선임 글로벌 어카운트 SA
- Eneko Bilbao: Amazon Web Services 수석 SAP 전문가 SA
- Sabari Radhakrishnan: Amazon Web Services 수석 SAP 전문가 SA
- Somckit Khemmanivanh: Amazon Web Services EC2 Enterprise 부문 선임 시스템 개발 엔지니어
- Sander Bleijenbergh: Amazon Web Services ISV 부문 선임 SA
- Harpreet Singh: Amazon Web Services 파트너 SA 선임 관리자
- Manoj Muthukrishnan: Amazon Web Services 선임 SAP 전문가 SA
- Jongnam Lee: Amazon Web Services Well-Architected 데이터 분석 렌즈 부문 수석 SA
- Ben Potter: Amazon Web Services Well-Architected 보안 원칙 부문 수석 SA

문서 이력

이 백서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

변경 사항	설명	날짜
마이너 업데이트	연결되지 않는 링크가 수정되었습니다.	January 20, 2022
최초 게시	SAP Lens가 처음 게시되었습니다.	October 28, 2021

Note

RSS 업데이트를 구독하려면 사용 중인 브라우저에서 RSS 플러그인이 활성화되어 있어야 합니다.

원칙별로 배열된 설계 원칙

다음은 이 백서에 설명된 설계 원칙을 AWS Well-Architected Framework의 원칙별로 정리한 것입니다.

운영 우수성

- 1 - 상태를 이해하고 대응할 수 있도록 SAP 워크로드를 설계
- 2 - SAP 변경의 결함 축소, 수정 용이화 및 워크플로 개선
- 3 - 워크로드가 어떻게 작동할지 이해
- 4 - 정기적으로 SAP 워크로드 검증 및 개선

보안

- 5 - 보안 표준 및 SAP 워크로드에 해당 표준이 적용되는 방식 이해
- 6 - 인프라 및 소프트웨어 제어를 사용하여 보안 구성 오류 감소
- 7 - 자격 증명 및 권한을 통해 SAP 워크로드에 대한 액세스 제어
- 8 - 저장 및 전송 중 SAP 데이터 보호
- 9 - 보안 이벤트 로그, 테스트 및 대응을 위한 보안 전략 구현

안정성

- 10 - 내결함 설계
- 11 - 장애 탐지 및 대응
- 12 - 데이터 복구 계획

성능 효율성

- 13 - 최적의 컴퓨팅 솔루션 선택
- 14 - 최적 스토리지 솔루션 선택
- 15 - 운영 체제, 데이터베이스 및 SAP 애플리케이션 계층에 대한 튜닝 옵션 평가
- 16 - 지속적인 성능 및 최적화 옵션 이해

비용 최적화

- 17 - SAP 아키텍처 패턴에서 비용 효율성 평가
- 18 - 비용 효율성을 위한 SAP 컴퓨팅 리소스 평가
- 19 - 스토리지 비용 효율성을 위해 SAP 데이터 사용 최적화
- 20 - 가시성, 계획 및 거버넌스로 비용 관리

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.

© 2022 Amazon Web Services, Inc. 및/또는 자회사. All rights reserved.

AWS Glossary

For the latest AWS terminology, see the [AWS glossary](#) in the AWS 용어집 Reference.