IBM Security Verify (IBM Güvenlik Doğrulaması)

Bu Hizmet Tanımında, Bulut Hizmeti açıklanır. Müşterinin siparişine ilişkin fiyatlandırma ve ek ayrıntıları geçerli sipariş belgelerinde sağlanır.

1. Bulut Hizmeti

IBM Cloud Identity, dahili (çalışanlar) ve harici kullanıcı tipleri için Tek Oturum Açma (SSO), çok faktörlü kimlik doğrulama ve kimlik yaşam döngüsü denetimleri sağlar.

1.1 Olanaklar

Müşteri, aşağıda belirtilen mevcut olanaklar arasından seçim yapabilir.

1.1.1 IBM Security Verify

IBM Security Verify, Müşterilerin, bulutta sunulan, Tek Oturum Açma, çok faktörlü kimlik doğrulaması, yaşam döngüsü yönetimi, uyarlanabilir kimlik doğrulaması, tek bir parça numarası altında kimlik analitiği ve kimlik yönetişimi ile kullanıcıların üretkenliğini güvence altına almalarına yardımcı olur. Bu Bulut Hizmeti aynı zamanda, şirket içi uygulamaların bütünleştirilmesine yardımcı olmak amacıyla sık kullanılan bulut hizmeti uygulamalarına ve önceden oluşturulmuş şablonlara erişim sağlanmasına yardımcı olmak için önceden oluşturulmuş binlerce bağlayıcıyı destekler.

- Tek Oturum Açma

  Bu Bulut Hizmeti; Tek Oturum Açma (SSO) ve Open ID Connect (OIDC), bulut tabanlı API kimlik doğrulaması için Hizmet Olarak Sunulan Kimlik Doğrulaması, bir uygulama başlatma bölmesi, sistem yöneticisi raporlama ve analitik gösterge panosu sağlar. Bu Bulut Hizmeti, yaygın uygulamalar için yüzlerce bağlayıcı dahil olmak üzere modern standartlara dayalı kimlik doğrulaması ve birleştirme protokollerini kullanarak kullanıcıları uygulamalara bağlar. Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, etkinleştirme yazılımı olarak dahil edilen şirket içi IBM Security Verify Access yazılım programı ve IBM Security Verify Application Gateway yazılım programı ile güçlü bir şekilde bütünleşir.

- Çok Faktörlü Kimlik Doğrulaması

  Bu Bulut Hizmeti, Cloud Identity Connect tarafından korunan uygulamalar için veya doğrudan API çağırma aracılığıyla ve bir dijital hizmete erişirken kimliklerini doğrulamak amacıyla RADIUS istemcileri, Unix/Linux PAM sunucuları ve Windows sunucuları dahil olmak üzere diğer uygulama noktaları için çok faktörlü kimlik doğrulaması sağlar. Buna e-posta, SMS ve süreli (yazılım tokeni) tek kullanımlık parolalar gibi mekanizmalar ve gücünü IBM Verify'dan alan anlık bildirim tabanlı mobil biyometrik kimlilik doğrulaması dahildir. Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, şirket içi IBM Security Verify Access yazılım programı ile bütünleşir.

- Uyarlanabilir Erişim

  Bu Bulut Hizmeti, bir kullanıcının hizmetle korunan bir uygulamaya erişmeye çalışması halinde, kuruluşların, kötü amaçlı kullanıcılar ile gerçek kullanıcıları birbirinden doğru olarak ayırt etmesine yardımcı olmak için Tehdit İstihbaratı ile Yapay Zekanın bir bileşimini kullanır. Hizmet, gerçek zamanlı risk azaltma eylemini belirlemek amacıyla kullanıcılar, onların aygıtları ve davranış kalıpları hakkındaki içgörüleri kullanır. Risk azaltma eylemleri arasında erişime izin verme, kimlik doğrulamasını uygulama veya erişimi engelleme yer alır. Hizmet, aygıtta parmak izi oluşturmak ve oturumun bütünsel risk seviyesini hesaplamak için son kullanıcının aygıtından toplanan bağlamsal bilgileri ve yüzlerce veri noktasını kullanır. Erişim ilkesinde tanımlanan risk tabanlı erişim kuralları, sistemin eylemini belirlemek amacıyla ek parametrelerle birlikte oturumun risk seviyesini kullanır. Bu hizmet, Security Verify sistem yöneticisi raporlarıyla, erişim ilkesi kuralları düzenleyicisiyle ve çok faktörlü kimlik doğrulaması hizmetiyle sıkı bir şekilde bağlantılıdır.

- Yaşam Döngüsü Yönetimi ve Yönetişimi

  Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan kimlik yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, etkinleştirme yazılımı olarak dahil edilen şirket içi IBM Security Identity Governance and Intelligence (IGI) ve IBM Security Identity Manager (ISIM) yazılım programı ile güçlü bir şekilde bütünleşir. Bu Bulut Hizmeti, kuruluşlara, hesap eşitlemesi, uygulama erişim isteği iş akışı, erişim sertifikasyonu, bulut ve şirket içi uygulamalar için ortamın hazırlanması gibi işlemleri içeren bulut içinde gelişmiş kimlik yaşam döngüsü yönetimi yetenekleri sağlar. Müşteriler, IBM Security Verify Account Synchronization'ı bir eklenti hizmeti olarak dahil edebilirler.

- Analitik

  Bu Bulut Hizmeti, yönetilen kullanıcılara yönelik bütünsel bir risk profili sağlamak için IBM Security Identity Governance and Intelligence (IGI) ve IBM Security Identity Manager (ISIM) gibi mevcut IBM çözümlerini geliştirir. Bu Bulut Hizmeti, çeşitli kaynaklardan gelen etkinlik ve yetki verilerini işleyen ve bu risk içgörüleri temelinde harekete geçme yeteneği sunarak erişim risklerine 360 derecelik görünüm sağlayan şirket içi ve çok amaçlı bir analitik motoru içerir.

1.1.2 IBM Cloud Identity Connect

Bu Bulut Hizmeti; Tek Oturum Açma (SSO) ve Open ID Connect (OIDC), bulut tabanlı API kimlik doğrulaması için Hizmet Olarak Sunulan Kimlik Doğrulaması, bir uygulama başlatma bölmesi, sistem yöneticisi raporlama ve analitik gösterge panosu sağlar. Bu Bulut Hizmeti, yaygın uygulamalar için yüzlerce bağlayıcı dahil olmak üzere modern standartlara dayalı kimlik doğrulaması ve birleştirme protokollerini kullanarak kullanıcıları uygulamalara bağlar. Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, etkinleştirme yazılımı olarak dahil edilen şirket içi IBM Security Access Management (ISAM) yazılım programı ile güçlü bir şekilde bütünleşir.

1.1.3 IBM Cloud Identity Connect for ISAM (ISAM İçin IBM Bulut Kimliği Bağlantısı)

Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, şirket içi IBM Security Access Management (ISAM) yazılım programı ile güçlü bir şekilde bütünleşir. Bu Bulut Hizmeti, Müşterinin, IBM Security Access Management (ISAM) programı için aktif bir Yazılım Aboneliği ve Destek yetkisine sahip olmasını gerektirir. Abonelik ve Destek, Müşterinin Bulut Hizmeti aboneliği süresi boyunca aktif kalmalıdır. Müşterinin bu Bulut Hizmetine ilişkin yetkisi, Müşterinin şirket içi ISAM lisansı yetkisi ile eşdeğer olmalıdır. Müşterinin Yazılım Aboneliği ve Destek hizmetinin sona erdirilmesi, bu Bulut Hizmetinin de sona erdirilmesine yol açacaktır. Madde 5.2'de tanımlanan etkinleştirme yazılımına erişim, bu Bulut Hizmetine dahil değildir.

1.1.4 IBM Cloud Identity Essentials (IBM Bulut Kimliği Esasları)

Bu Bulut Hizmeti, kullandığı çeşitli IBM uygulamaları ve genel erişime açık bulut uygulamaları için Müşterilere Tek Oturum Açma (SSO) yetenekleri sağlar. Bu Bulut Hizmeti, koşullu erişim gibi ek güvenlik kontrolü seviyeleri sağlamak amacıyla IBM'in MaaS360 ürünüyle birlikte kullanılabilir.

1.1.5 IBM Cloud Identity Verify (IBM Bulut Kimliği Doğrulaması)

Bu Bulut Hizmeti, Cloud Identity Connect tarafından korunan uygulamalar için veya doğrudan API çağırma aracılığıyla ve bir dijital hizmete erişirken kimliklerini doğrulamak amacıyla RADIUS istemcileri, Unix/Linux PAM sunucuları ve Windows sunucuları dahil olmak üzere diğer uygulama noktaları için çok faktörlü kimlik doğrulaması sağlar. Buna e-posta, SMS ve süreli (yazılım tokeni) tek kullanımlık parolalar gibi mekanizmalar ve gücünü IBM Verify'dan alan anlık bildirim tabanlı mobil biyometrik kimlilik doğrulaması dahildir. Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, şirket içi IBM Security Access Management (ISAM) yazılım programı ile bütünleşir. Bağımsız olarak ya da Cloud Identity Connect, Cloud Identity Connect for ISAM ve Cloud Identity Essentials için tamamlayıcı olarak mevcuttur.

1.1.6 IBM Cloud Identity Govern (IBM Bulut Kimliği Yönetişimi)

Bu Bulut Hizmeti, Müşterilerin, hem kendi şirket içi uygulamalarına hem de bulut uygulamalarına yayılan erişim yönetimi için iş kollarının taleplerini desteklemek amacıyla Müşterilere bir çözüm sağlamak üzere, etkinleştirme yazılımı olarak dahil edilen şirket içi IBM Security Identity Governance and Intelligence (IGI) and IBM Security Identity Manager (ISIM) yazılım programı ile güçlü bir şekilde bütünleşir. Bu Bulut

Hizmeti, kuruluşlara, uygulama erişim isteği iş akışını içeren bulut içinde gelişmiş kimlik yaşam döngüsü yönetimi sağlar.

1.1.7 IBM Cloud Identity Connect and Verify (IBM Bulut Kimliği Bağlantısı ve Doğrulaması)

Bu Bulut Hizmeti, IBM Cloud Identity Connect ile IBM Cloud Identity Verify ürünlerinin işlevlerini Müşteriye tek olanak olarak sunar.

1.1.8 IBM Cloud Identity Analyze (IBM Bulut Kimliği Analizi)

Bu Bulut Hizmeti, yönetilen kullanıcılara yönelik bütünsel bir risk profili sağlamak için IBM Security Identity Governance and Intelligence (IGI) ve IBM Security Identity Manager (ISIM) gibi mevcut IBM çözümlerini geliştirir. Bu Bulut Hizmeti, çeşitli kaynaklardan gelen etkinlik ve yetki verilerini işleyen ve bu risk içgörüleri temelinde harekete geçme yeteneği sunarak erişim risklerine 360 derecelik görünüm sağlayan şirket içi ve çok amaçlı bir analitik motoru içerir.

1.1.9 IBM Cloud Identity Adaptive Access (IBM Bulut Kimliğine Uyarlanabilir Erişim)

Bu Bulut Hizmeti, kuruluşların doğru kimlik doğrulama ilkelerini uygulamasına yardımcı olmak üzere kullanıcılara, onların aygıtlarına ve davranış kalıplarına yönelik Yapay Zeka destekli bağlamsal içgörülerden yararlanır.

1.1.10 IBM Cloud Identity Connect Verify and Govern (IBM Bulut Kimliği Bağlantısı Doğrulaması ve Yönetimi)

Bu Bulut Hizmeti, IBM Cloud Identity Connect, IBM Cloud Identity Verify ve IBM Cloud Identity Govern ürünlerinin işlevlerini Müşteriye tek olanak olarak sunar.

1.2 İsteğe Bağlı Hizmetler

1.2.1 IBM Security Verify Non-Production (IBM Güvenlik Doğrulaması - Üretim Dışı)

IBM Security Verify Non-Production Environment on Cloud, IBM Security Verify platformunun ayrı bir eşgörünümüdür ve Müşteri tarafından yalnızca testler, performans ayarlaması, hata tanılaması, dahili karşılaştırmalı değerlendirme, üretime hazırlık kalite güvence faaliyeti ve/veya yayınlanmış uygulama programlama arabirimleri kullanılarak Bulut Hizmeti için dahili olarak kullanılan ekler ya da uzantılar geliştirilmesi dahil, ancak tamamı bunlarla sınırlı olmamak üzere üretim amaçlı olmayan dahili faaliyetlerde kullanılabilir. Bu Bulut Hizmeti, Hizmet Seviyeleri ve Teknik Destek başlıklı Madde 3'ün koşullarına tabi olarak, kullanılabilirliğe ilişkin hizmet seviyesi sözleşmesini dahil etme seçeneğine sahiptir. Bu Bulut Hizmeti, saniyede 100 Olaylık kapasiteye sahiptir.

1.2.2 IBM Security Verify Vanity (IBM Güvenlik Doğrulaması - Özel)

Bir kurumsal etki alanı (bir etki alanı), Müşterinin platform tarafından kullanıma hazır olarak sağlanan varsayılan kiracı etki alanı yerine kendi kuruluşuna ait ve kuruluşu ile daha ilgili bir etki alanını kullanmasına olanak sağlar. Bu etki alanı için IBM tarafından bir SSL sertifikası sağlanacaktır ve yıllık olarak yenilenecektir.

1.2.3 IBM Security Verify Application Gateway Hosted (IBM Güvenlik Doğrulaması - Barındırılan Uygulama Ağ Geçidi)

Uygulama ağ geçidi, standart olmayan veya eski kimlik doğrulama mekanizmaları için destek arayan Müşteriler için IBM tarafından yönetilen ve barındırılan basit bir araç sağlar. Bu mekanizmalar LTPA ve HTTP üst bilgisi tabanlı kimlik doğrulamasını içerir. Sürekli izleme ve bakım IBM tarafından yönetilir.

1.2.4 IBM Security Verify SMS and Email One-time Password (IBM Güvenlik Doğrulaması - SMS ve E-postayla Gönderilen Bir Kerelik Parola)

Hizmet, ikinci kimlik doğrulama mekanizması olarak e-posta ve SMS ile gönderilen bir kerelik parola sağlar.

1.2.5 IBM Security Verify Account Synchronization (IBM Güvenlik Doğrulaması - Hesap Eşitlemesi)

Hesap eşitlemesi, ortam sağlanması için yapılandırılan hedef uygulamalardaki hesapların Security Verify'a getirildiği süreçtir. Bu süreç, mevcut hesap ayrıntılarında doğrulama gerçekleştirir, sistemi hedef uygulamayla tutarlı bir şekilde tutmak için benimseme ve iyileştirme ilkelerini uygular.

1.2.6 IBM Cloud Identity Non-Production (IBM Bulut Kimliği - Üretim Dışı)

IBM Cloud Identity Non-Production Environment on Cloud, IBM Cloud Identity platformunun ayrı bir eşgörünümüdür ve Müşteri tarafından yalnızca testler, performans ayarlaması, hata tanılama, dahili

karşılaştırmalı değerlendirme, hazırlık kalite güvence faaliyeti ve/veya yayınlanmış uygulama programlama arabirimleri kullanılarak Bulut Hizmeti için dahili olarak kullanılan ekler ya da uzantılar geliştirilmesi dahil, ancak tamamı bunlarla sınırlı olmamak üzere üretim amaçlı olmayan dahili faaliyetlerde kullanılabilir. Bu Bulut Hizmeti, Hizmet Seviyeleri ve Teknik Destek başlıklı Madde 3'ün koşullarına tabi olarak, kullanılabilirliğe ilişkin hizmet seviyesi sözleşmesini dahil etme seçeneğine sahiptir. Bu Bulut Hizmeti, saniyede 100 Olaylık kapasiteye sahiptir.

1.2.7 IBM Cloud Identity Vanity Domain (IBM Bulut Kimliği Kurumsal Etki Alanı)

Bir kurumsal etki alanı (bir etki alanı), Müşterinin platform tarafından kullanıma hazır olarak sağlanan varsayılan kiracı etki alanı yerine kendi kuruluşuna ait ve kuruluşu ile daha ilgili bir etki alanını kullanmasına olanak sağlar. Bu etki alanı için IBM tarafından bir SSL sertifikası sağlanacaktır ve yıllık olarak yenilenecektir.

1.2.8 IBM Cloud Identity Application Gateway Hosted (IBM Bulut Kimliği Barındırılan Uygulama Ağ Geçidi)

Uygulama ağ geçidi, standart olmayan veya eski kimlik doğrulama mekanizmaları için destek arayan Müşteriler için IBM tarafından yönetilen ve barındırılan basit bir araç sağlar. Bu mekanizmalar LTPA ve HTTP üst bilgisi tabanlı kimlik doğrulamasını içerir. Sürekli izleme ve bakım IBM tarafından yönetilir.

1.3 Hızlandırma Hizmetleri

1.3.1 IBM Security Verify Solution Planning (IBM Güvenlik Doğrulaması - Çözüm Planlaması)

Bu hizmet, bir (1) haftalık profesyonel hizmetler sağlar ve IBM, bu süre içinde aşağıda belirtilenlerden bazılarını ya da tamamını yerine getirecektir:

- Bulut tabanlı hizmet olarak sunulan yazılım uygulamaları için tek oturum açmanın oluşturulması
- Kolay uygulama lokasyonu için bir başlatma bölmesinin yapılandırılması
- Uygulamaların hazır bağlayıcılarla bağlanması
- Çözümün planlanması, mimari ve rehberlik
- IBM tarafından önerilen yaklaşım ve uygulamalar

1.3.2 IBM Security Verify Workshop for Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulaması İçin IBM Güvenlik Doğrulaması Çalıştayı)

Bu hizmet, çok faktörlü kimlik doğrulamasının zorluklarına ve IBM Cloud Identify Verify kullanılarak bir Müşterinin uygulamalarının güvenliğinin sağlanmasına ilişkin üç (3) günlük bir profesyonel hizmetler çalıştayı sağlar. Çalıştay, aşağıda belirtilenlerden bazılarını ya da tamamını kapsayacaktır:

- Tanıdık kimlik doğrulamasının, kimlik doğrulaması gerektiren tüm dijital ve yüz yüze etkileşimlerde yerleşik hale getirilmesi
- Geliştirici dostu REST API kullanılarak bir uygulamanın güçlü kimlik doğrulaması uygulamasının sağlanması
- Kimlik güvenliğine ilişkin sektördeki en iyi uygulama önerilerinin sağlanması
- Telefonlar, tabletler ve dizüstü bilgisayarlar dahil olmak üzere tüm biçim katsayıları üzerinde hızlandırılmış kullanıcı deneyimi ve kullanmaya başlama

1.3.3 IBM Security Verify Strategy and Planning (IBM Güvenlik Doğrulaması - Strateji ve Planlama)

Bu hizmet, altyapı ve uygulama güvenliğine odaklı bir biçimde, bulut güvenliği en iyi uygulamalarının nasıl uygulanacağına ilişkin üç (3) haftalık bir profesyonel hizmetler çalıştayı sağlar. Çalıştay, aşağıda belirtilenlerden bazılarını ya da tamamını kapsayacaktır:

- Bulut tabanlı hizmet olarak sunulan yazılım uygulamaları için tek oturum açmanın oluşturulması
- Kolay uygulama lokasyonu için bir başlatma bölmesinin yapılandırılması
- Uygulamaların hazır bağlayıcılarla bağlanması
- Çözümün planlanması, mimari ve rehberlik
- Siber güvenlik alanındaki yeni eğilimlere ilişkin içgörüler
- IBM tarafından önerilen yaklaşım ve uygulamalar

1.3.4 IBM Security Verify Expert On Demand (İsteğe Bağlı IBM Güvenlik Doğrulaması Uzmanı)

Bu hizmet, başlangıç tarihinden itibaren otuz (30) gün içerisinde iki (2) saatlik oturumlar biçiminde sağlanan yirmi (20) saatlik profesyonel hizmetler sunar. Hizmetler, soruların yanıtlanması için bir IBM Security Verify mimarı ve aşağıda belirtilenler dahil, ancak tamamı bunlarla sınırlı olmamak üzere rehberlik ve öneriler sağlayacaktır:

- Bir Müşterinin çözümünün uygulanmasının desteklenmesi için teknik beceriler
- Müşterinin çözümünün mimarisine ve uygulanmasına ilişkin sorular
- Müşterinin çözümüne ve/veya stratejisine ilişkin rehberlik

1.3.5 IBM Cloud Identity Connect Solution Planning (IBM Bulut Kimliği Bağlantısı Çözüm Planlaması)

Bu hizmet, bir (1) haftalık profesyonel hizmetler sağlar ve IBM, bu süre içinde aşağıda belirtilenlerden bazılarını ya da tamamını yerine getirecektir:

- Bulut tabanlı hizmet olarak sunulan yazılım uygulamaları için tek oturum açmanın oluşturulması
- Kolay uygulama lokasyonu için bir başlatma bölmesinin yapılandırılması
- Uygulamaların hazır bağlayıcılarla bağlanması
- Çözümün planlanması, mimari ve rehberlik
- IBM tarafından önerilen yaklaşım ve uygulamalar

1.3.6 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulaması İçin IBM Bulut Kimliği Doğrulaması Çalıştayı)

Bu hizmet, çok faktörlü kimlik doğrulamasının zorluklarına ve IBM Cloud Identify Verify kullanılarak bir Müşterinin uygulamalarının güvenliğinin sağlanmasına ilişkin üç (3) günlük bir profesyonel hizmetler çalıştayı sağlar. Çalıştay, aşağıda belirtilenlerden bazılarını ya da tamamını kapsayacaktır:

- Tanıdık kimlik doğrulamasının, kimlik doğrulaması gerektiren tüm dijital ve yüz yüze etkileşimlerde yerleşik hale getirilmesi
- Geliştirici dostu REST API kullanılarak bir uygulamanın güçlü kimlik doğrulaması uygulamasının sağlanması
- Kimlik güvenliğine ilişkin sektördeki en iyi uygulama önerilerinin sağlanması
- Telefonlar, tabletler ve dizüstü bilgisayarlar dahil olmak üzere tüm biçim katsayıları üzerinde hızlandırılmış kullanıcı deneyimi ve kullanmaya başlama

1.3.7 IBM Cloud Security Strategy and Planning (IBM Bulut Güvenliği Stratejisi ve Planlaması)

Bu hizmet, altyapı ve uygulama güvenliğine odaklı bir biçimde, bulut güvenliği en iyi uygulamalarının nasıl uygulanacağına ilişkin üç (3) haftalık bir profesyonel hizmetler çalıştayı sağlar. Çalıştay, aşağıda belirtilenlerden bazılarını ya da tamamını kapsayacaktır:

- Bulut tabanlı hizmet olarak sunulan yazılım uygulamaları için tek oturum açmanın oluşturulması
- Kolay uygulama lokasyonu için bir başlatma bölmesinin yapılandırılması
- Uygulamaların hazır bağlayıcılarla bağlanması
- Çözümün planlanması, mimari ve rehberlik
- Siber güvenlik alanındaki yeni eğilimlere ilişkin içgörüler
- IBM tarafından önerilen yaklaşım ve uygulamalar

1.3.8 IBM Cloud Identity Expert On Demand (İsteğe Bağlı IBM Bulut Kimliği Uzmanı)

Bu hizmet, başlangıç tarihinden itibaren otuz (30) gün içerisinde iki (2) saatlik oturumlar biçiminde sağlanan yirmi (20) saatlik profesyonel hizmetler sunar. Hizmetler, soruların yanıtlanması için bir Cloud Identity mimarı ve aşağıda belirtilenler dahil, ancak tamamı bunlarla sınırlı olmamak üzere rehberlik ve öneriler sağlayacaktır:

- Bir Müşterinin Cloud Identity çözümünün uygulanmasının desteklenmesi için teknik beceriler
- Müşterinin Cloud Identity çözümünün mimarisine ve uygulanmasına ilişkin sorular
- Müşterinin Cloud Identity çözümüne ve/veya stratejisine ilişkin rehberlik

2. Veri İşleme ve Veri Koruma Sayfaları

IBM'in http://ibm.com/dpa adresinde yer alan Veri İşleme Ek Sözleşmesi ile aşağıda belirtilen bağlantılarda yer alan Veri İşleme ve Veri Koruma Veri Sayfası/Sayfaları (veri sayfası/sayfaları ya da Veri İşleme Ek Sözleşmesi Eki/Ekleri olarak anılır), işlenebilecek İçerik türleri, ilgili işleme etkinlikleri, veri koruma özellikleri ve İçeriğin saklanmasına ve iadesine ilişkin belirli bilgiler dahil olmak üzere Bulut Hizmetlerine ve seçeneklerine ilişkin ek veri koruma bilgileri sağlar. İçerikte yer alan kişisel veriler için, i) Avrupa Genel Veri Koruma Yönetmeliği'nin (EU/2016/679) (GDPR veya GVKY) ya da ii) http://ibm.com/dpa/dpl adresinde belirtilen diğer veri koruma kanunlarının geçerli olması halinde ve geçerli olduğu ölçüde, Veri İşleme Ek Sözleşmesi geçerli olur.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

3. Hizmet Seviyeleri ve Teknik Destek

3.1 Hizmet Seviyesi Sözleşmesi

IBM, Müşteriye aşağıda belirtilen kullanılabilirlik hizmet seviyesi sözleşmesini sağlar. IBM, aşağıdaki tabloda gösterildiği şekilde, Bulut Hizmetinin kümülatif kullanılabilirliği doğrultusunda geçerli olan en yüksek telafi ücretini uygulayacaktır. Kullanılabilirlik oranı, sözleşmenin yürürlükte olduğu bir ay içindeki toplam dakika sayısından sözleşmenin yürürlükte olduğu bir ay içindeki toplam Hizmet Kapalı Kalma Süresi dakikalarının sayısı çıkarılarak ve sonuç sözleşmenin yürürlükte olduğu bir ay içindeki toplam dakika sayısına bölünerek hesaplanır ve etkilenen bölgeye ve bu bölgede abone olan kullanıcıların sayısına özeldir. Hizmet Kapalı Kalması tanımı, ödeme talebi süreci ve hizmetin kullanılabilirliğine ilişkin sorunlar için IBM ile nasıl iletişim kurulacağı, https://www.ibm.com/software/support/saas_support_overview.html adresinde yer alan IBM Hizmet Olarak Sunulan Yazılım desteğine genel bakış sayfasında belirtilmiştir.

Kullanılabilirlik	Alacak (aylık abonelik ücretine oranı*)
%99,9'dan daha az	%10

* Abonelik ücreti, ödeme talebine konu olan ay için sözleşmede belirtilen fiyattır.

3.1.1 Bu Hizmet Seviyesi Sözleşmesine ilişkin diğer bilgiler

Müşteri, süresinin ilk altmış (60) günü boyunca ("Deneme Süresi"), bu Sözleşme kapsamında IBM Cloud Service ortamının en az %99,9'luk Çalışma Süresi Yüzdesine ulaşamaması nedeniyle herhangi bir alacağa hak kazanmayacaktır. IBM, Deneme Süresinden önce veya Deneme Süresi boyunca Bulut Hizmetine geçişi yapılması planlanan mevcut Müşteri yapılandırmaları, ilkeleri, verileri veya kodları ("Önceden Var Olan Bileşenler") belirlerse (bu durumda, Bulut Hizmetinin bu Sözleşme kapsamında Çalışma Süresine başarılı bir şekilde ulaşması engellenmiş olacaktır), IBM'in bu Önceden Var Olan Bileşenleri Müşteriye bildirme ve yalnızca kendi tek taraflı takdirine bağlı olarak bunları Hizmet Seviyesi Sözleşmesinde sağlanacaklardan muaf tutma hakkı saklı olacaktır. IBM, muaf tutulmuş Önceden Var Olan Bileşenleri Müşteriye bildirirse, mümkün olan ölçüde Müşteriye bir iyileştirme planı sunmaktan sorumlu olacaktır. Bu da, bu tür muaf tutulmuş bileşenlerin bu Sözleşmenin Çalışma Süresi Yüzdesini karşılamasını sağlar. Taraflarca aksi kararlaştırılmadıkça, söz konusu iyileştirmenin maliyetinden yalnızca Müşteri sorumlu olacaktır.

3.2 Teknik Destek

Destek iletişim bilgileri, önem dereceleri, desteğin sağlanacağı saatler, müdahale süreleri ve diğer destek bilgileri ile süreçleri dahil olmak üzere Bulut Hizmetine ilişkin teknik destek, https://www.ibm.com/support/home/pages/support-guide/ adresinde yer alan IBM destek kılavuzunda Bulut Hizmeti seçilerek bulunabilir.

4. Ücretler

4.1 Ücret Ölçüleri

Bulut Hizmeti için ücret ölçüsü/ölçüleri, İşlem Belgesinde belirtilir.

Bu Bulut Hizmeti için aşağıda belirtilen ücret ölçüleri geçerlidir:

- Eşgörünüm, Bulut Hizmetlerinin belirli bir yapılandırmasına olan her erişimi ifade eder.
- Taahhüt, Bulut Hizmetleri ile bağlantılı bir profesyonel hizmet ya da eğitim hizmetidir.
- Olay, Bulut Hizmetleri tarafından işlenen veya Bulut Hizmetlerinin kullanımıyla bağlantılı belirli bir olayın gerçekleşmesini ifade eder.
    - Security Verify SMS ve Bir Kerelik Parolası için bir Olay, e-postayla veya SMS ile gönderilen bir kerelik paroladır.
    - Cloud Identity Connect için bir Olay, Bulut Hizmetine yönelik bir http isteğidir.
- Cloud Identity Verify için bir Olay, Bulut Hizmeti aracılığıyla başlatılan herhangi bir çok faktörlü yöntemdir. Yetkili Kullanıcı, Bulut Hizmetlerine doğrudan veya dolaylı olarak herhangi bir araçla (örneğin, bir multipleks programı, aygıtı veya uygulama sunucusu aracılığıyla) herhangi bir şekilde erişme yetkisine sahip olan tek bir kullanıcıdır.
- Çalışan, Bulut Hizmetlerine erişim verilmiş olsun veya olmasın, Müşteri Teşebbüsü tarafından çalıştırılan veya başka bir şekilde ödemesi yapılan veya Müşteri Teşebbüsü adına hareket eden tek bir kişidir.
- Hak Kazanan Katılımcı, Bulut Hizmetleri tarafından yönetilen ya da izlenen herhangi bir hizmet sağlama programına katılmaya hak kazanan bir gerçek ya da tüzel kişidir.
- Kaynak Birimi, Bulut Hizmeti tarafından yönetilen, işlenen veya Bulut Hizmetinin kullanımıyla bağlantılı olan bir kaynağın bağımsız bir ölçüsünü ifade eder.

  Her işlevsel yeteneğin kullanımı için bu Bulut Hizmeti aboneliğine ilişkin belirlenen sayıda Kaynak Birimi yetkisi gerekir.

		Her Kullanıcı için gereken ağırlıklı Kaynak Birimindeki İşlevsel Yetenek				
Kademeli Seviye (Graduated Tier)	**Azami Aylık Aktif Kullanıcı**	**Tek Oturum Açma**	**Çok Faktörlü Kimlik Doğrulaması**	**Uyarlanabilir Erişim**	**Yaşam Döngüsü Yönetimi ve Yönetişimi**	**Analitik**
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5.000	0,0800	0,0800	0,0800	0,0750	0,1000
3	10.000	0,0600	0,0600	0,0600	0,0500	0,0750
4	100.000	0,0080	0,0080	0,0080	0,0050	0,0200
5	500.000	0,0025	0,0025	0,0025	0,0020	0,0150
6	1.000.000	0,0020	0,0020	0,0020	0,0010	0,0010
7	5.000.000	0,0015	0,0015	0,0015	0,0005	0,0005
8	10.000.000	0,0015	0,0015	0,0015	0,0002	0,0002
9	50.000.000	0,0010	0,0010	0,0010	0,0001	0,0001
10	999.999.999	0,0005	0,0005	0,0005	0,0001	0,0001

Not: Tüm hesaplamalar, tam sayıya yuvarlanacaktır.

5. Ek Koşullar

1 Ocak 2019 tarihinden önce imzalanmış olan Bulut Hizmeti Sözleşmeleri (ya da eşdeğer çerçeve bulut sözleşmeleri) için https://www.ibm.com/acs adresinde yer alan koşullar geçerlidir.

5.1 Müşteri Referansı

Müşteri, IBM'in bir basın veya pazarlama iletişiminde Müşteriyi Bulut Hizmetlerinin bir abonesi olarak kamuya açık bir şekilde referans verebileceğini kabul eder.

5.2 Etkinleştirme Yazılımı

Bulut Hizmeti aşağıda belirtilen Etkinleştirme Yazılımlarını içerir:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login
- IBM Security Verify Gateway for PAM (on AIX)
- IBM Security Verify Gateway for PAM
- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials (IBM Güvenlik Doğrulaması Kimlik Bilgileri)

Aşağıda belirtilen etkinleştirme yazılımı, yalnızca IBM Cloud Identity Connect (IBM Cloud Kimlik Bağlantısı), IBM Cloud Identity Connect and Verify (IBM Cloud Kimlik Bağlantısı ve Doğrulaması) ve IBM Cloud Identity Connect Verify and Govern (IBM Cloud Kimlik Bağlantısı Doğrulaması ve Yönetişimi) Bulut Hizmetleriyle birlikte kullanılabilir:

- IBM Security Access Manager Virtual Enterprise Edition (IBM Güvenlik Erişim Yöneticisi Sanal Kurumsal Sürümü)

Aşağıda belirtilen etkinleştirme yazılımı, yalnızca IBM Security Verify, IBM Cloud Identity Govern, IBM Cloud Identity Connect Verify and Govern Bulut Hizmetleriyle birlikte kullanılabilir:

- IBM Security Identity Governance and Intelligence Enterprise Edition (IBM Güvenlik Kimlik Yönetişimi ve İstihbaratı Kurumsal Sürüm)
- IBM Security Identity Manager (IBM Güvenlik Kimliği Yöneticisi)

Kabul eden:	Kabul eden:
{Müşteri Şirketinin Ticari Unvanı adına} ("Müşteri")	**{İlgili IBM Şirketinin Ticarı Unvanı adına} ("IBM")**
İmza_____	İmza_____
Yetkili imza	Yetkili imza
Unvan:	Unvan:
İsim (el yazısı veya daktiloyla):	İsim (el yazısı veya daktiloyla):

Tarih:	Tarih:
Müşteri Numarası:	Sözleşme Numarası:
Müşteri Adresi:	IBM Adresi: