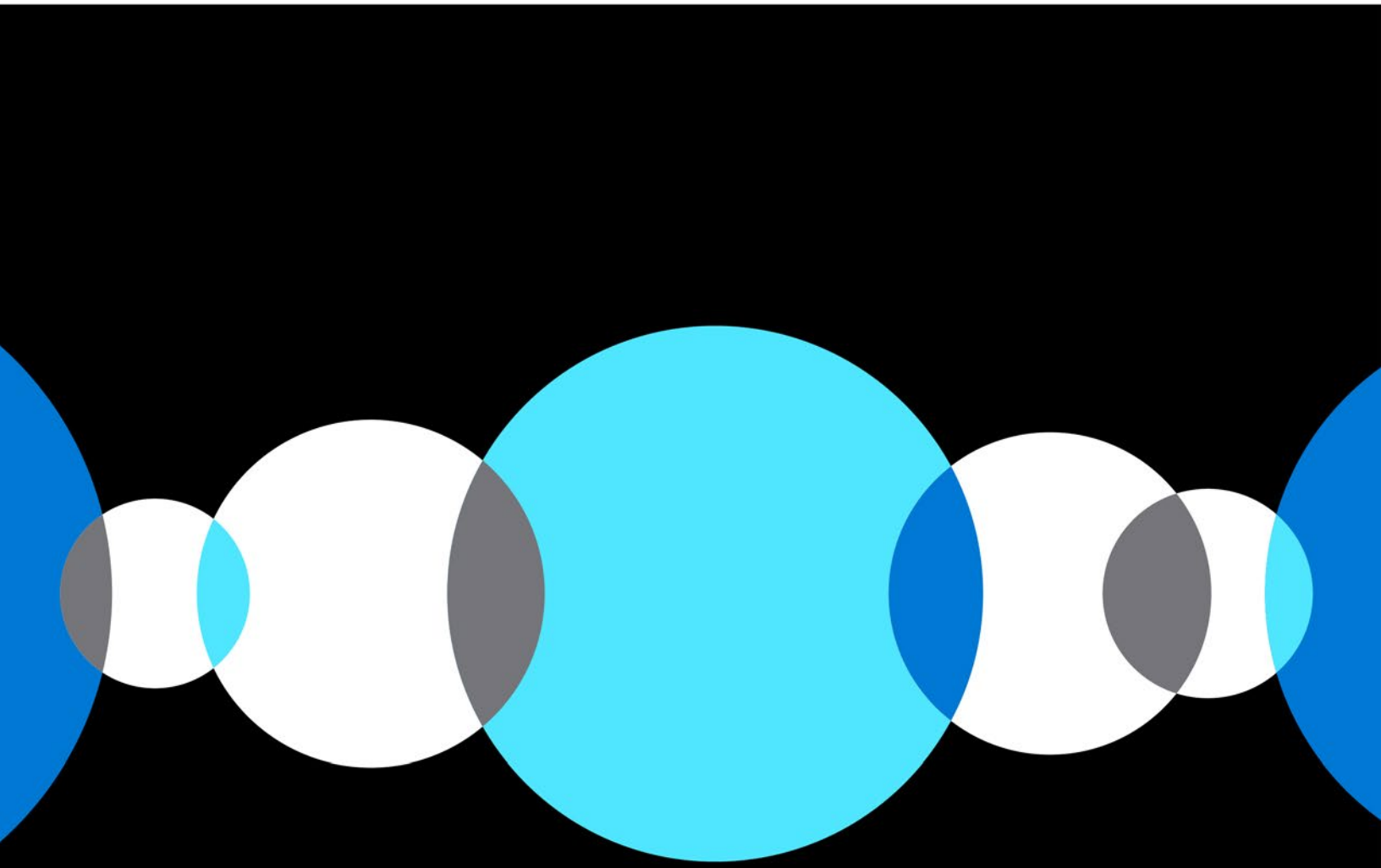
Azure e-kitap serisi

Microsoft Azure

Azure Sanal Masaüstü El Kitabı:
Felaketten Kurtarma



3 /
Giriş

3 Azure Sanal Masaüstü'ne genel bakış
6 Azure Sanal Masaüstü için felaketten kurtarmaya giriş

9 /
Azure Sanal Masaüstü'nde felaketten kurtarmayı ayarlama

9 Sanal ağ
10 Sanal makineler
14 Kullanıcı kimliklerini yönetme
15 Kullanıcı ve uygulama verilerini yapılandırma

24 /
Felaketten kurtarmayı test etme

25 /
Optimizasyonlar ve en iyi uygulamalar

28 /
Sonuç ve kaynaklar

Giriş

Azure Sanal Masaüstü ile kurumunuz için uzaktan çalışmayı sağlama yolculuğunuzda ilerledikçe, bölgeler arasında güvenilirliği güçlendirmek ve iyi bir kullanıcı deneyimi sağlamak için felaketten kurtarma yeteneklerini ve en iyi uygulamaları anlamak önemlidir.

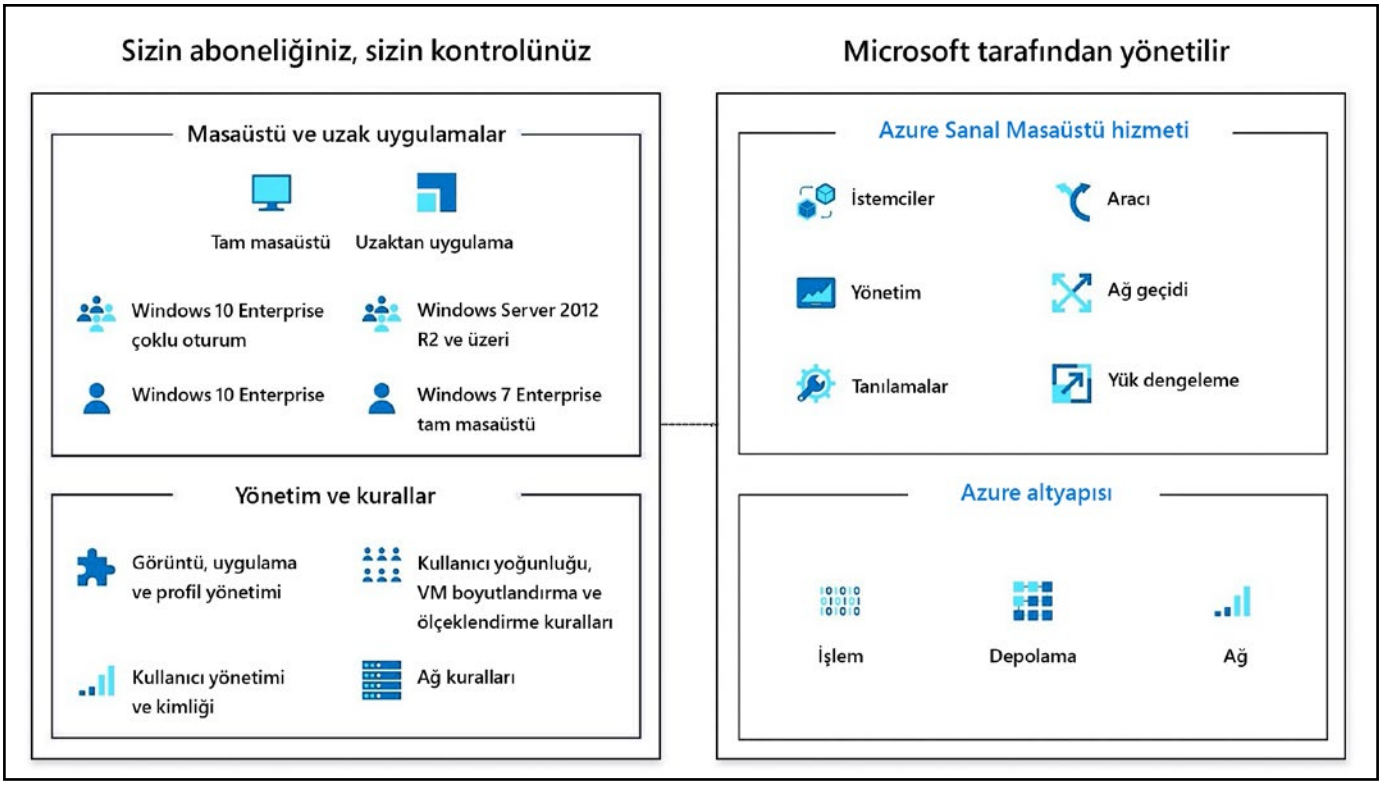
Bu el kitabı size **iş sürekliliği ve felaketten kurtarma (BCDR)** önkoşulları, kurulum adımları ve en iyi uygulamalar hakkında dikkat edilecekleri sağlar. Bu, çalışmama ve kesintiler sırasında kurumunuza daha fazla esneklik getirmenize yardımcı olarak başarılı bir BCDR planı hazırlamanıza olanak tanır. Teknik gereksinimler hakkında sorularınız varsa veya uzaktan çalışmaya imkan tanımak için kısa ve uzun vadeli çözümlerle ilgili tavsiyeye ihtiyacınız varsa bir Azure satış uzmanıyla konuşabilirsiniz.

Azure Sanal Masaüstü'ne genel bakış

Azure Sanal Masaüstü, Microsoft Azure üzerinde çalışan, kurumların iş esnekliğini güçlendirmelerine yardımcı olan güvenli bir uzaktan masaüstü deneyimi sağlamaya yardımcı olan kapsamlı bir masaüstü ve uygulama sanallaştırma hizmetidir. Basitleştirilmiş yönetim, Windows 10 Enterprise çoklu oturum, kurumlar için Microsoft 365 Apps optimizasyonu ve **Uzak Masaüstü Hizmetleri (RDS)** ortamlarına geçiş desteği sunar. Azure Sanal Masaüstü, Windows masaüstlerinizi ve uygulamalarınızı Azure'da dakikalar içinde kurmanıza ve ölçeklendirmenize olanak tanıyarak uygulamalarınızı ve verilerinizi güvende tutmanıza yardımcı olacak tümleşik güvenlik ve uyumluluk özellikleri sağlar.

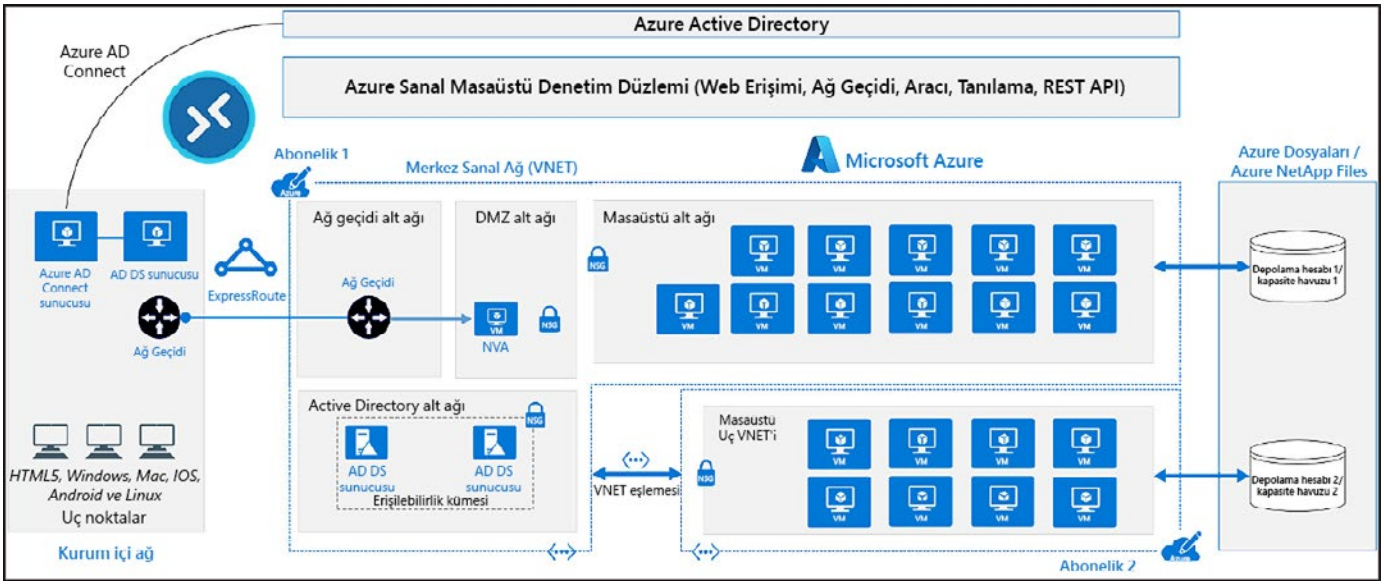
Esnek bir bulut VDI platformu olarak Microsoft, çözümün altyapıyla ilgili birçok bölümünü sizin adınıza yönetir. Esas olarak masaüstü ve uygulama iş yükleriyle ilgili diğer parçalar siz veya bir iş ortağınız tarafından yönetilir.

Şekil 1, bileşenlerin dört farklı alana gruplandığını gösterir. **Azure Sanal Masaüstü hizmeti** ve **Azure altyapısı** grupları Microsoft tarafından yönetilir. **Masaüstü ve uzak uygulamalar** ve **Yönetim ve kurallar** grupları, sizin tarafınızdan yönetilir ve bu da oturum ana bilgisayarı sunucularınızı ve uygulama manzaralarınızı kontrol altında tutma konusunda size tam esneklik sağlar.



Şekil 1: Azure Sanal Masaüstü bileşenleri ve sorumlulukları

Uygulamanın arka uç bileşenleri kurum içi ağınızdadır. ExpressRoute, kurum içi ağınızı Azure buluta genişletir. İsteğe bağlı olarak, arka uç bileşenleri veri merkezi geçiş senaryosuna dayanarak Azure'a da geçirilebilir. Azure AD Connect bileşenleri, **Active Directory Etki Alanı Hizmetleri (AD DS)** veya **Azure Active Directory Etki Alanı Hizmetleri (Azure AD DS)** kimlikleri ile senkronize olur. AD DS ve Azure AD, Azure abonelikleri, **sanal ağlar (VNet)**, Azure Dosyaları veya Azure NetApp Files ve Azure Sanal Masaüstü havuzları ve çalışma alanlarını barındırır. *Şekil 2*, tipik bir Azure Sanal Masaüstü mimari kurulumunu göstermektedir.



Şekil 2: Tipik Azure Sanal Masaüstü mimari kurulumu

Azure Sanal Masaüstü hizmet mimarisi, Windows Server RDS'ye benzerdir. Ancak, Azure Sanal Masaüstü ile Microsoft, kendi masaüstü ana **sanal makinelerinizi (VM)**, verilerinizi ve istemcilerinizi yönetirken altyapıyı ve aracılık bileşenlerini yönetir. Bu, odağınızı sizin için gerçekten önemli olan kullanıcı deneyimine kaydırmanıza olanak tanır. Kurum içindeki RDS, Azure'a geçiş ve Azure Sanal Masaüstü'ne geçiş arasındaki farkları anlamak için *Tablo 1*'e bakın.

Sorumluluk	Kurum içinde RDS	Azure'da RDS	Azure Sanal Masaüstü
Kimlik			
Son kullanıcı cihazları (mobil cihazlar ve bilgisayarlar)			
Uygulama güvenliği			
Oturum ana bilgisayarı işletim			
Kurulum yapılandırması			
Ağ denetimleri			
Sanallaştırma denetim düzlemi			
Fiziksel ana bilgisayarlar			
Fiziksel ağ			
Fiziksel veri merkezi			

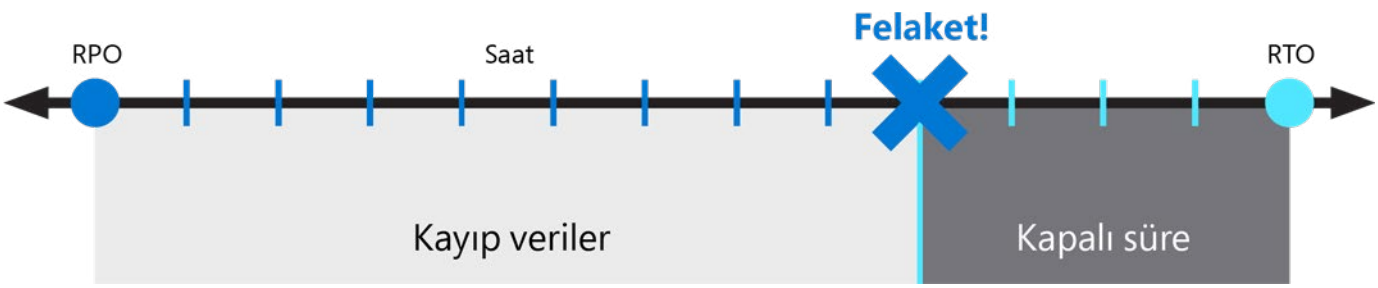
Müşteri Microsoft

Tablo 1: Kurum içinde RDS, Azure'da RDS ve Azure Sanal Masaüstü'ndeki sorumluluklar

Kurum için Azure Sanal Masaüstü hakkında daha fazla bilgi edinmek için bu sayfayı ziyaret edin.

Azure Sanal Masaüstü için felaketten kurtarmaya giriş

Kurumunuzun Azure Sanal Masaüstü erişilebilirliğini güçlendirmek ve verileri güvende tutmak için bir BCDR stratejisi uygulamanız gerekir. İyi bir BCDR stratejisi, planlı ve plansız hizmet veya Azure kesintileri sırasında uygulamalarınızı ve iş yüklerinizi çalışır durumda tutar. *Şekil 3*, **kurtarma noktası hedefini (RPO)** veri kaybı olarak ve **kurtarma süresi hedefini (RTO)** bir felaketten kurtulma süresi olarak tasvir etmektedir.



Şekil 3: RPO kaybı ve kurtarma için RTO süresi

Azure Sanal Masaüstü hizmeti, kesintiler sırasında müşteri meta verilerini korumak için BCDR'yi sunar. Bir Azure bölgesinde bir kesinti meydana geldiğinde, hizmet altyapısı bileşenleri ikincil bir konuma yük devri ve beklendiği gibi çalışmaya devam eder.

Kullanıcılarınızın bir Azure bölgesi kesintisi sırasında hala bağlanabildiğinden emin olmak için, kişisel VM'leri farklı bir Azure bölgesine (ikincil konum) çoğaltmanız gerekebilir. Kesintiler sırasında birincil bölge, ikincil konumdaki çoğaltılan VM'lere yük devri yapar. Kullanıcılar, uygulamalara kesintisiz olarak ikincil konumdan erişmeye devam edebilir. VM çoğaltmasına ek olarak, kullanıcı kimliklerinin ikincil konumda erişilebilir olduğundan emin olmanız gerekir. Bu, profil kapsayıcıları kullanarak gerçekleştirilebilir. VM çoğaltmasına alternatif olarak, bölgeler arasında otomatik tedarik etme ile birden fazla Havuzda toplanmış ana bilgisayar havuzu da kullanabilirsiniz.

Not: Birincil Azure bölgesindeki verilere dayanan iş uygulamalarının, geri kalan verilerle yük devredebildiğinden emin olun.

Bir kesinti sırasında kullanıcılarınızın bağlı olduğundan emin olmak için *Tablo 2*'de kronolojik sırayla gösterilen beş bileşeni göz önünde bulundurun.

	Bileşen	Açıklama
1	Sanal ağ	Bir kesinti sırasında ağ bağlantınızı göz önünde bulundurun.
2	Sanal makineler	VM'leri ikincil bir konumda çoğaltın veya Azure bölgelerinde birden çok kalıcı olmayan ana bilgisayar havuzu kurun.
3	Kullanıcı ve uygulama verileri	FSLogix profil kapsayıcılarını kullanarak ikincil konumda veri çoğaltma ayarlayın. Veri çoğaltması, MSIX uygulama eki kullananlar için de gereklidir.
4	Kullanıcı kimlikleri	Birincil konumda ayarladığınız kullanıcı kimliklerinin ikincil konumda bulunduğundan emin olun.
5	Uygulama bağımlılıkları	Birincil konumunuzdaki verilere dayanan tüm iş kolu uygulamalarının ikincil konuma devredildiğinden emin olun.

Tablo 2: Azure Sanal Masaüstü felaketten kurtarma için dikkate alınması gereken beş alan

Şimdi Azure VNet'lerle başlayarak Azure Sanal Masaüstü için felaketten kurtarmanın beş temel bileşenini ayarlamaya yönelik adımlara bakacağız.

Azure Sanal Masaüstü'nde felaketten kurtarmayı ayarlama

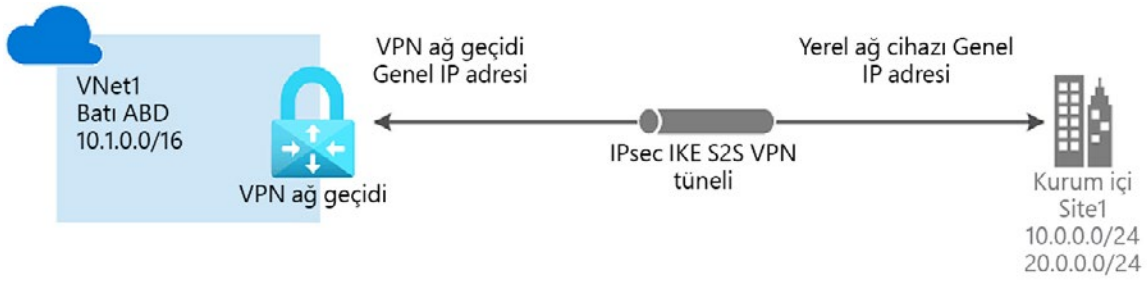
Her Azure Sanal Masaüstü ortamı, tasarım ve yapılandırma açısından farklıdır. Azure Sanal Masaüstü için bir felaketten kurtarma çözümü tasarlanırken ve uygulanırken aşağıdaki beş temel bileşen dikkate alınmalıdır.

Sanal ağ

Başlangıç noktası olarak, bir kesinti sırasında ağ bağlantınızı göz önünde bulundurmanız gerekir. Azure kaynaklarının yük devretmesi veya ikincil bir bölge ile iletişim kurması için ikincil bölgenizde/konumunuzda bir VNet kurulduğundan emin olmanız gerekir.

Kullanıcılarınızın kurum içindeki kaynaklara ve hizmetlere erişmesi gerektiğini varsayalım. Bu senaryoda, VNet'i bunlara bir VPN üzerinden erişecek şekilde yapılandırmanız gerekir. Kurum içi bağlantılar bir ExpressRoute, VPN veya sanal WAN ile kurulabilir. Ayrıca bir **ağ sanal cihazı (NVA)** kullanarak kurum içi ortamlara bağlanabilirsiniz.

Azure Site Recovery, birincil ağınızın ayarlarını koruduğu ve ağ eşlemesi gerektirmediği için VNet'i bir yük devretme bölgesinde kurmak için de kullanılabilir. Bu, kurulum gereksinimleri açısından basitliği nedeniyle daha küçük Azure Sanal Masaüstü kurulumu için tak ve çalıştır hizmeti olarak düşünülebilir. *Şekil 4*, kurum içi bir siteye bağlanan basit bir VPN ağ geçidini gösterir. Bu, kurum içinde Azure'dan bağlanmak için kullanılan yaygın bir bağlantı yöntemidir.



Şekil 4: Kurum içi bir siteye bağlanan basit bir VPN ağ geçidi

Şekil 5 iki Azure bölgesi arasındaki VNet eşlemesini gösterir. Eşleme, VPN kullanmadan iki VNet'i birbirine bağlamak isteyenler için yararlıdır.

Şekil 5: İki Azure bölgesi arasındaki VNet eşlemesi

DNS

Müşterilerin Azure Sanal Masaüstü ile karşılaştığı yaygın bir sorun, VNet ile ilgili DNS yapılandırma sorunlarıdır. VNet'inizin DNS ile doğru şekilde ayarlandığından emin olun. Azure Sanal Masaüstü FQDN'lerini ve AD DS'yi iki bölge arasında çözebilirsiniz.

Azure Sanal Masaüstü için gerekli URL listesinin devamını buradan okuyabilirsiniz.

Sanal makineler

Azure Sanal Masaüstü ana bilgisayar havuzları için hem *aktif-aktif* hem de *aktif-pasif*, uygulanabilir BCDR seçenekleri olabilir.

Aktif-aktif durumdayken, tek bir ana bilgisayar havuzunun birden çok Azure bölgesinden VM'leri olabilir. Bu senaryoda, FSLogix Bulut Önbelleği kullanımı, kullanıcı profilini / Office kapsayıcılarını bölgeler arasında etkin şekilde çoğaltmak için gereklidir. Her bölgedeki VM'ler için, konumları belirten Bulut Önbelleği kayıt defteri girdisinin yerel olana öncelik verecek şekilde ters çevrilmesi gerekir. Aktif-aktif aşağıdaki şekilde özetlenebilir:

- Bu karmaşık bir yapılandırmadır. Aktif-aktif seçilirse kullanıcının yeniden oturum açmasına gerek kalmadan depolama kesintilerine karşı kurum koruması sağlarken aynı zamanda felaketten kurtarma konumunun sürekli test edilmesini sağlar. Bu yapılandırma türü, ne performans ne de maliyet iyileştirme çözümü olarak kabul edilir; felaketten kurtarmayı sürekli olarak test eder.

- Gelen kullanıcı bağlantılarının yük dengelemesi yakınlığı göz önüne alamaz: Tüm ana bilgisayarlar eşit olur ve kullanıcılar Azure Sanal Masaüstü ana bilgisayar havuzu VM'sine uzak değil, en uygun noktaya yönlendirilebilir.
- Bu yapılandırma, *Havuza alınmış* (paylaşılan) ana havuz türü ile sınırlıdır. Bir *Kişisel* (adanmış) tür, bir masaüstü belirli bir oturum ana bilgisayarı VM'sinde bir kullanıcıya atandığında sabit kalır ve kullanılamaz olsa bile değişmez.

Aktif-pasif, Azure Site Recovery veya felaketten kurtarma bölgesinde ikincil bir ana bilgisayar havuzu (etkin bekleme) durumunda aşağıdaki seçenekler kullanılabilir:

- Azure Site Recovery, *Kişisel* (özel) ve *Havuza alınmış* (paylaşılan) ana bilgisayar havuzu türlerine sahiptir ve tek bir ana bilgisayar havuzu varlığını sürdürmenize olanak tanır.
- Yük devretme bölgesinde yeni bir ana bilgisayar havuzu oluşturmak da mümkündür, bu da tüm bu kaynakları kapalı tutmanızı sağlar. Bu yöntem için, yük devretme bölgesinde yeni uygulama grupları ayarlamanız ve bunlara kullanıcı atamanız gerekir. Daha sonra bir Azure Site Recovery "*kurtarma planı*" kullanarak ana bilgisayar havuzlarını açabilir ve düzenlenmiş bir işlem oluşturabilirsiniz.

Azure'dan Azure'a felaketten kurtarma mimarisinde açıklandığı gibi, diğer Azure bölgelerindeki çoğaltma VM'lerini yönetmek için Azure Site Recovery'yi kullanmanız önerilir. Azure Site Recovery, sunucu ve istemci tabanlı SKU'ları desteklediğinden kişisel ana bilgisayar havuzları için Azure Site Recovery kullanmanız önerilir.

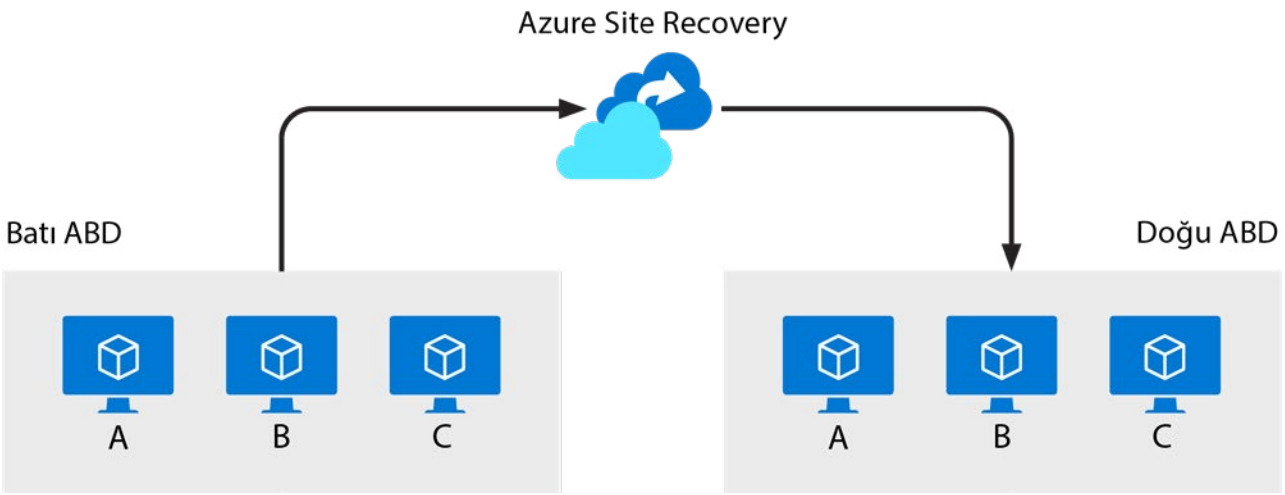
Azure Sanal Masaüstü felaketten kurtarma tasarımı konuları hakkında daha fazla bilgi için bu belgeye bakın.

Not: Bir erişilebilirlik kümesi içindeki maksimum VM sayısı, bu makalede belirtildiği gibi 200'dür.

Azure Sanal Masaüstü ana bilgisayar havuzu kurulumu için varsayılan esneklik seçeneği bir erişilebilirlik kümesidir: Ana bilgisayar havuzu esnekliğini yalnızca % 99,95'lik yüksek erişilebilirlikle tek bir Azure veri merkezi düzeyinde sağlar. Daha fazla bilgiye buradan erişebilirsiniz.

Kişisel masaüstü bilgisayarlarınızı korumak için Azure Backup kullanmanızı, özellikle bu masaüstü bilgisayarlar için profil kapsayıcıları kullanmamanızı öneririz. Azure Backup hizmeti hakkında daha fazla bilgiye buradan erişebilirsiniz.

Şekil 6, Azure Site Recovery'nin Doğu ve Batı ABD bölgelerindeki üç VM'deki iş yüklerini çoğaltmadaki rolünü göstermektedir.



Şekil 6: İş yüklerini birincil bölgeden ikincil bölgeye çoğaltan Azure Site Recovery

Azure Site Recovery kullanırken bu VM'leri manuel olarak kaydetmeniz gerekmez. İkincil VM'de yapılandırılan Azure Sanal Masaüstü aracısı, en yakın Azure Sanal Masaüstü hizmeti örneğine bağlanmak için otomatik olarak en son güvenlik belirtecini kullanır. İkincil bölgedeki VM (oturum ana bilgisayarı) otomatik olarak ana bilgisayar havuzunun bir parçası olur. Müşterinin yalnızca bu işlem sırasında yeniden bağlanması gerekir. Kullanıcının bunu bir kez yeniden bağlaması dışında, başka manuel işlem gerekmez.

Azure Sanal Masaüstü'ndeki kullanıcıların bağlantısını kesin

Bir kesinti sırasında mevcut herhangi bir kullanıcı bağlantısı olamaz. Yöneticinin ikincil bölgeye yük devretmeyi başlatmadan önce, geçerli Azure bölgesindeki kullanıcı bağlantılarını "sonlandırmanız" gerekir. Kullanıcıların Azure Sanal Masaüstü ile olan bağlantısını kesmek için bu cmdlet'i çalıştırabilirsiniz:

```
Remove-AzWvdUserSession
```

Tüm kullanıcılar birincil Azure bölgesinden çıkış yaptıktan sonra, devam edip birincil bölgedeki VM'ler üzerinde hata verebilirsiniz. Tamamlandıktan sonra, kullanıcıların ikincil bölgedeki VM'lere bağlanmasına izin verebilirsiniz. Bu işlemin nasıl çalıştığı hakkında daha fazla bilgi için bkz. Azure VM'lerini başka bir Azure bölgesine çoğaltma.

İkinci bir yük devretme sırasında kullanıcı oturumlarının bağlantısının kesilmesini otomatikleştirmek için bir runbook veya komut dosyası oluşturulması önerilir. Bu görevin manuel olarak tamamlanması zaman alabilir. Bu kılavuzu kullanarak bir Azure Automation runbook'u oluşturabilirsiniz.

Yedek koruma

Bu *Sanal makineler* bölümünün başında belirtildiği gibi kritik kullanıcı verilerinin kaybının önlenmesi önemlidir. İlk adım, kaydedilmesi ve korunması gereken verileri değerlendirmektir. Dikkat edilmesi gereken bazı noktalar şunlardır:

- OneDrive veya yerel olmayan başka bir depolama biçimi kullanılıyorsa kullanıcı profilini veya Office kapsayıcı verilerini kaydetmek gerekli olmayabilir.
- Kritik kullanıcı verilerini korumak için uygun bir mekanizma dikkate alınmalıdır:
  - Azure Backup hizmeti, Standart veya Premium katmanında Azure Dosyalarında depolandığında Profil ve Office kapsayıcı verilerini koruyabilir.
  - Azure NetApp Files Anlık görüntüler ve Kurallar, Azure NetApp Files (tüm katmanlar) için kullanılabilir.
  - Azure Backup, ana bilgisayar havuzu VM'lerini korumak için de kullanılabilir; ana bilgisayar havuzu VM'lerinin durum bilgisi bulunmasa bile bu uygulama desteklenir.

Altın görüntü erişilebilirliği

Azure Sanal Masaüstü ana bilgisayar havuzu VM'lerini kurmak için özel görüntüler kullanırken, büyük bir felaket durumunda bile bu yapıların tüm bölgelerde erişilebilir olmasını sağlamak önemlidir. Azure Paylaşılan Görüntü Galerisi hizmeti, bir ana bilgisayar havuzunun kurulduğu tüm bölgelerdeki görüntüleri yedek depolama alanı ile ve birden çok kopyayla çoğaltmak için kullanılabilir.

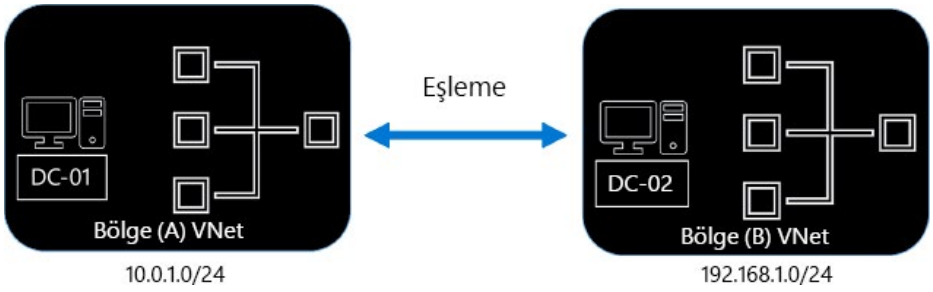
Artık VM'lerle bir felaketten kurtarma çözümünün nasıl tasarlanıp uygulanacağını bildiğinize göre, bir sonraki önemli bileşen kullanıcı kimliklerini yönetmek ve kullanıcı ve uygulama verilerini yapılandırmaktır.

Kullanıcı kimliklerini yönetme

Bu bölümde, kullanıcı kimliklerini yönetmeyi öğrenecek ve kullanabileceğiniz farklı seçenekleri keşfedeceksiniz.

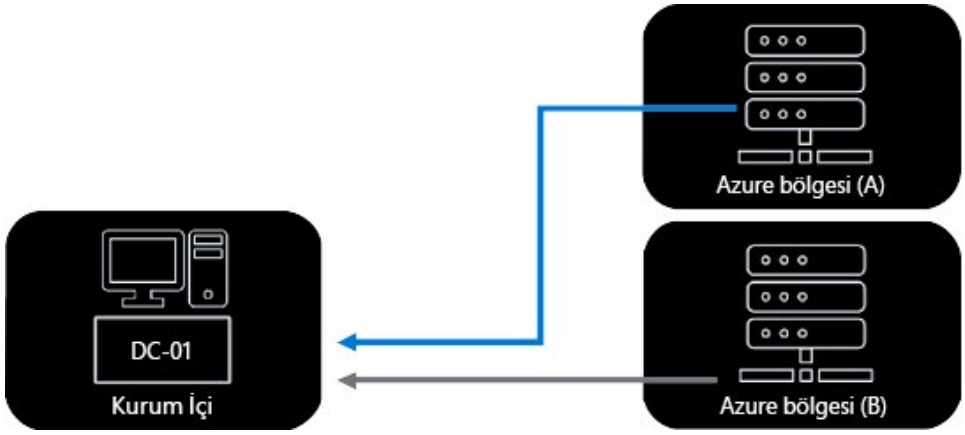
Bir yük devri durumunda, etki alanı denetleyicisinin ikincil konumda/bölgede kullanılabilir olduğundan emin olunmalıdır. Bir kesinti sırasında etki alanı denetleyicisini kullanılabilir tutmak için aşağıdaki üç seçenek kullanılabilir:

1. İkincil konuma bir AD etki alanı denetleyicisi kurun. *Şekil 7* ağ eşleme kullanılarak yapılandırılan iki VNet'i gösterir ve iki etki alanı denetleyicisinin eşleme kullanarak iki VNet arasında iletişim kurmasını sağlar.



Şekil 7: Ağ eşleme örneği

2. Kurum içinde AD etki alanı denetleyicisi kullanın. *Şekil 8* bir Azure VNet'i bir kurum içi siteye bir VPN ağ geçidi kullanarak bağlayan kurum içi bir ortamı gösterir.



Şekil 8: VPN ağ geçidi aracılığıyla kurum içindeki bir siteye bağlanan birden çok bölge

3. AD etki alanı denetleyicinizi Azure Site Recovery kullanarak çoğaltın. *Şekil 9* bir AD etki alanı denetleyicisinin Azure Site Recovery kullanılarak çoğaltıldığını gösterir.

Şekil 9: Azure Site Recovery kullanarak ikincil bölgeye çoğaltılan etki alanı denetleyicisi

Azure Sanal Masaüstü için bir BCDR çözümü tasarlarken kullanabileceğiniz kullanıcı kimliği seçeneklerini artık sunduğumuza göre, kullanıcı ve uygulama verilerinin nasıl yapılandırılacağını görelim.

Kullanıcı ve uygulama verilerini yapılandırma

Yerel profiller kullanıyorsanız kullanıcı verilerini ve oturum ana bilgisayarlarını ikinci bölgeye çoğaltmak için Azure Site Recovery'nin kullanılması önerilir. Profil kapsayıcıları kullanan çoğu kurum için sonraki adım, profil kapsayıcı çoğaltmayı ikincil konuma ayarlamak olacaktır.

Bir BCDR durumunda, verileri kullanıcı profili ile Office kapsayıcısı disklerini ayırarak yedeklemek, geri yüklemek ve çoğaltmak için harcanan zamanı azaltmak mümkündür. FSLogix, bunları ayrı depolama konumlarına tahsis etme olanağı ve kabiliyeti sunar. Normal kullanımda, Office diski profilden çok daha fazla kapasite (GB olarak ölçülür) tüketebilir. Profil diskinin yedeklenmesi, çoğaltılması ve geri yüklenmesi, önbellek verisi eklenmeden çok daha hızlı olacaktır. Office diskinin yeniden dayanıklı olması gerekmez; bu disk yeniden yüklenebilir; içerdiği veriler Office 365 online hizmetlerinde zaten mevcuttur.

Not: FSLogix Bulut Önbelleği özelliği, performans özelliklerini yüksek gecikme süreli hedeflere artırmak ve böylece zaman uyumsuz çoğaltma kullanmak için tasarım gereği "geri yazmak"tır.

FSLogix profillerini depolamak için üç standart seçenek vardır:

- Azure Dosyaları
- Azure NetApp Files
- Çoğaltma için FSLogix Bulut Önbelleği

Microsoft Azure, FSLogix Profili ve Office kapsayıcılarınızı depolamak için kullanabileceğiniz birden çok depolama çözümü sunar. Azure Sanal Masaüstü'ndeki FSLogix profil kapsayıcıları için depolama seçenekleri Azure'un Azure Sanal Masaüstü FSLogix kullanıcı profili kapsayıcıları için sunduğu çeşitli yönetilen depolama çözümlerini karşılaştırır.

Profiller için felaketten kurtarma ayarlarken aşağıdaki seçenekleri kullanabilirsiniz:

- Azure çoğaltmasını ayarlayın (örneğin, Azure Files Standard depolama hesabı çoğaltması, Azure NetApp Files çoğaltması veya dosya sunucuları için Azure Files Sync).
- Hem uygulama hem de kullanıcı verileri için FSLogix Bulut Önbelleği'ni ayarlayın. Dayanıklılık ve erişilebilirlik için Bulut Önbelleği'nin nasıl kullanılacağı hakkında daha fazla bilgi edinin.
- Üçüncü seçenek, yalnızca iş açısından kritik öneme sahip verilere her zaman erişim sağlamak amacıyla uygulama verileri için felaketten kurtarma sağlamaktır. Bu senaryoda, kesinti sona erdikten sonra kullanıcı verilerini alabilirsiniz. Bu, esas olarak kullanıcıların kesinti süresi boyunca yeni kullanıcı profilleri ve ilk kez oturum açma deneyimi alacakları anlamına gelir.

Not: NetApp çoğaltma, ilk kez ayarlandıktan sonra otomatik olarak yapılır. Azure Site Recovery planlarıyla, VM dışı kaynaklar üzerinde hata yapmak için öncesi veya sonrası komut dosyalarını ekleyebilirsiniz.

BCDR tasarımınıza nasıl fayda sağlayacağını görmek için şimdi Bulut Önbelleği'ne daha ayrıntılı olarak bakalım.

Bulut Önbelleği

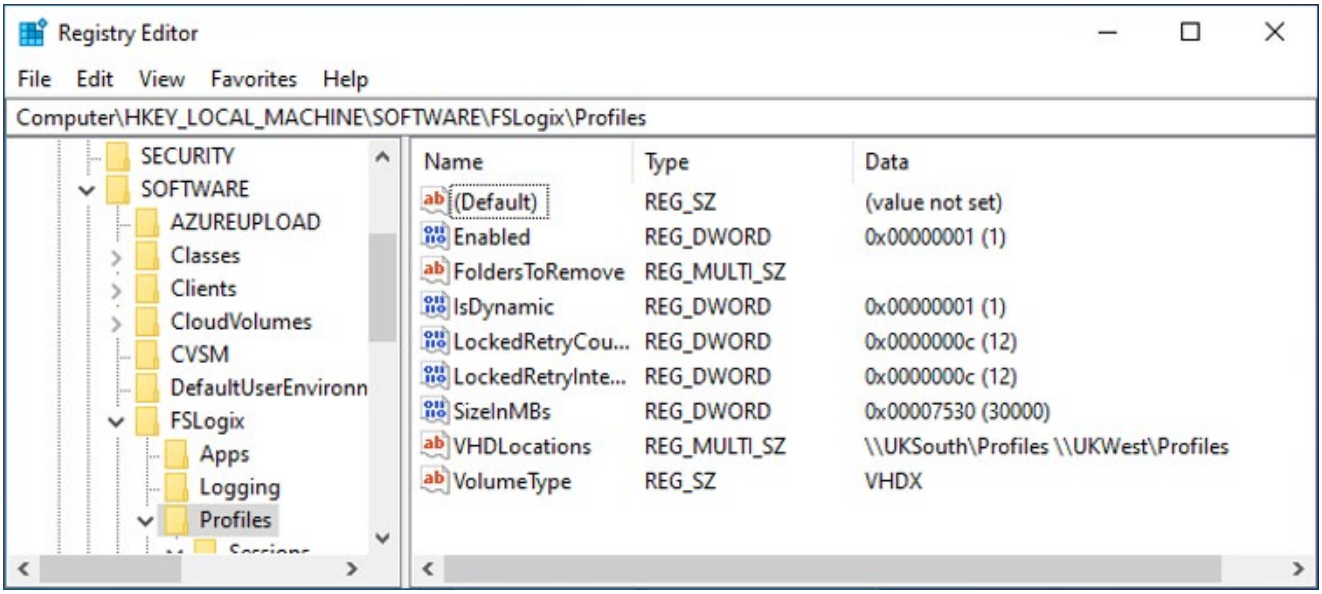
Bulut Önbelleği, ilk okuma tamamlandıktan sonra yönlendirilen bir Profilden veya Office kapsayıcısından okumalara hizmet sunmak için yerel bir profil kullanır. Bulut Önbelleği, kullanıcı oturumu sırasında sürekli olarak güncelleştirilen birden çok uzak konumu kullanabilir. Bulut Önbelleği, kullanıcıları uzak profil kapsayıcılarına kısa süreli bağlantı kaybı riskinden yalıtabilir. Ayrıca, Bulut Önbelleğinin Profil ve Office kapsayıcıları için aktif-aktif yedeklilik sağlayabileceğine dikkat etmek de önemlidir.

Not: Lütfen Bulut Önbelleği ile ilgili temel faktörler için *Tasarımda Göz Önünde Bulundurulması Gerekenler* bölümüne bakın. Oturum ana bilgisayarlarını, veri kaybı olmamasına yardımcı olmak amacıyla yerel önbellek dosyası için **Premium SSD** diskleriyle yapılandırmanız önerilir.

Birden çok profil konumu kullanarak FSLogix profil kapsayıcılarının yapılandırması

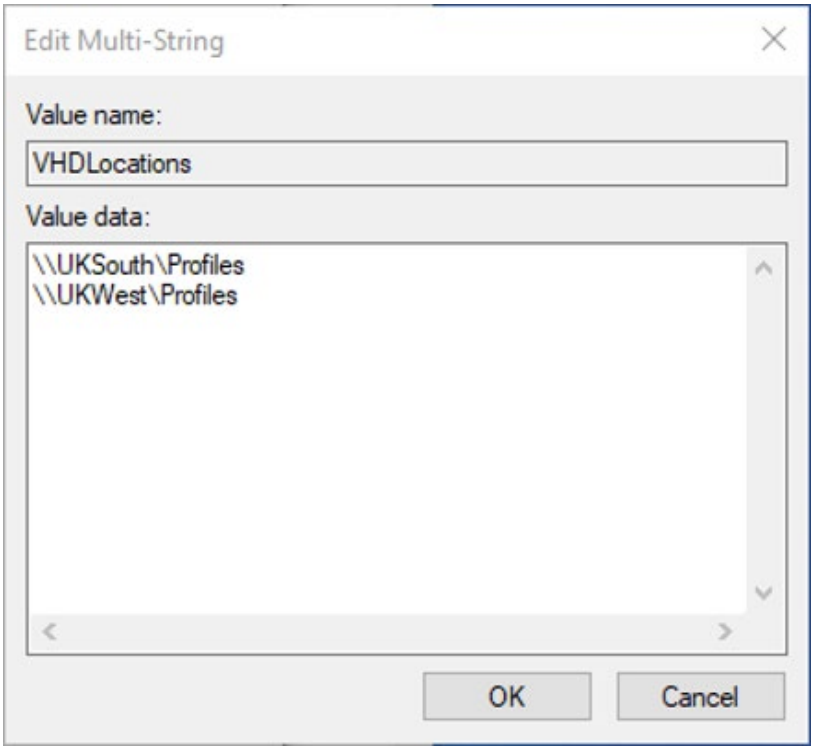
FSLogix aracısı, FSLogix için kayıt defteri girdilerini yapılandırdığınızda birden çok profil konumunu destekler. Kayıt defteri girdilerini yapılandırmak için:

1. **Kayıt Defteri Düzenleyicisi**'ni açın.
2. **Bilgisayar** > **HKEY_LOCAL_MAKİNE** > **YAZILIM** > **FSLogix** > **Profiller** yoluna gidin.



Şekil 10: FSLogix Profili kapsayıcıları için kayıt defteri ayarları

3. **VHDLocations**'a sağ tıklayın ve **Çok Dizeli Düzenleme**'yi seçin.



Şekil 11: FSLogix profil kapsayıcıları için kayıt defterinde VHDLocations seçeneği

4. **Değer verisi** alanında, kullanmak istediğiniz depolama konumlarını girin. İşlemi tamamladığınızda, **TAMAM**'ı seçin.

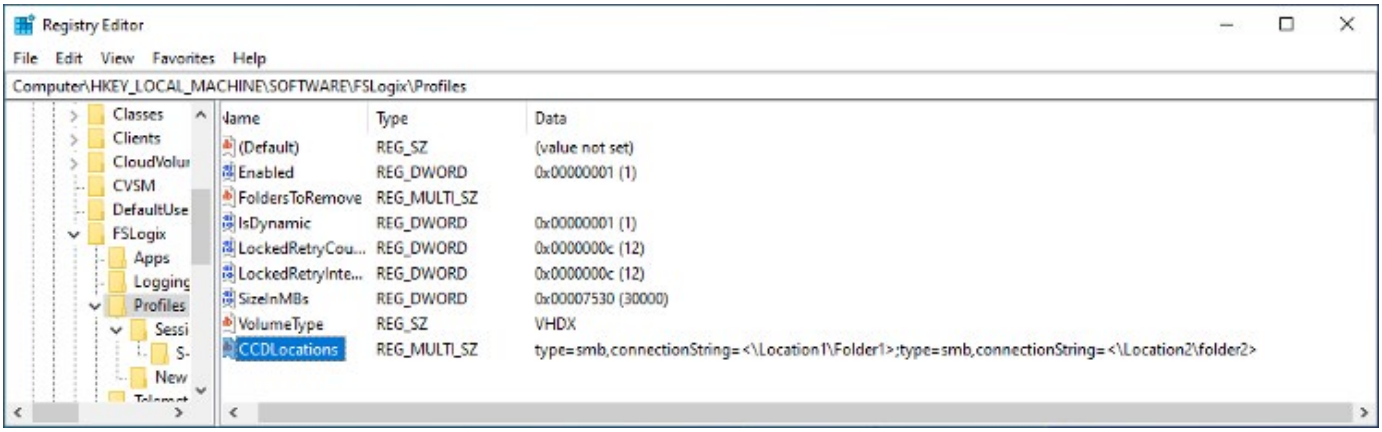
İlk depolama konumu kullanılamıyorsa FSLogix aracısı otomatik olarak ikinciye devredilir. Birincil bölge oturumu ana bilgisayarlarını (ilk kurulum) yapılandırırken FSLogix aracısını ikincil bir konum yolu ile önceden yapılandırmanızı öneririz.

İpucu: Bunları grup kuralına göre yapılandırmak için lütfen bu bağlantıya bakın.

Birincil bölgenin / konumun kapatıldığını varsayın. Bu durumda, FSLogix aracı yapılandırması VM'nin (Azure Site Recovery çoğaltması) bir parçası olarak çoğaltılır. Çoğaltılan VM'ler ikincil bölgede hazır olduğunda, aracı önceden yapılandırıldığı için otomatik olarak ikincil bölgenin yolunu dener.

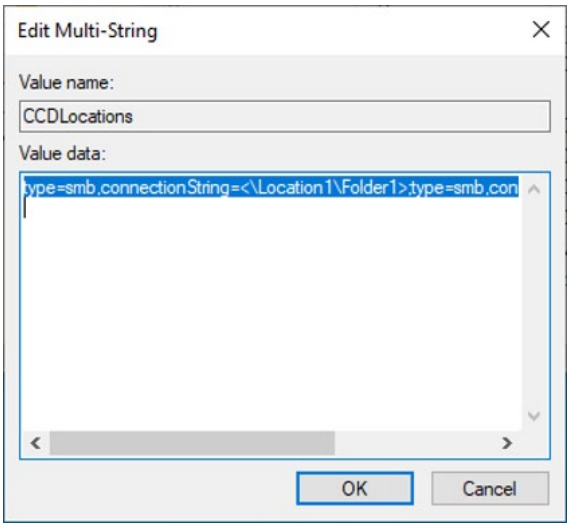
FSLogix profili Bulut Önbelleği yapılandırması

Aşağıdaki adımlarda, Bulut Önbelleği kurulumunun gereksinimleri özetlenmektedir.



Şekil 12: FSLogix profili kapsayıcıları için kayıt defteri

1. **Kayıt Defteri Düzenleyicisi**'ni açın.
2. **Bilgisayar** > **HKEY_LOCAL_MAKİNE** > **YAZILIM** > **FSLogix** > **Profiller** yoluna gidin.
3. **VHDLocations** ayarlarını kaldırın.
4. **CCDLocations** öğesini **REG_MULTI_SZ** olarak ekleyin ve konum 1 ile konum 2'yi dahil edecek şekilde belirtilen değeri ekleyin: **type=smb,connectionString=<\Location1\Folder1>;type=smb,connectionString=<\Location2\folder2>**



Şekil 13: FSLogix Bulut Önbelleği için CCDLocations

Kurulum tamamlandıktan sonra, Bulut Önbelleği iki konum arasındaki profili çoğaltır.

Azure Dosyaları

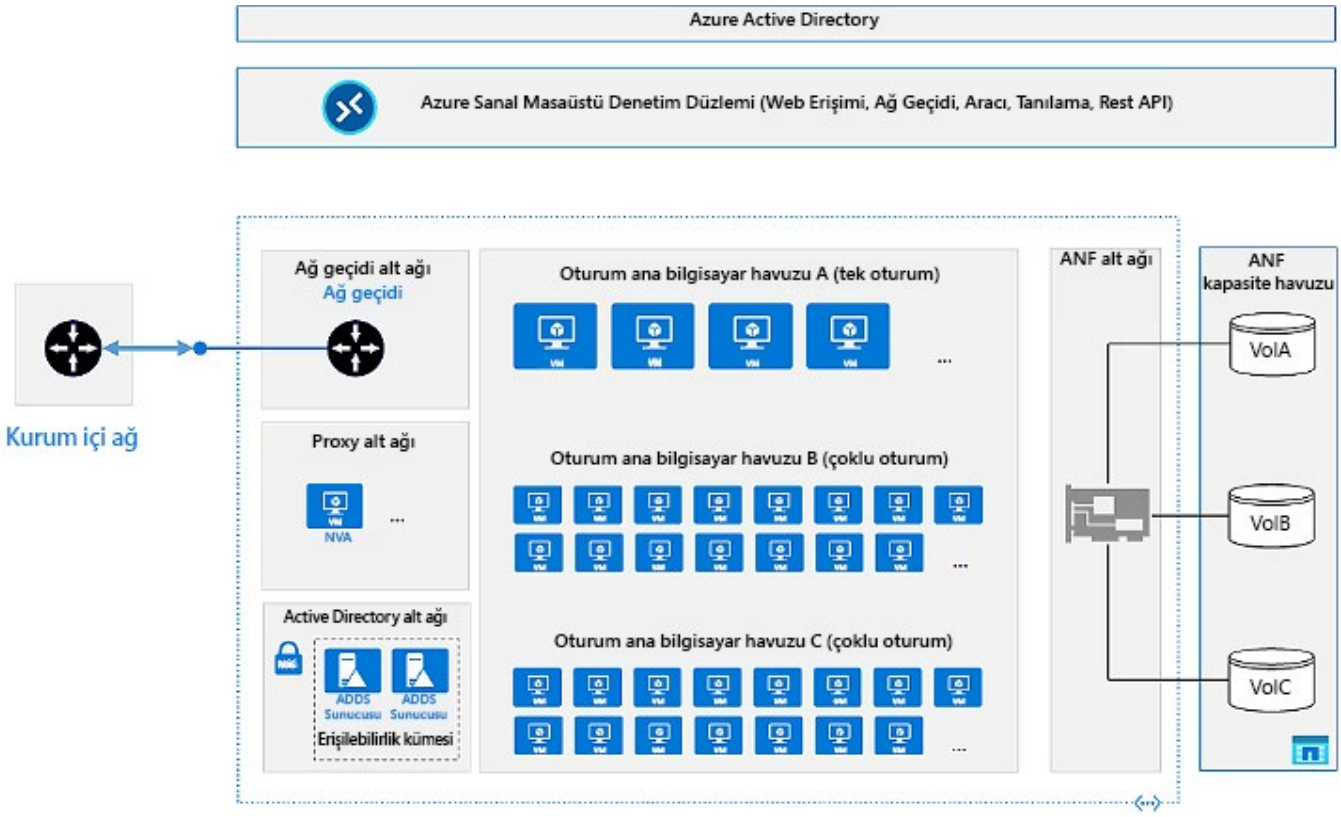
Azure Dosyaları, bir depolama hesabı oluştururken belirtebileceğiniz bölgeler arası zaman uyumsuz çoğaltmayı destekler. Azure Dosyaları'nın zaman uyumsuz yapısı zaten felaketten kurtarma hedeflerinizi karşılıyorsa ek yapılandırmalar gerçekleştirmeniz gerekmez.

Azure Dosyaları, depolama hesabı yedeklilik planınızda yapılandırılmış olan diğer bölgeye karşı bir depolama hesabı yük devretme çoğaltma seçeneği sunar. Bu, yalnızca **coğrafi yedekli depolama (GRS)** kullanan standart depolama hesabı türü için desteklenir. Diğer seçenekler arasında *AzCopy* veya herhangi bir dosya kopyalama mekanizması (ör. *Robocopy* kullanımı da yer alır.

Not: Azure Dosyaları paylaşım premium katmanı veya Azure Dosyaları paylaşım standart katmanı, büyük dosya desteği etkinken GRS kullanılamaz. Azure NetApp Files birimlerinin bölgeler arası çoğaltılması hakkında daha fazla bilgi için burayı okuyun.

Azure NetApp Files

Azure NetApp Files, herhangi bir kod değişikliğine gerek kalmadan Azure'daki en zorlu dosya iş yüklerinizi çalıştırabilen yüksek performanslı bir dosya depolama hizmetidir. NetApp'ın ONTAP teknolojisi üzerine kurulmuş ve Microsoft tarafından desteklenen birincil bir Azure hizmetidir. Kurulumu yalnızca dakikalar süren Azure NetApp Files, hem Linux hem de Windows uygulamalarının kurum içi benzeri bir deneyim ve karşılık gelen performans için sorunsuz bir şekilde bulutta geçiş yapmasını ve bulutta çalışmasını sağlar. *Şekil 14*, NetApp Files kullanan bir Azure Sanal Masaüstü ortamını gösterir.



Şekil 14: Azure NetApp Files kullanan Azure Sanal Masaüstünün mimari şeması

Azure NetApp Files hakkında daha fazla bilgi için: Azure NetApp Files için çoğaltma eşlemesi oluşturma. Daha fazla bilgi için Kurumlar için FSLogix - Azure Mimari Kılavuzu 'na bakın.

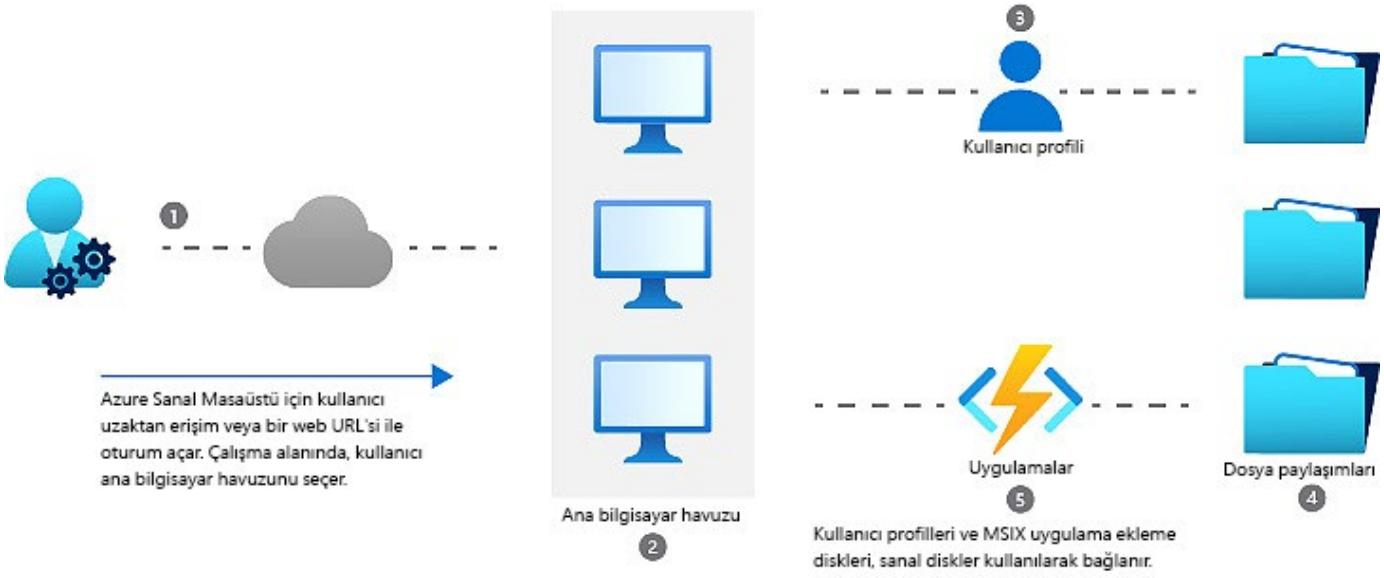
OneDrive kullanımı

OneDrive, varsa bilinen klasörleri (Masaüstü, Belgeler, Resimler, Ekran Görüntüleri ve Film Rulosu) yeniden yönlendirebilir. Bu, BCDR senaryosunda özel bir değerlendirmeye ihtiyaç duymak yerine OneDrive tarafından işleneceği için bu özel klasörlerin dayanıklılığını artırır.

MSIX uygulama eki

MSIX uygulama eki, Azure Sanal Masaüstü'ndeki Microsoft uygulama teslim özelliğidir ve modern bir çalışma alanı için tasarlanmıştır. MSIX uygulama eki ile, Azure Sanal Masaüstü içindeki Havuza alınmış ve Kişisel masaüstlerine uygulamalar teslim etmek için bir uygulama biçimi (MSIX) kullanabilirsiniz.

Şekil 15 MSIX uygulama ekinin nasıl çalıştığını tasvir eder. MSIX görüntülerini depolamak için dosya paylaşımlarının gerekli olduğunu göreceksiniz.



Şekil 15: MSIX uygulama eki uygulamalarını bir kullanıcıya sunma adımları

Dikkate alınması gereken iki alan vardır. İlk olarak, MSIX görüntülerinin ikinci konumda erişilebilir olduğundan emin olmak için depolamaya dikkat etmeniz gerekir. Profil kapsayıcılarına benzer şekilde, MSIX uygulama eki işlemi için de MSIX görüntülerini depolamak üzere ağ depolaması gerekir. Bu, Azure Dosyaları, NetApp Files veya bir dosya paylaşımı olabilir. Seçilen seçeneğe bağlı olarak, bu MSIX görüntülerinin bir BCDR senaryosunda kullanılabilir olduğundan emin olmanız gerekir.

İkinci konu ise, ikinci bölgede yeni bir depolama kaynağı kullanmayı seçtiyseniz MSIX görüntü yolunun değişmiş olabileceğidir. Bunu yaptığınızda depolama yolları değişmiştir. Bu, kullanıcıların bu uygulamalara bir ana bilgisayar havuzu aracılığıyla erişebilmesi için önce tüm MSIX görüntü yollarınızı PowerShell veya Azure yönetim kullanıcı arabirimi aracılığıyla yeniden yapılandırmanız gerektiği anlamına gelir.

MSIX uygulama ekini ve MSIX görüntü yollarını yeniden yapılandırma karmaşıklığını önlemek için aşağıdaki seçeneklerden birini kullanın.

- İkincil bölge için ayrı bir ana bilgisayar havuzu oluşturun.
- GRS ile Azure Dosyaları kullanın.
- Azure NetApp Files bölgeler arası çoğaltmayı uygulayın.

Azure portalı üzerinden MSIX uygulama ekini nasıl ayarlayabileceğinizi bu belgeden öğrenebilirsiniz.

Uygulama bağımlılıkları

Dikkate alınması gereken son bir alan, birincil uygulamada çalışan ve bir kesinti sırasında iş uygulaması hatalarını önlemek için devralınması gereken veri veya hizmetlerdir. Birincil bölgede bulunan verilere dayanan tüm iş uygulamalarının ikincil konuma yük devretme sağlayabildiğinden emin olun. Bu, özel web hizmetleri, SQL veritabanları veya diğerleri olabilir.

Ayrıca gerekli ayarların uygulamalar için yapılandırıldığından da emin olunmalıdır. Çoğaltma veya yüksek erişilebilirlik yapılandırıldıktan sonra bu hizmetlere ek yapılandırmalar eklemeniz gerekebilir. Bir örnek, uygulamalardan biri SQL arka ucuna bağlıysa ikincil konumda SQL'i çoğalttığınızdan ve SQL yüksek erişilebilirlikli bağlantı dizelerini yapılandırdığınızdan emin olun.

Uygulamayı, ikinci bölgeyi yük devretme işleminin parçası olarak veya varsayılan yapılandırması olarak kullanacak şekilde yapılandırabilirsiniz. Uygulama bağımlılıklarını Azure Site Recovery planlarında da modelleyebilirsiniz.

Özet:

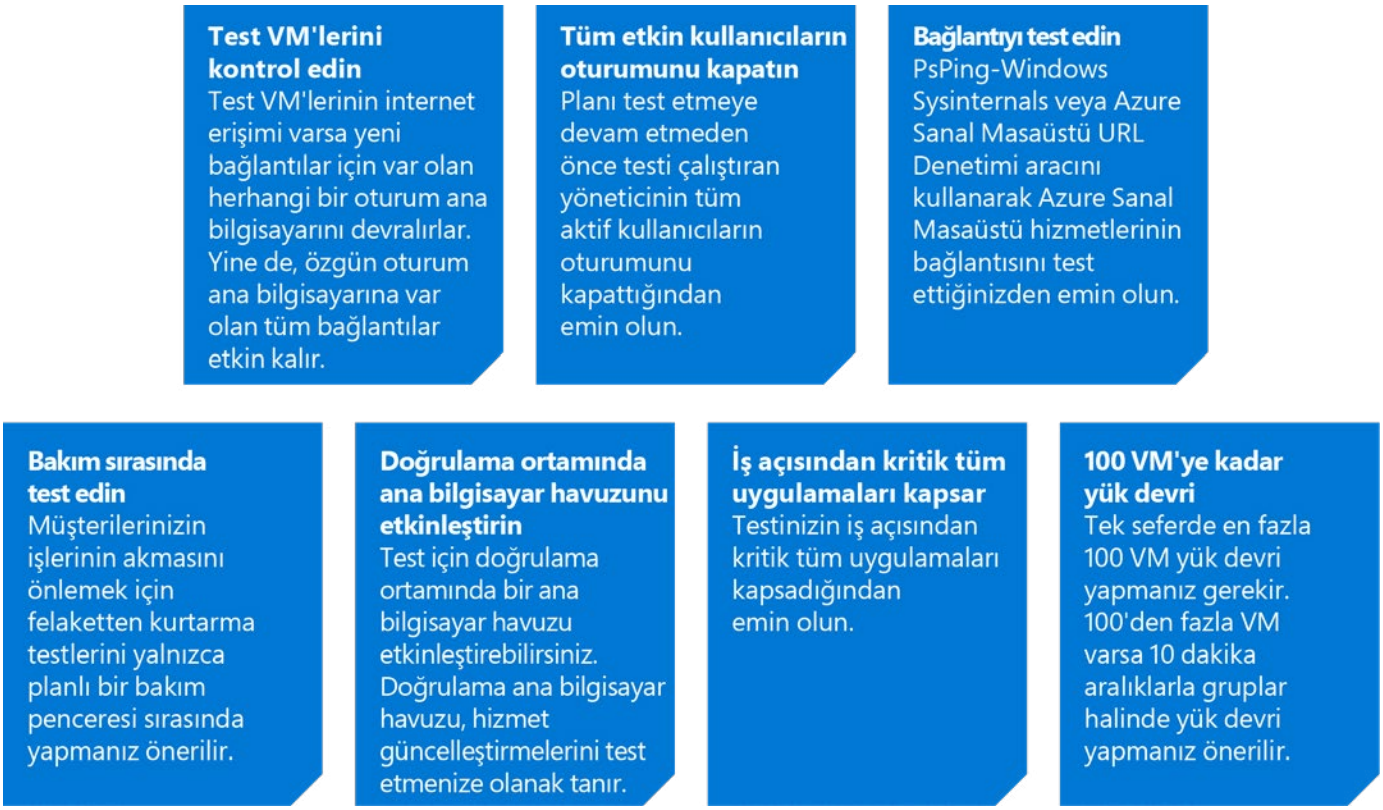
- Azure Sanal Masaüstü altyapısı kullanıcıları kurum içi kaynak erişimine ihtiyaç duyuyorsa bağlanmak için gereken ağ altyapısının yüksek erişilebilirliği de önemlidir ve dikkate alınması gerekir.
- Kimlik doğrulama altyapısının esnekliğinin incelenmesi ve değerlendirilmesi gerekir.
- İkincil felaketten kurtarma konumunda erişilebilirliği sağlamak için bağımlı uygulamalar ve diğer kaynaklar için BCDR yönlerinin dikkate alınması gerekir.

Daha fazla bilgi edinmek için kurtarma planları belgelerine bakın.

Felaketten kurtarmayı test etme

Azure Sanal Masaüstü için felaket kurtarmayı ayarlayıp yapılandırdıktan sonra, çalıştığından emin olmak ve kullanıcıların yine de gerekli kaynaklara ve hizmetlere erişebildiğini onaylamak için planınızı test etmelisiniz.

Azure Sanal Masaüstü BCDR planınızı test ederken aşağıdaki noktalar dikkate alınmalıdır.



Şekil 16: Azure Sanal Masaüstü BCDR planını test ederken dikkat edilmesi gereken noktalar

Gerekli URL Kontrol aracı için aşağıdaki kılavuza bakın.

İpucu: Ayrıca Azure Sanal Masaüstü hizmetlerine olan bağlantıyı PsPing - Windows Sysinternals kullanarak test edebilirsiniz.

Son bölümde, Azure Sanal Masaüstü için optimizasyon ve en iyi uygulamalar için bazı temel araçlara göz atacağız.

Optimizasyonlar ve en iyi uygulamalar

Felaketten kurtarma tasarım yapılandırmanız için dikkate almanız gereken en iyi uygulamalar şunlardır:

Active Directory
AD kimlik doğrulaması, felaketten kurtarma bölgesinde mevcut olmalıdır veya kurum içi etki alanı ile bağlantı garanti edilmelidir.

Sanal makineler
Azure Sanal Masaüstü ana bilgisayar havuzu bilişim kurulum modeli BCDR için, RPO ve RTO'ya yönelik gerekliliklerinizi karşılıyorsa *aktif-pasif* seçeneğini kullanın.

Azure Site Recovery
Azure Site Recovery, Havuza alınmış (*paylaşılan*) ana bilgisayar havuzları için desteklenir. Bu seçenek değerlendirilebilir ve ikincil felaketten kurtarma bölgesinde başka bir ana bilgisayar havuzunun kurulumuyla karşılaştırılabilir.

Not: Azure Site Recovery, Kişisel (*özel*) ana bilgisayar havuzları için önerilir. Hedef bölge, FSLogix tarafından kullanılan depolama arka ucunun felaketten kurtarmasıyla uyumlu hale getirilmelidir.

Erişilebilirlik bölgeleri
Erişilebilirlik bölgeleri, tek bir bölgede ana bilgisayar havuzunun maksimum esnekliği gerektiğinde kullanılmalıdır. Müşteriler, öncelikle gerekli bölgedeki erişilebilirlik bölgesinin özellik erişilebilirliğini ve tüm bölgelerde belirli VM boyutlandırma türünün **stok saklama birimleri (SKU'lar)** erişilebilirliğini doğrulamalıdır.

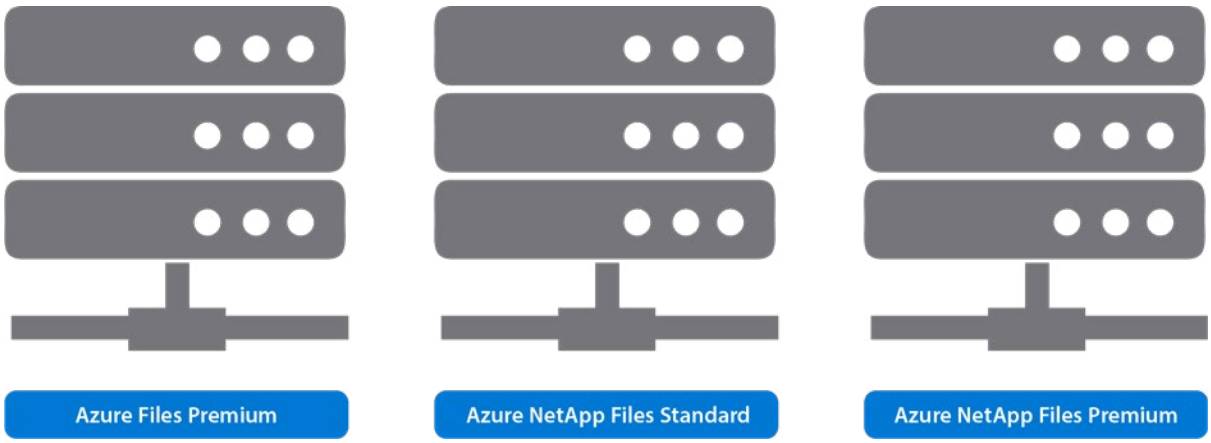
Azure Paylaşılan Görüntü Galerisi
Altın görüntüleri farklı bölgelere çoğaltmak için Azure Paylaşılan Görüntü Galerisi kullanılmalıdır. Görüntü oluşturmak için kullanılan depolama alanı **bölgesel çoğaltılan depolama (ZRS)** olmalı ve bölge başına en az iki kopya saklanmalıdır.

FSLogix

Çoğu müşteri senaryosu için Azure Dosyaları veya Azure NetApp Files'da FSLogix kullanıcı Profili ve Office kapsayıcılarının depolanmasını öneririz.

Not: Kullanıcı Profili ve Office kapsayıcılarını ayırmanız önerilir.

FSLogix kapsayıcı depolama türleri için önerilen seçenekler *Şekil 17'de* ayrıntılı olarak verilmiştir.



Şekil 17: FSLogix kapsayıcı depolama türü için önerilen seçenekler

Azure Dosyaları türünün kullanımı, belirli iş yükünün gerektirdiği kaynaklara ve gecikme süresine bağlıdır. Büyük kurumlar genellikle Azure Files Premium veya Azure NetApp Files Premium kullanır.

En iyi performans için FSLogix kapsayıcıları, depolama alanında kullanıcının oturum açtığı VM'ye mümkün olduğunca yakın, tercihen aynı veri merkezinde olmalıdır.

Mümkün olduğunda BCDR için Azure depolama yerleşik çoğaltma mekanizmaları kullanılmalıdır; daha az kritik ortamlar için ZRS veya Azure Dosyaları için GRS önerilir. Hiçbir alan/bölge koruması gerekli değilse, yalnızca yerel esnekliğe sahip yerel olarak yedekli depolama (LRS) kullanılabilir.

Not: Büyük kurumlar için Microsoft FSLogix Profil Kapsayıcısı çözümünün tasarlanması, boyutlandırılması ve uygulanması konusunda görüşler edinmek için bu makaleye bakın.

Bulut Önbelleği

Bulut Önbelleği yalnızca şu durumlarda kullanılmalıdır:

- Kullanıcı Profili veya Office kapsayıcıları veri kullanılabilirliği gereklidir; yüksek erişilebilirlikli SLA kritik öneme sahiptir ve bölge hatasına karşı dayanıklı olmalıdır.
- Seçilen depolama seçeneği BCDR gereksinimlerini karşılayamıyor. Örneğin, Azure Dosyaları paylaşım premium katmanı veya Azure Dosyaları paylaşım standart katmanı, büyük dosya desteği etkinken GRS kullanılamaz.
- Farklı depolama arasında çoğaltma gerektiğinde.

Bulut Önbelleği kullanıldığında, Azure Sanal Masaüstü ana bilgisayar havuz VM'lerinin yönetilen diski için bir SSD kullanılması ve kullanıcı profilini ve Office kapsayıcılarını korumak için bir yedekleme çözümünün bulunması önerilir.

Azure Backup

Azure Dosyaları, standart veya premium katmanları paylaşırken kritik kullanıcı verilerini veri kaybından veya mantıksal bozulmadan korumak için Azure Backup'ı kullanabilirsiniz. Azure Backup'ı kullanırken aşağıdaki noktaları göz önünde bulundurun:

- Azure NetApp Files hizmeti kullanıldığında anlık görüntüleri ve kuralları kullanın.
- Desteklense bile vatansız olması gerektiğinden ana bilgisayar havuzunda bir VM durumunu kaydetmek için Azure Backup kullanılması önerilmez.
- Bağımlı kaynaklar (ağ, kimlik doğrulama, uygulamalar ve Azure veya kurum içindeki diğer dahili hizmetler) için dayanıklılık ve BCDR planlarınızı dikkatle gözden geçirin.
- Hub ve bağlı bileşen veya sanal WAN mimarisinin bir parçası olarak ağ altyapısının da ikincil bölgede bulunması gerekir.
- Hibrit bağlantı, hem birincil hem de ikincil bölgelerde yüksek düzeyde erişilebilir olmalıdır.

Bu bölümde paylaşılan felaketten kurtarma ile ilgili tüm en iyi uygulamalar ve ipuçları, güçlü ve esnek bir BCDR'ye sahip olmanızı sağlamaya yardımcı olacaktır.

Felaketten kurtarma planınızda size yardımcı olacak birkaç kaynak aşağıda verilmiştir

- İş sürekliliği ve felaketten kurtarma planı geliştirin
- BCDR planınızın bir parçası olarak Azure Site Recovery'yi kullanın
- Dayanıklı uygulama hizmetleri oluşturun
- İş sürekliliği ve felaketten kurtarma planı oluşturun

Sonuç ve kaynaklar

Özet

Bu el kitabına Azure Sanal Masaüstü'ne kısa bir genel bakış ve ortamınız için bir felaketten kurtarma stratejisi planlamanın önemiyle başladık. İyi bir BCDR stratejisine sahip olmak oldukça önemlidir. VNet'ler, VM'ler, kullanıcı kimlikleri, kullanıcı ve uygulama verileri dahil olmak üzere Azure Sanal Masaüstü felaket kurtarmanın temel alanlarını da dikkate almak önemlidir.

El kitabının ilerleyen kısımlarında, Azure Sanal Masaüstü felaketten kurtarma uygulamasının nasıl test edileceğine hızlıca baktık. Bununla birlikte, Azure Sanal Masaüstü için bir BCDR çözümü uygularken tasarımla ilgili hususlar hakkında tartışılan en iyi uygulamaları ve kılavuzları takip etmek çok önemlidir.

Bu el kitabının, Azure Sanal Masaüstü için felaket kurtarmayı planlama, tasarım ve kurma konularında daha hazırlıklı hissetmenize yardımcı olacağını umuyoruz.

Başlamanıza yardımcı olacak destek ve ilave okumalar için *Kaynaklar* bölümüne bakın.

Kaynaklar

Azure Sanal Masaüstü ve BCDR ile yolculuğunuza devam ederken size yardımcı olabilecek birkaç kaynak aşağıda verilmiştir:

- Azure Sanal Masaüstü için BCDR hakkında daha fazla bilgi edinin.
- Azure Sanal Masaüstü rehberliği için Azure güvenlik temellerini takip edin
- Ücretsiz Azure hesabıyla hemen başlayın
- Kişiselleştirilmiş rehberlik almak ve fiyatlandırma, teknik gereklilikler ve güvenli uzaktan çalışma çözümlerini görüşmek için bir Azure satış uzmanıyla iletişime geçin
- Kurum için VDI'nızın geçişiyle ilgili rehberlik ve uzman yardımı almak için Azure Geçiş ve Modernizasyon Programı'na katılın.

Terimler sözlüğü

Aşağıdaki tablo, bu el kitabında kullanılan terminoloji sözlüğünü içermektedir.

Ad	Açıklama
Active Directory Etki Alanı	Dizin, ağdaki nesneler hakkında bilgi depolayan hiyerarşik bir yapıdır. Active Directory Etki Alanı Hizmetleri (AD DS) gibi bir dizin hizmeti, dizin verilerini depolama ve bu verileri ağ kullanıcıları ve yöneticileri için kullanılabilir hale getirme yöntemleri sağlar.
Azure Active Directory (Azure AD)	Azure AD, Microsoft'un bulut tabanlı kimlik ve erişim yönetimi hizmetidir ve çalışanlarınızın oturum açmasına ve kaynaklara erişmesine yardımcı olur.
Azure Dosyaları	Azure Dosyaları, bulutta Sunucu İleti Bloğu (SMB) protokolü veya Ağ Dosya Sistemi (NFS) protokolü üzerinden erişilebilen, tam olarak yönetilen dosya paylaşımları sunar.
Azure NetApp Files	Azure NetApp Files hizmeti, kurumsal sınıf, yüksek performanslı, ölçülü bir dosya depolama hizmetidir. Azure NetApp Files herhangi bir iş yükü türünü destekler ve varsayılan olarak yüksek erişilebilirliğe sahiptir.
Azure Site Recovery	Azure Site Recovery hizmeti, bölgeler arasında Azure Sanal Masaüstü'nün çoğaltmasını yönetir.
FSLogix	FSLogix, Azure Sanal Masaüstü gibi uzak bilişim ortamlarında profilleri dolaşmak için tasarlanmıştır. Tam bir kullanıcı profilini tek bir kapsayıcıda depolar.
Windows 10 çoklu oturum	Eskiden Sanal Masaüstü Bilgisayarlar için Windows 10 Enterprise (EVD) olarak bilinen Windows 10 Enterprise çoklu oturum, birden çok eş zamanlı etkileşimli oturum sağlayan yeni bir Uzak Masaüstü oturum ana bilgisayarıdır.

Yazar hakkında

Son kullanıcı bilişimi (EUC) uzman, konuşmacı ve sunucu Ryan Mangan, müşterilere ve teknik topluluklara çeşitli alanlarda küçük ila genel 30.000'den fazla kullanıcılı kurumsal kurulumlar arasında değişen son kullanıcı bilişim çözümleri konusunda yardımcı olur. Ryan, 3 milyonu aşkın ziyaretçisi bulunan ve Uzak Masaüstü Hizmetleri ile Azure Sanal Masaüstü hakkında 70'in üzerinde makale içeren ryanmangansitblog.com'un sahibi ve yazarıdır. Ryan'ın yayımlarından bazıları ile topluluk ve teknik ödüllerinden bazıları aşağıda verilmiştir:

- Yazarı:
  - *Azure Sanal Masaüstü Hızlı Başlangıç Kılavuzu*
  - *MSIX Uygulama Ekine Giriş*
- VMware vExpert, art arda sekiz yıl
- VMware vExpert EUC 2021
- Parallels RAS VIPP – art arda beş yıl
- LoginVSI Teknoloji Avukatı - art arda iki yıl
- 2017 KEMP Technologies yılın teknik kişisi
- Parallels RAS EMEA Teknik Destekçisi 2018
- Microsoft Topluluğu Sözcüsü
- En İyi 50 BT Blogu 2020: Feedspot
- En İyi 50 Azure Blogu 2020: Feedspot

Blog sitesi: https://ryanmangansitblog.com
GitHub: https://github.com/RMITBLOG