

TANITIM BELGESİ

Runecast Analyzer ile Operasyonel Karmaşıklığın Azaltılması

vSphere Optimum Performansına ve
Minimal Aksaklık Süresine Ulaşmak

Teknik Danışman, Demitasse Ltd.
tarafından kaleme alınmıştır



Runecast

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com



İçindekiler

Yönetici Özeti	3
Kurum Sanallaştırma Problemi	4
1. Teknoloji karmaşıklığı	4
2. Karşılıklı Bağımlılık	4
3. Toplam değişim oranı	4
4. Bilgi Tabanı makalelerinin hacmi	5
5. Geçici sorun giderme değişiklikleri	5
6. Çözümün uzun sürmesi	5
7. Reaktif hata çözümü	5
Küçük Ölçekli Kurum Sanallaştırma Problemi	7
Küçük Kurum, Küçük Ekip	7
Hata ve Problem Yönetimine Yeni Bir Yaklaşım	8
1. Güvenilir bir üçüncü tarafça işletilen uzman sistem	8
2. En iyi uygulamanın tespiti	8
3. Güvenlik taraması	8
4. Otomatik tarama	8
5. Log izleme	9
6. Bilinen hataların tespiti	9
7. Basitleştirilmiş uygunluk	9
8. Güvenli dağıtım	10
Sonuç	10



Yönetici Özeti

Kurumsal bir vSphere ortamı kullanmak karmaşık bir işlemdir ve bu ortamların kullanılması birçok BT departmanı için kritik bir faaliyettir. Bu vSphere platformları üzerinde uygulamaları olan iş birimleri optimum performans ve minimal aksaklık süresi gerektirir.

Sistem kesintileri işletmelere paraya mal olmakta ve işin genel sağlığını büyük oranda riske atabilir. Aksaklık süresinin ortalama maliyetinin saatte 300,000\$ olduğu tahmin edilmektedir. Kesinti meydana geldiği her an yalnızca mali yönden kayıp var demek doğru olmaz, kurum aynı zamanda BT departmanına olan güvenini de kaybedebilir.

Operasyon ekibinin ne kadar iyi olduğu dikkate alınmaksızın, reaktif hata çözümü aksaklık veya performans problemleri ile sonuçlanır. Sorunun suçunu bir şeyin üzerine atmak gerekirse, problemlerin birçoğu çözümlerinin bilindiği bilinen sorunlardan kaynaklanır.

Kır-onar döngüsünden kurtulmak için farklı bir yaklaşım gerekir. Runecast aksaklık riskini en aza indirmek için proaktif bir hata giderme sağlar.

Runecast çözümü vSphere yapılandırması ve logları bilinen sorun kaynağı ve en iyi uygulamalar ile karşılaştıran otomatik bir sistemdir. Runecast bilinen potansiyel sorunları tespit ederek BT operasyon ekiplerinin hataların önüne geçmesini ve kesintileri önlemesini sağlar. Bilinen hatalar kesintilere sebebiyet vermeden önce giderilebildiği için aksaklık süresi azalır. En iyi uygulamalara tutarlı bir şekilde sürekli olarak bağlı kalınmasını sağlayarak, aksaklık riskini ve bununla ilişkili işletme maliyetlerini azaltır.

Birçok BT departmanı için güvenli denetim ve uygunluk her daim var olan bir sorundur. Runecast kaynağında VMware Güvenlik Güçlendirme Kılavuzundan alınan bir güvenlik kılavuzu yer alır. Güvenlik uygunluğu ile ilgili anında geri bildirim sağlamak için güvenlik kılavuzlarına karşı aynı tarama ve log analizi kullanılır. Dolayısıyla, sanallaştırma altyapısı çok daha güvenlidir.

Altyapı katmanı güçlendirilerek ihlal riski azalır. Ek olarak, denetim uygunluk logu sayesinde güvenlik denetimleri daha basit bir hale gelir.

Sanallaştırılmış bir altyapıda sorunların ele alınmasına yönelik birçok zorluk vardır. Bunların birçoğu kurumun BT karmaşıklığından kaynaklanır. Diğerleri ise operasyon ekiplerinin söz konusu altyapı ile sorunları nasıl çözdüğü ile ilgilidir.

Altyapı ekibinde sıkıntılara yol açabilecek yedi özel alan vardır:

1. Teknoloji karmaşıklığı
2. Karşılıklı bağımlılık
3. Toplam değişim oranı
4. Bilgi Tabanı makalelerinin hacmi
5. Geçiş sorun giderme değişiklikleri
6. Çözümün uzun sürmesi
7. Reaktif hata çözümü



Kurum Sanallaştırma Problemi

1. Teknoloji karmaşıklığı

Mevcut teknolojilere yenileri eklendikçe kurum IT altyapısı giderek daha da karmaşık bir hal almıştır. Blade (yaprak) sunucular rack sunucuların yanına eklenmiştir. Lifli Kanalin ve yerel depoya yanına IP deposu eklenmiştir. Şerit sistemlere disk tabanlı yedeklemeler eklenmiştir ve şu anda birçok veri merkezine birleşik yedekleme eklenir. Hesap bölümüne başka bir katman eklenerek sunucular sanallaştırılır. Depo sanallaştırılır, dolayısıyla daha fazla karmaşıklık yaratılmış olur. Son zamanlar da, ağ ekipleri daha da fazla karmaşıklığa sebep olan Yazılım Tanımlı Ağ (SDN) eklemeye başlamıştır.

Belirli kusurların ele alınması için genellikle nokta çözümler eklenir. Depolama dizininin önüne performansı yeterli olmayan, ancak değişime uygun bir ön bellek yüklenir. Kurumun BT ekipleri benzer sunucularla dolu raf sıralarına sahip bulut ölçekli veri merkezlerinin resimlerine imrenerek bakmaktadır. Kurumların genellikle farklı teknolojileri bir arada bulunduran veri merkezlerinde gördüğümüz şey bu değildir. Eski teknolojileri kullanmayı bırakmaktansa yeni teknolojiler eklemek daha kolaydır. Tüm bu teknoloji parçaları uygunluk ve performansı garanti altına almak için yönetim ve izleme gerektirir. Yönetim gerektiren farklı unsurlar eklerken, daha fazla personel ekleyemeyiz. BT'nin daha iyi operasyon yazılımlarına ihtiyacı vardır. Sanallaştırmanın veri merkezine getirdiği ekstra karmaşıklık ise uygun şekilde belgelendirilmiştir.

2012 yılında DCIG tarafından yapılan bir çalışma, düşük çeviklik ve yavaş şartlandırma sebebi olarak sanallaştırılmış ortamların karmaşıklığına dikkat çekmiştir.

2. Interdependence

Sanallaştırma, teknolojiyi silolara bölmüş ve yeni teknolojilerin benimsenmesini hızlandırmıştır. Sanallaştırma aynı zamanda BT altyapısının farklı kısımları arasında birçok bağıllık ortaya çıkarmıştır. Sanallaştırmadan önce, her bir sunucu bir adaydı ve bu adalar tarafından yalnızca ağ paylaşılırdı. Her sunucunun kendi CPU'su, RAM'i, deposu ve ağ kartları vardı. Sanallaştırılmış bir altyapıda ise her şey paylaşılır ve her şey bağlıdır. Her bir SM, diğer SMLer ile paylaşan bir hipervizör sunucusuna bağlıdır, dolayısıyla hipervizör üzerinde yapılan yanlış bir yapılandırma onlarca SM'yi etkileyebilir. Birçok hipervizör sunucusu üzerindeki birçok SM aynı paylaşılmış depoya erişir ve bir SM ile deposu arasındaki bağlantı birçok katmandan geçer. Depo dizinine ulaşmadan önce VM'den başlayıp hipervizörün içinden, daha sonra depolama ağının üzerinden geçer. Bu katmanların her biri, herhangi bir katmanda meydana gelen yanlış yapılandırma genel performans veya uygunluk problemlerine sebep olabileceğinden optimum düzeyde yapılandırılmalıdır. Sanallaştırılmış bir veri merkezi üst üste yığılmış bir teknolojiler kulesidir. Kuledeki her bir kat veri merkezinin bütününde tutarsızlığa sebep olabilir. BT ekipleri kulenin tamamında tutarlılık sağlayan operasyon yazılımına ihtiyaç duyar.

3. Toplam değişim oranı

Kurum ortamları değişimi kontrol altında tutmaya çalışır, ancak değişim her zaman vardır ve büyük bir ortamda neredeyse devamlı bir değişim hali vardır. Bu ay yedekleme ekibi yeni bir disk yedekleme hedefi verebilir. Bir sonraki hafta ise sanallaştırma ekibi 20 switch için altı VLAN ekleyebilir. Her bir unsurun değişmesi yavaş olurken, kurumun

Kurum Sanallaştırma Problemi

veri merkezindeki unsurların sayısı değişimin sürekli olduğu anlamına gelir. Her bir değişim BT altyapısının yığılmış kulesi aracılığıyla bağlılıklara sahiptir. Her değişim bütün bir yığınin istikrarını bozabilir ve her biri bir şeylerin ters gitmesine veya gizli bir sorunun bir probleme neden olmasına sebep olur.

Bir değişimin etkisini tahmin etmek her zaman mümkün değildir. Her BT operasyon ekibinin değişimin negatif sonuçlarını hızlı bir şekilde tespit etmenin yollarına ihtiyacı vardır. Aynı zamanda ortamdaki güncellemeler veya değişiklikler uygulandığında problemlere neden olabilecek her türlü gizli sorunu da tespit etmeleri gerekir.

4. Bilgi Tabanı makalelerinin hacmi
VMware Bilgi Tabanında, farklı VMware versiyonları ve kombinasyonları ile üçüncü taraf ürünleri ile ilgili potansiyel sorunları belgelendiren yüzlerce makale yer alır. Kesinti riskini minimum seviyeye indirmek ve performansı optimize etmek adına, tüm Bilgi Tabanı makalelerinde verilen ilgili tavsiyelere uyulmalıdır. Herhangi bir konudaki ilgili makalelerin zamanla öğrenilmesi büyük oranda zordur. Daha önemli bir zorluk ise değişime ayak uydurmaktır. Yalnızca sanallaştırma ortamında değişiklikler olmaz, aynı zamanda VMware'in Bilgi Tabanında yer alan makalelere haftalık olarak eklemeler yapılır ve mevcut olanlar güncellenir. Makaleleri yayınlandıkça okuyarak veya herhangi bir değişiklik yapılmadan önce Bilgi Tabanını aratarak güncel kalmak yeterli değildir. VMware Bilgi Tabanından tam olarak faydalanmak için bir tür otomatik sistem gereklidir.

5. Geçiş sorun giderme değişiklikleri
Planlanan aktiviteler yalnızca Kurumun veri merkezlerindeki değişimden kaynaklanmaz. Genellikle değişim bir hata nedeniyle başlar. Yinelenen bir sistem arızası yaşayan bir ESXi sunucusu donanım yazılımını güncellettirmiş olabilir. Şu anda bu sunucu diğer sunucularımızdan farklıdır. Genellikle sorun giderme süreci kriz anında çoklu değişikliklerin yapılmasını kapsar. Değişimlerin birçok etkisizdir ve yedeklenmelidir, ancak genellikle gerçekleştirildiği yerde bırakılır.

Tutarsızlık daha fazla destek gereksinimlerine yol açacaktır. Tutarsızlık kesinti riskini artırır ve çözüm süresini geciktirir. Ancak, tutarlılığın yeniden kazandırılması daha fazla değişim gerektirecektir.

Sunucu standart yapılandırma ile düzeltilmeli veya diğer sunucular aynı değişikliğe sahip olmalıdır. Değişim çoğu kez unutulur ve giderek her sunucunun yapılandırması özel bir hal alır. Operasyon ekibinin önceliği çoğu durumda çalışma zamanı ve hatanın çözümünü olmalıdır. Tutarlılığı yeniden kazanmak şöyle dursun, emsalsizliği takip etme yöntemine bile sahip olmayabilirler. Her BT ekibinin tutarlılığı ve uygunluğu tespit eden uygun standartlara sahip otomatik bir sisteme ihtiyacı vardır.

6. Çözümün Uzun Sürmesi
Bu sanallaştırma platformlarının karmaşıklığı nedeniyle, hata ve düzeltici eylem tespit edilse dahi hata çözümü ertelenebilir. Hata raporlamanın teknik bir kaynak tarafından

Kurum Sanallaştırma Problemi

görülmesi günler alabilir. Araştırmalar başladıktan sonra, verilerin toplanması, logların alınması ve yapılandırma analizi için zaman gerekebilir. Hata tespit edildikten ve çözüm formüle edildikten sonra, çözüm sürecinin test edilmesi biraz zaman alabilir. Değişim yönetimi genellikle performans ve uygunluk değişikliklerinin onaylanana kadar geciktirilmesini talep eder.

Büyük kurumlar için bu işlem birkaç hafta sürebilir ve kurumu büyük çapta bir risk veya performans sorunlarına maruz bırakır. BT problemlerinin yavaş çözülmesi doğrudan BT sistemlerinin memnuniyeti ile ilişkilidir. Teknik destek endüstrisi grubu HDI tarafından yürütülen bir çalışma, yavaş çözüm ile düşük memnuniyet arasında doğrudan bir ilişki olduğunu göstermektedir. Bilinen sorunların problemlere sebep olmadan tespiti, değişim yönetim sürecinin kurum etkilenmeden önce başlamasını sağlar.

7. Reaktif hata çözümü

Birçok hata çözümünün herhangi bir şekilde harekete geçilmeden önce üretime etki etmesi gerekir. Herhangi bir şekilde harekete geçmeden önce bir sunucu hata vermeli veya bir uygulamanın performansı düşmelidir. Bu hatalar kurumlarda ciddi maliyetler doğurmaktadır; bazı sistem kesintileri milyon dolarlara mal olmaktadır.

Bu durum Runecast'ın tasarlanma nedeninin merkezine nokta atışı yapmaktadır. İyi yönetilen bir veri merkezinde bir kesinti meydana geldiği zaman, bunun sebebi çoğu zaman sistem sağlayıcısı tarafından bilinen bir hatadır. Daha sonraki yazılım sürümünde yamalanmış bir hata veya özel bileşen kombinasyonunda çalışmayan hatalı bir yapılandırma

olabilir. Sorunu gideren mühendis, bilinen sorunu bulmak ve bilinen çözümü uygulamak için Google'ı kullanacaktır. Birçok bileşen kombinasyonuna sahip binlerce bilinen sorun vardır. VMware Bilgi Tabanında yer alan makalelerdeki yeni durumları her hafta belgeler. Bazı operasyon ekipleri her yeni makaleyi ortamları ile ilişkisi bakımından inceler, ancak birkaç ekip aynı zamanda ortamları ile ilişkili makalelerin değişimini takip eder. Bir probleme sebebiyet vermeden önce bu bilinen kötü durumların tespit edilmesinin elverişsiz olması Runecast ürününün tasarlanmasına neden olmuştur.

BT operasyon ekipleri, kesintiye sebep olmadan önce bilinen sorunları tespit edebilecek bir yazılıma ihtiyaç duymaktadır. Küçük ölçekli kurumlar da büyük şirketler gibi aynı sorunları daha küçük bir ölçekte yaşarlar. Bu şirketlerin sanallaştırma altyapıları halen birbirine bağımlı olan karmaşık teknolojilerin toplanması şeklindedir. Reaktif hata çözümünü uygulamaya devam etmektedirler ve bu çözümde gecikmeler olabilmektedir. Küçük ölçekli bir kurum ortamında, daha yetersiz bir BT yönetim süreci uygulandığı için tutarlılık yakalamak dahi daha zor olabilir.

Kurum tarafından vSphere dağıtımında ESXi sunucular genelinde kısa süreli tutarlılığa yönelik Host Profilleri kullanılabilir, küçük ölçekli bir kurumun Host Profillere sahip vSphere ruhsatını alma ihtimali düşüktür. Bu kurumlar sürekli manuel yapılandırmaya bağlı olacaktır ve en iyi uygulamalar için manuel olarak harekete geçeceklerdir.

Manuel süreçler tutarsız olmamalarıyla bilinir, bu da SMB vSphere dağıtımlarında tutarlılığın sağlanamamasına neden olur.



Küçük Ölçekli Kurum Sanallaştırma

Küçük Kurum, Küçük Ekip

Küçük kurumlara ilişkin ekstra bir zorluk da daha az personele ve bu personelin uzmanlaşması için daha az imkana sahip olmasıdır. Küçük ölçekli kurumlardaki BT personeli genellikle vSphere ortamından çok daha fazlasından sorumludur. Genellikle bir kişi Windows altyapısı ve uygulamaları ile ilgilenir ve vSphere platformuna odaklanmak için yalnızca sınırlı zamanı vardır.

Bu personelin ayrıntılı bir uzmanlığa gerek olmaksızın kapsamlı olarak becerikli olması gerekir. Uzmanlar genellikle belirli projeler için danışmanlık şirketlerinden alınmaktadır. Bu uzmanlar ücret bakımından bir hayli pahalıdır ve yalnızca proje süresince hizmet verir. Proje sonra erdikten sonra sorumluluk yine BT yetkililerine kalır. SMB BT personelinin veri merkezlerinde yer alan tüm teknolojileri güncel tutması imkansızdır. Danışmanlık ücreti olmadan dış kaynaklı bir uzmanlığı içeri getiren otomatik bir sistem, küçük kurumların sanallaştırma işleminin minimum maliyetlerle gerçekleştirilmesini sağlamanın tek yoludur.

Bu sorunların ele alınması kurum sanallaştırma platformunun yönetilmesine farklı bir bakış açısı getirilmesini gerektirir. Bir husus ideal olarak günde birçok kez yapılacak şekilde otomatik ortam taramasını kullanmaktır. Diğer bir husus ise analiz için sistem loglarının merkezileştirilmesidir. Sonuçların bilinen sorunlar dizisi ve en iyi uygulamalar ile karşılaştırılması gerekir. Bütün amaç, uygunluğu etkilemeden önce her türlü bilinen problematik durumu tespit etmektir.

1. Güvenilir bir üçüncü tarafça işletilen uzman sistem

VMware Destel Bilgi Tabanında sorun giderme ile ilgili çok sayıda bilgi bulunmaktadır. Çoğu zaman Google'da vSphere problemlerini aratan mühendislerin varacağı nokta burasıdır. Bu Bilgi Tabanı kendisine otomatik tarama uygulamaz; yazılıdır ve formatı insanlar tarafından okunmak üzere tasarlanmıştır. VMware ortamınız ile ilgili herhangi bir Bilgi Tabanı makalesi olup olmadığını kontrol etme yolu sunmaz.

Runecast bu işlevi sağlar, ürünün merkezinde yer alarak programlanabilir bir biçimde erişilebilir bir kaynaktır. Runecast VMware Bilgi Tabanındaki tüm makaleleri analiz etmiş ve Runecast merkez kaynağına eyleme geçirilebilir sonuçlar eklemiştir. Her bir Runecast aracıda analizlerin tümüne yönelik referans olarak kaynağın yerel bir kopyası yer alır. VMware Bilgi Tabanına yeni makaleler ekledikçe, bunlar da merkez kaynağına eklenir. Bu güncellemeler yerinde çalışan Runecast araçlarına çevrim içi olarak iletilir. Bilgi Tabanındaki en güncel makaleler daha sonra yerinde analize dahil edilir.

2. En iyi uygulamanın tespiti

VMware Bilgi Tabanı stabilite ve performans için yapılandırmalar tespit eder. Güvenli ve çalıştırması ve yükseltmesi kolay bir vSphere dağıtımını oluşturmaya yönelik kılavuz bilgileri içermesi gerekmez. En iyi uygulama kılavuzunun Runecast kaynağının bir parçası olmasının sebebi budur: bir kümedeki tüm ESXi sunucularına erişebilen aynı paylaşılmış



Hata ve Problem Yönetimine Yeni Bir Yaklaşım

veri deposuna sahip olmak veya küçe için koordineli zaman sağlayan aynı sunuculara sahip olmak gibi basit bir kılavuz.

3. Güvenlik taraması

Güvenlik uygunluğu yalnızca denetimlerden geçmek ile ilgili değildir; güvenlik ihlallerinin kurumlarda ciddi finansal maliyetler doğurur. Pnemon Institute tarafından yapılan bir çalışma, bir güvenlik ihlalinin ortalama maliyetinin

4 milyon \$ civarında olduğunu saptamıştır. Finansal problemlere ek olarak, ihlal duyulduktan sonra müşteri güveninde ciddi kayıplara sebep olabilir. Target, Sony ve Ashley Madison gibi kurum isimleri güvenlik ihlalleri ile eş anlamlı hale gelmiştir. Güvenli uygulamaların ve faaliyetlerin desteklenmesi için altyapının baştan sonra güvenli olması esastır.

VMware, Güvenlik Güçlendirme Kılavuzlarında güvenlik yapılandırmasına ilişkin kılavuz yayınlamaktadır. Bu güçlendirme kılavuzları aynı zamanda Runecast kaynağını da zenginleştirir. Kaynak, vSphere dağıtımı ile ilgili yolunda gidebilecek veya gitmeyebilecek her şeye dair düzenli bir kaynak oluşturmak adına VMware Bilgi Tabanını, VMware Güvenlik Güçlendirme Kılavuzu ve en iyi uzman uygulamaları bir araya getirir.

4. Otomatik tarama

Yanlış yapılandırmalar her zaman olabilir ve serviste risk teşkil edebilir. Otomatik bir tarama sistemi risk durumlarını hızlı bir şekilde tespit edebilir. Haftalık veya aylık kontrolleri beklemek, servisi gereğinden fazla uzun bir süre risk altında bırakır. Sistem taramasının sanallaştırma platformu

üzerindeki performans etkisi ağırlıklı olarak keşfedilmemiş durumların öylece bırakılması riskine karşıdır.

Hafif tarama yöntemi Runecast'ın vSphere ortamının tamamını dakikalar içerisinde taramasına olanak tanır. Tarama performansı etkilemeden her gün birçok kez yapılabilir. Sık yapılan tarama işlemi, kesinti riskini azaltarak hata durumunun bulunduğu süre miktarını minimuma indirecektir. Runecast kaynağının sık sık güncellenmesi, VMware Bilgi Tabanına eklenen yeni sorunların bir sonraki taramada hemen tespit edilmesini sağlar.

5. Log izleme

Bütün hatalar ESXi sunucu yapılandırmaları ile ilgili değildir. Birçok hata ESXi sunucularının örneğin switch ve depolama ağları gibi dış unsurlarla etkileşiminden kaynaklanır. Runecast, depolama zaman aşımaları veya VMkernel hata mesajları gibi her türlü hata mesajı da dahil olmak üzere ESXi sunucularından ve SMLerden (sanal makinelerden) bütün logları almak için otomatik bir Syslog yapılandırması kullanır. Syslog mesajları Runecast aracı tarafından alınırken gerçek zamanlı olarak Runecast kaynağındaki bilinen sorunlar ile karşılaştırılır.

6. Bilinen Hataların Tespiti

Tarama ve log toplama ile kaynağı birleştirerek, büyük belirtiler göstermeden önce potansiyel hataların tespiti için bir mekanizma oluşturmuş oluruz. Bilinen bir hata ile ilişkili her türlü olay Runecast konsolunda bir uyarıyı tetikleyecektir.



Hata ve Problem Yönetimine Yeni Bir Yaklaşım

Benzer şekilde, sorunlara yol açtığı bilinen yazılım ve yapılandırma kombinasyonları tespit edilecektir.

Örneğin, ESXi versiyonları ve sürücülerinin kombinasyonu özel gelişmiş ortamın stabil olmasını gerektiriyorsa, Runecast bu durumu tespit edebilir. Bir sorun tespit edildiğinde, Runecast konsolu düzeltme adımlarını belirler ve bilgi kaynağı ile bağlantı kurar.

7. Basitleştirilmiş Uygunluk

Denetim altındaki birçok sektör için güvenlik uygunluğu sürekli bir uygulamadır. Güvenlik açıklarını önlemek için, güvenli yapılandırmaların ve sağlam prosedürlerin uygulanması önemlidir. Runecast, VMware Güvenlik Güçlendirme Kılavuzunda yer alan tavsiyelere uygunluğu kontrol edecektir. Doğal olarak, bu uygunluk kontrolü kurumunuzun gerektirdiği özel güvenlik yapılandırmaları kombinasyonuna göre ayarlanabilir.

Periyodik güvenlik taraması, sistemlerin zaman içerisindeki uygunluğunun korunmasını sağlayarak, güvenlik uygunluğu için önemli bir prosedürdür. Basit bir şekilde zaman içerisinde tek bir noktada uygun hareket etmekten ziyade bu çok daha iyi bir çözümdür ve manüel uygunluk kontrolünden daha güvenilirdir. Bir tabana karşı sürekli tarama yapmak güvenlik denetimlerinin daha basit olmasını sağlar.

8. Güvenli Dağıtım

Runecast yerinde vSphere ortamınızın içerisinde sanal bir araç olarak dağılır. Tüm tarama ve analiz işlemleri araç üzerinde yerel olarak gerçekleştirilir.

Araç Runecast kaynağının tam kopyasını içerir. Verilerinizin veya üst verilerinizin hiçbirisi İnternete aktarılmaz; esasen Runecast aracının çalışması için İnternet bağlantısına gerek duyulmaz. Kaynak güncellemeleri doğrudan İnternet üzerinden VAMI arayüzü kullanılarak araç güncellemeleri olarak iletilir. Alternatif olarak, güncellemeler İnternet olmadan bağlanan dağıtımlara yüklenebilir ve iletilebilir.

Sonuç

Runecast, vSphere dağıtımınızda bu dağıtımı gelecekte etkileyebilecek sorunları tespit etmenizi sağlar. Bu sorunların proaktif bir şekilde çözülmesi kesinti ve aksaklık riskini, dolayısıyla kurumun da ilgili maliyetini azaltacaktır.

Runecast, VMware Bilgi Tabanı belgelerinin bir kaynağını, güvenlik güçlendirme kılavuzu ve en iyi uzman uygulamaları sunar. vSphere yapılandırmanız ve loglarınız muhtemel sorunları ortamınızda bir hataya sebep olmadan önce tespit etmek amacıyla bu kaynak ile karşılaştırılır.

Tespit edilen sorunların düzeltilmesi hataları önler ve daha iyi çalışma zamanı sağlar ve riski azaltır. Sonuç ise kurum için daha değerli ve kurum tarafından daha fazla güven duyulan bir vSphere altyapısıdır.

Altyapınızı kaya gibi sağlamlaştırmaya başlamak için <https://www.runecast.com/> adresini ziyaret edin.

Runecast Analyzer'ı nasıl dağıtabilirim:
Runecast Analyzer aracınızın değerlendirme kopyasını aktif hale getirmek için

<https://portal.runecast.com/registration> adresin üzerinden kayıt olabilirsiniz.

Runecast İletişim
innovate@runecast.com
www.runecast.com

