COHESITY

ARTIGO TÉCNICO

Topologias modernas de segurança e gerenciamento de dados: um guia para líderes de TI

Modelos e melhores práticas para reduzir o risco e fortalecer a resiliência dos negócios

CONTEÚDO

Introdução

Três fatores impulsionam a necessidade de uma nova abordagem para a segurança e o gerenciamento de dados. O primeiro é imperativo para a transformação digital e infraestrutura orientada por API. Os líderes de TI estão modernizando todos os aspectos de suas propriedades de TI para viabilizar maior automação, extensibilidade, escala em nuvem, arquiteturas definidas por software e os princípios de segurança shift-left.

Em segundo lugar, o cenário de ameaças cibernéticas está evoluindo de maneiras complexas e imprevisíveis. Os patrimônios de dados existentes de muitas organizações estão isolados, resultando em maior risco operacional de um ataque cibernético. Uma pesquisa recente indica que 32% das organizações acreditam que a agilidade na recuperação é prejudicada por sistemas de backup e recuperação obsoletos. Da mesma forma, 34% dizem que a falta de integração entre as equipes de TI e segurança também prolonga os tempos de recuperação.

E terceiro, o advento da IA fez com que os líderes buscassem plataformas de dados modernas que tornem os dados corporativos acessíveis a tecnologias de IA generativas.

Todos os executivos de TI que lideram um projeto de modernização de dados podem se beneficiar "subindo nos ombros de gigantes". Neste artigo técnico, descrevemos as considerações de design mais importantes e como chegar à melhor abordagem de resiliência de dados, considerando os requisitos comuns da empresa. Nossa experiência em milhares de implantações e nosso conhecimento das melhores práticas influenciaram nossas perspectivas.

A orientação a seguir pretende ser independente de fornecedores, mas usaremos os nomes de marca da Cohesity para simplificar.

Principais fatores de design

Todos os projeto de modernização que valem a pena trazem riscos. Isso certamente se aplica ao transformar os processos e as ferramentas de segurança e gerenciamento de dados corporativos. Mas há boas notícias: é possível construir a partir do trabalho que os outros fizeram antes de você. Muitas organizações modernizaram com sucesso sua propriedade de dados, e nós catalogamos essas melhores práticas neste artigo.

Os líderes de TI e segurança cibernética têm a tarefa de equilibrar agilidade, risco e custo em sua propriedade de TI. Esse patrimônio é dinâmico e agora abrange dados e aplicativos executados em data centers locais, nuvens públicas, instalações de colocation e locais de borda. Os esforços de modernização crescem em escala e abrangência ao longo do tempo, à medida que o volume de aplicativos, dados e fontes de dados se multiplica.

A modernização do patrimônio de dados das empresas é ainda mais complicada por:

- Diversos alvos de infraestrutura em diferentes locais e várias cargas de trabalho, resultando em fragmentação de dados e processos de backup e recuperação ineficientes
- Falta de habilidades suficientes de TI e segurança cibernética na maioria das organizações
- Um cenário de segurança cibernética em rápida transformação, com centenas de ataques a cada minuto. A evolução e a sofisticação dos ataques tornam a identificação precoce crucial.

Dito isso, há alguns "princípios fundamentais" a serem lembrados.

A regra 3:2:1 ainda se aplica

A regra 3:2:1 declara que você deve manter pelo menos três cópias de dados, que esses backups devem ser armazenados em dois tipos diferentes de mídia ou plataformas e que pelo menos uma das cópias deve ser mantida fora do local.

O valor duradouro da regra 3:2:1 deriva de três conceitos que continuam a impulsionar o projeto de topologia do sistema na era nativa da nuvem:

- Requisitos de negócios
- Domínios de falha
- Eventos de força maior

Vamos descrever cada um desses conceitos em detalhes. Elas sempre foram os principais focos do setor e continuam assim hoje, especialmente com a intensificação das preocupações sobre ataques cibernéticos. Os ataques cibernéticos nem sempre estiveram no centro das atenções, mas agora certamente estão.

Definiremos como esses três conceitos influenciaram os projetos de backup e recuperação ao longo do tempo e discutiremos como as preocupações com ataques cibernéticos estão forçando nossos clientes a se perguntarem se suas topologias de implantação existentes ainda são suficientes (ou não).

Vamos abordar cada um de cada vez:

Requisitos de negócios

As empresas devem aderir a um amplo conjunto de requisitos de negócios, regulatórios e de conformidade. Muitos desses requisitos impulsionam a necessidade de retenção de cópias de dados atuais e passadas. Por exemplo, uma equipe de conformidade pode precisar obter um contrato assinado há três anos para responder

a uma solicitação de um regulador do setor. Ou uma equipe fiscal pode precisar recuperar arquivos para uma auditoria contínua. Ou, em termos mais próximos da realidade, talvez um arquivo crítico tenha sido excluído acidentalmente e precise ser restaurado.

Domínios de falha

É consenso no setor de tecnologia que tanto o software quanto o hardware falharão. Os fornecedores de hardware e software empregam recursos excepcionais para contornar essa realidade, contudo as falhas continuam. As equipes de TI precisam se preparar para falhas, e assegurar que essas intercorrências não afetem adversamente a empresa ou suas operações. Como exemplo, podemos citar falhas de carga de trabalho, como corrupção de máquina virtual ou volume de armazenamento, ou falha na implementação de patch de sistema operacional. Em ambos os casos, a equipe de TI precisa se recuperar da falha e, como parte dessa recuperação, provavelmente recorrerá a dados de seu sistema de backup e recuperação.

Há algumas décadas, os líderes não precisavam se preocupar com falhas causadas por agentes mal-intencionados. Hoje, os ataques cibernéticos não são apenas um dos principais impulsionadores de falhas do sistema, mas talvez a causa de falha mais visível, e que chama a atenção do conselho administrativo.

Eventos de força maior

Este termo refere-se a desastres naturais ou outros eventos que estão fora do controle humano e não podem ser previstos ou evitados por meios razoáveis. Eventos adversos como incêndios, terremotos, inundações e cortes de cabos podem ser considerados eventos de "força maior". Assim como ocorre em domínios de falhas, as organizações de TI precisam considerar o potencial para casos força maior e construir sistemas de projeto que sejam resilientes a eles.

A regra 3:2:1 oferece orientação prática diante de eventos de força maior.

Os sistemas falham, por isso é sensato ter várias cópias dos dados disponíveis. Devido a domínios de falhas, também é aconselhável manter os backups em dois tipos ou sistemas de mídia diferentes. Por fim, devido a riscos de eventos de força maior, é responsabilidade da governança manter pelo menos uma dessas cópias em um local remoto, talvez como parte de um local de recuperação de desastres ou data center remoto.

Seus requisitos podem variar, mas existem semelhanças

Embora a regra 3:2:1 seja uma prática sólida, as organizações podem optar por implantações com menos de três cópias. Outros aderem mais estritamente à regra 3:2:1. Outros ainda guardam mais de três cópias. (Vamos explicar a justificativa para essas escolhas de design mais adiante neste artigo.)

Em relação ao design, agrupamos as topologias de implantação ("modelos") em três tipos.

Tipo	Descrição
Básico	Uma topologia de implantação com duas ou menos cópias.
Aprimorado	Uma topologia de implantação com três cópias.
Missão crítica	Uma topologia de implantação com quatro ou mais cópias.

Arquiteturas de disponibilidade familiares ainda são relevantes hoje em dia

Vamos passar a usar um termo com o qual os líderes e profissionais de TI experientes estão mais familiarizados: arquitetura de disponibilidade.

Uma arquitetura de disponibilidade descreve como uma equipe de TI pode organizar seus sistemas de hardware e software para que sejam resilientes a uma possível interrupção. Em nossa experiência, a maioria das implantações empresariais consiste em uma das três arquiteturas de disponibilidade do cliente: ***"ativo-ativo", "ativo-standby" e "hub e spoke"***.

Cada uma dessas abordagens é mostrada na próxima página.

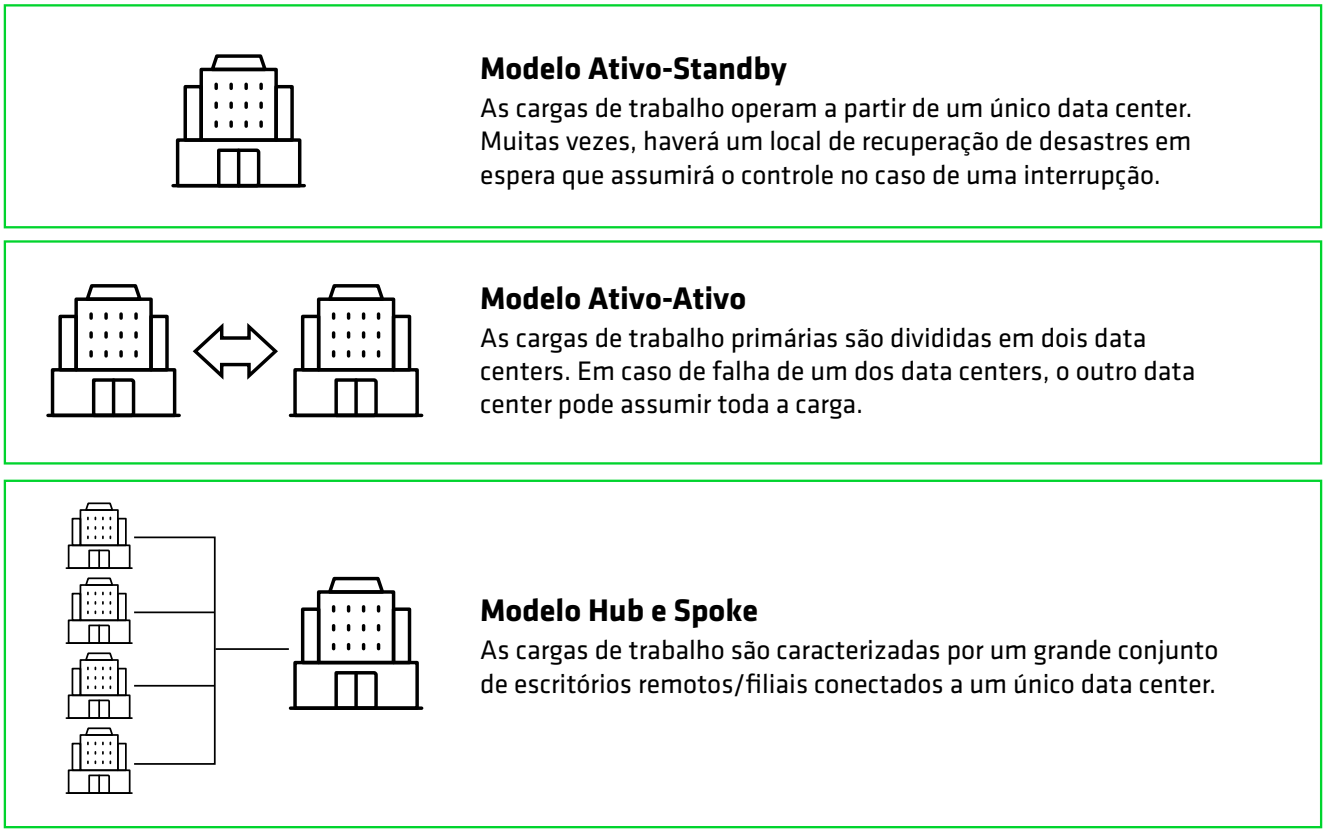


Fig. 1: Arquiteturas de disponibilidade do cliente

Em cada caso, a arquitetura de disponibilidade é projetada para garantir que as operações comerciais possam continuar em caso de falha. Quando o lado "ativo" de uma arquitetura **ativa-standby** apresenta uma falha, todo o processamento passa para o outro sistema em espera. Quando um dos lados de um sistema **ativo-ativo** falha, o outro lado assume 100% da carga de trabalho. E quando há uma falha em um sistema **hub e spoke**, como quando os dados são destruídos por uma falha de hardware ou outro problema em uma filial, o sistema e seus dados podem ser restaurados a partir do hub assim que a causa da falha for resolvida.

As equipes de TI responsáveis projetaram essas arquiteturas de disponibilidade e as testam rotineiramente para garantir que os mecanismos de resiliência funcionem adequadamente.

Nosso conjunto de melhores práticas de modelos é informado por essas arquiteturas de disponibilidade comprovadas. Na Cohesity, não implantamos sistemas de backup e recuperação em um vácuo. Nós os projetamos para se alinharem de perto com a infraestrutura de TI subjacente. Você verá isso em detalhes quando abordarmos várias topologias de backup e recuperação, e como essas topologias mapeiam para arquiteturas de disponibilidade de TI, mais adiante neste artigo.

Modelos para segurança e gerenciamento de dados modernos: tipos e topologias

Já discutimos tipos de backup básicos, aprimorados e de missão crítica. Agora, apresentaremos as topologias associadas a esses tipos.

Mas primeiro, algumas definições. Os sistemas de segurança e gerenciamento de dados podem armazenar dados por meio de diferentes métodos. Cópias de dados podem ser mantidas como ***backups, réplicas*** ou ***arquivos***.

Seguem algumas regras básicas:

- Os **backups** são formados a partir de uma cópia primária e resultam em dados deduplicados, comprimidos e criptografados. Esse processamento é realizado uma vez nos dados e, em seguida, os dados de backup processados podem ser copiados para uma réplica ou um arquivo.
- As **réplicas** são geralmente usadas para retenção de curto prazo, geralmente meses, mas não anos. Em geral, essas réplicas têm suporte para arquiteturas de disponibilidade de TI, como ativo-ativo ou ativo-standby.
- Em geral, os **arquivamentos** são usados para retenção de longo prazo e, muitas vezes, são mantidos por anos. Muitas vezes, os arquivamentos são usados para fins de conformidade e regulatórios, mas em alguns casos também são usados para arquiteturas de disponibilidade de TI.
- A **restauração de um backup ou réplica** é um processo de uma etapa e é mais rápida do que a restauração de um arquivo, que é um processo de duas etapas. O arquivo precisa ser baixado no sistema de backup e recuperação do fornecedor antes de ser restaurado no sistema de TI.
- A **restauração de um ataque de ransomware** é complicada pela necessidade de restaurar uma cópia limpa e não infectada que provavelmente não será o backup mais recente. Uma organização não pode simplesmente reestabelecer as operações após um ataque de ransomware da mesma forma que se restabelece de uma falha de domínio ou interrupção causada por um evento de força maior. A organização afetada terá que analisar o ambiente e garantir que as cópias que estão sendo recuperadas estejam livres da infecção por malware que causou o ataque em primeiro lugar.

A lista de topologias aparece na tabela abaixo. Observe que cada topologia tem um único backup onde os dados são deduplicados, comprimidos e criptografados. Além do backup, as várias topologias também podem manter uma ou mais réplicas e um ou mais arquivos. Atribuímos um descritor (B1, B2, E1, E2, M1, M2 etc.) a cada tipo de topologia para ajudar no acompanhamento.

Tipo	Cópias	Topologia/tipo de cópias
Básico	1	B1 – Backup
	2	B2 – Backup e arquivamento
	2	B3 – Backup e replicação
Aprimorado	3	E1 – Backup, replicação e arquivamento
	3	E2 – Backup e replicação dupla
Missão Crítica	4	M1 – Backup e replicação dupla com arquivamento
	4	M2 – Backup, replicação e arquivamento duplo
	5	M3 – Backup, replicação dupla e arquivo duplo

Uma combinação de tipo/topologia é definida pelo **número de cópias e pela natureza dessas cópias**. Por exemplo, um tipo Aprimorado, que sempre inclui três cópias, pode ter duas topologias distintas. Uma topologia é backup, replicação e arquivamento, enquanto a outra é backup e replicação dupla. Observe que nem toda permutação de cópias de dados está listada acima; essa lista simplesmente representa as implantações mais comuns. Algumas combinações simplesmente não fazem sentido comercial ou técnico.

É útil entender quais topologias são comumente usadas e quais não são. A popularidade relativa de cada padrão pode oferecer caminhos úteis de "atualização" à medida que as equipes de TI consideram proteção adicional para seu patrimônio de dados.

Modelos: a lista completa de topologias

Agora que descrevemos tipos, topologias e arquiteturas de disponibilidade de clientes, vamos apresentar a lista completa de modelos do setor.

Este gráfico inter-relaciona todos os conceitos que discutimos anteriormente. Todas as configurações representam uma escolha frequente em empresas reais que operam em escala com a Cohesity.

Tipo	Topologia/tipo de cópias	Arquitetura de disponibilidade do cliente		
		Modelo Ativo-Standby	Modelo Ativo-Ativo	Modelo Hub e Spoke
Básico	B1 Backup (1)	•	•	
	B2 Backup e Arquivo (2)	•	•	
	B3 Backup e Replicação (2)	•	•	
Aprimorado	E1 Backup, replicação e arquivamento (3)	•	• •	•
	E2 Backup e replicação dupla (3)	•	•	
Missão Crítica	M1 Backup e replicação dupla com arquivamento (4)	•		
	M2 Backup, replicação e arquivamento duplo (4)	•	•	
	M3 Backup, replicação dupla e arquivamento duplo (5)		•	

Uma ressalva sobre as topologias de missão crítica. Essas topologias foram implantadas, demonstradas, testadas ou discutidas em detalhes com empresas ou outros grandes clientes. Observamos anteriormente que muitos clientes buscam maior resiliência para suas implantações. As discussões envolvem maneiras práticas de proteger cópias adicionais de dados. Uma solução comum é aprimorar a implantação com um cofre cibernético. Por esse motivo, muitas das topologias de missão crítica contêm um arquivo configurado como um cofre cibernético. (Oferecemos o Cohesity FortKnox para este cenário.) Muitas topologias podem se tornar mais resilientes com a adição de um cofre cibernético.

Agora discutiremos os tipos e as topologias em detalhes, um grupo de cada vez.

Básico

Topologia	Data Center Primário	Modelo Ativo-Ativo
B1 – Backup	✓	✓
B2 – Backup e arquivamento	✓	✓
B3 – Backup e replicação	✓	✓

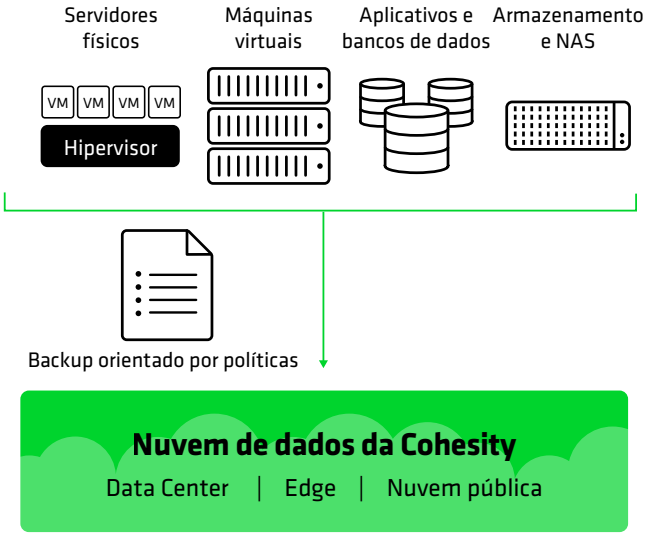
Básico é usado com frequência para dados de valor baixo e moderado ou nos casos em que o cliente já tem várias cópias de seus dados. Topologias básicas são usadas quando há um único data center primário, e também para abordagens do modelo ativo-ativo.

O que é um cofre cibernético?

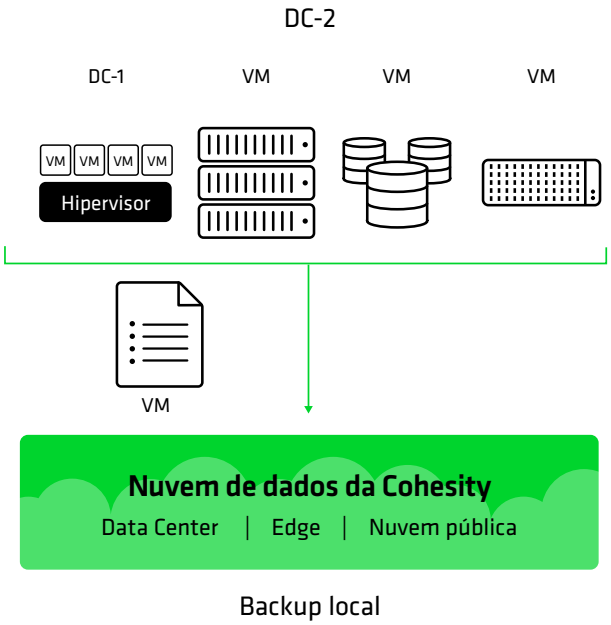
Um cofre cibernético armazena uma cópia isolada dos dados de produção, muitas vezes fora do local. Com uma cópia limpa, separada e protegida dos dados sempre em standby, as organizações podem recuperar rapidamente os dados de volta ao original ou a locais de backup alternativos, em caso de ataque de ransomware ou outro incidente que comprometa os sistemas de produção ou de backup primário. Uma estratégia moderna de cofre cibernético usa a tecnologia de "virtual air gap", que protege os backups, mas permite conexões de rede temporárias para acesso remoto, embora com controles muito fortes, isolando ainda mais os dados na nuvem, conforme necessário. Um cofre cibernético bem projetado pode ser uma parte eficaz de uma estratégia robusta de isolamento de dados e resiliência cibernética.

Básico: B1 – Backup local

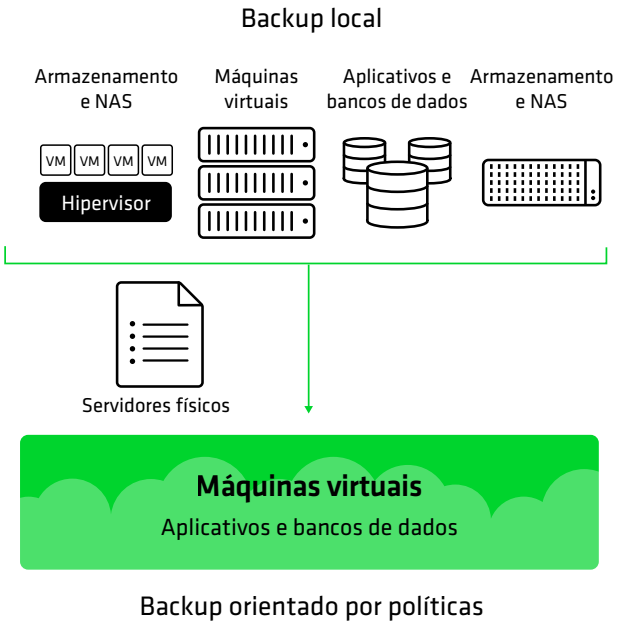
Esta é uma abordagem básica, com apenas uma cópia de backup dos dados. Muitos data centers de TI ainda usam essa abordagem, embora ela não tenha provisão para recuperação de desastres ou retenção de dados de backup de longo prazo. Essa abordagem é normalmente usada para dados de baixo valor.



Básico: B1 – Backup (Ativo-Ativo)



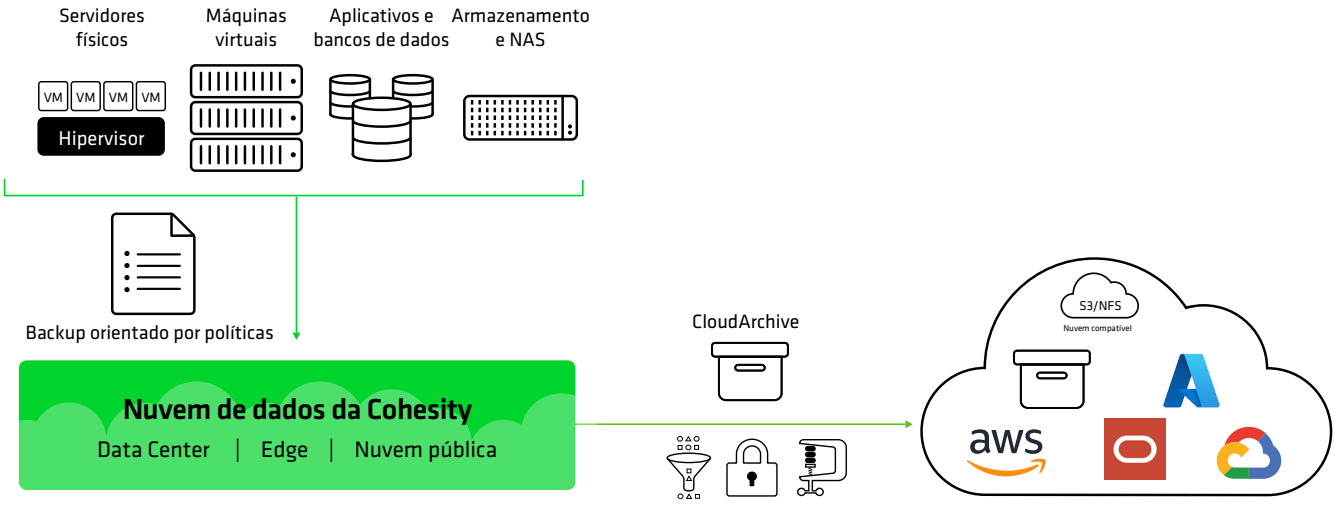
Backup local



Backup orientado por políticas

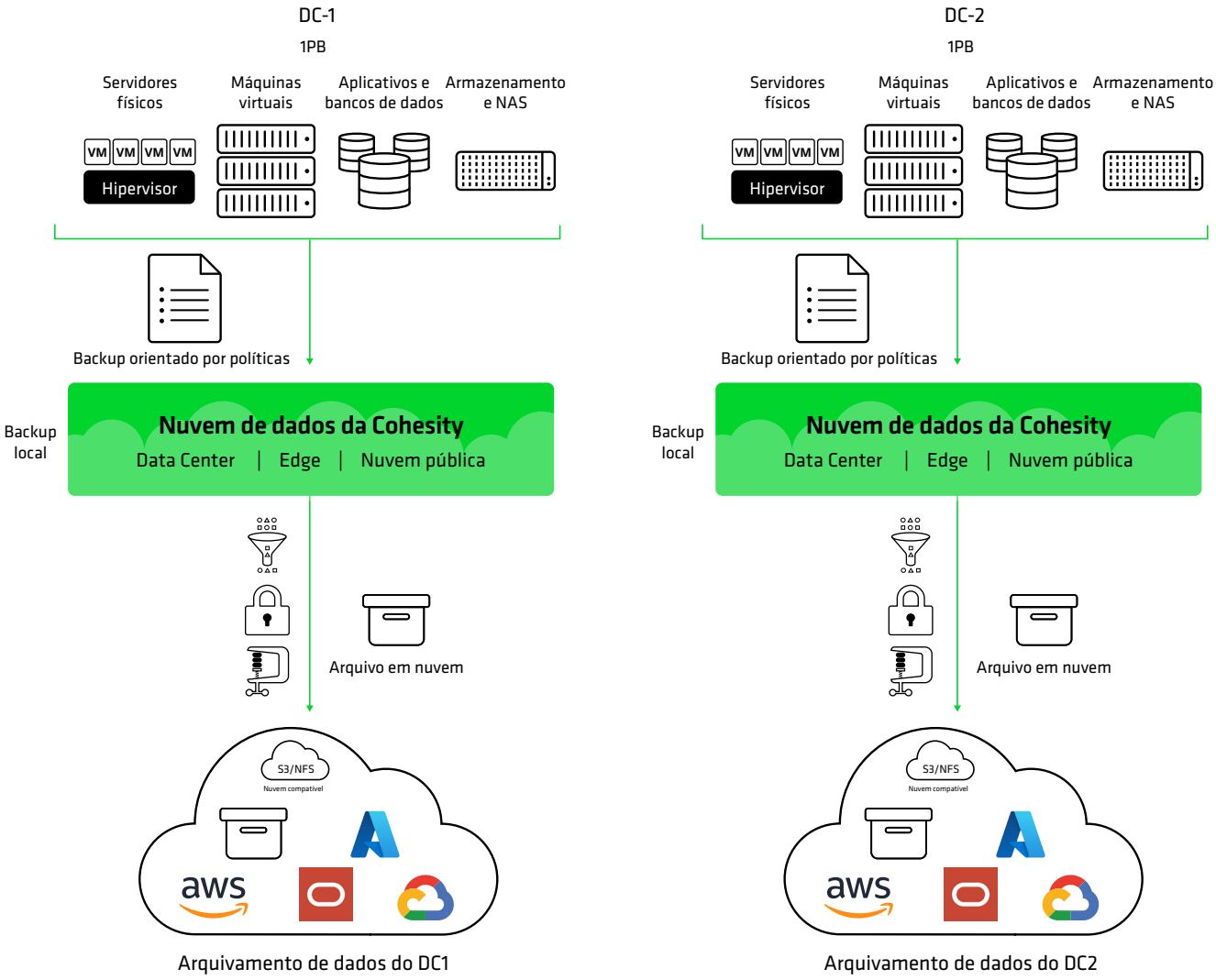
Diversos tipos e topologias são adequados a uma abordagem ativo-ativo. Uma abordagem Ativo-Ativo equivale efetivamente a duas de um único tipo de topologia, espelhadas e consecutivas. Nesta topologia, temos um par de data centers de modelo Ativo-Ativo, cada um com seu próprio backup. Qualquer um dos data centers pode assumir as operações do outro em caso de indisponibilidade. Cada data center também tem um backup completo de seus dados e cargas de trabalho. Para clientes com uma grande quantidade de largura de banda WAN disponível, até mesmo o backup pode ser geograficamente separado do data center para fornecer prevenção adicional em caso de desastres. Toda replicação de cargas de trabalho e dados ocorre na camada de carga de trabalho, portanto, essa topologia não requer replicação.

Básico: B2 – Backup e arquivamento



Neste caso, o backup é associado a um arquivamento com um período de retenção muito mais longo do que o do próprio backup O Cohesity FortKnox é uma escolha popular neste cenário, pois fornece segurança adicional para essa topologia. O FortKnox é um arquivo isolado e só é conectado quando está sendo realizada uma gravação no arquivo ou uma restauração a partir do arquivo. O arquivamento também pode ser realizado em uma nuvem privada local/remota ou em uma nuvem pública, como AWS, Google Cloud, Microsoft Azure, Oracle Cloud ou qualquer serviço em nuvem compatível com S3/NFS.

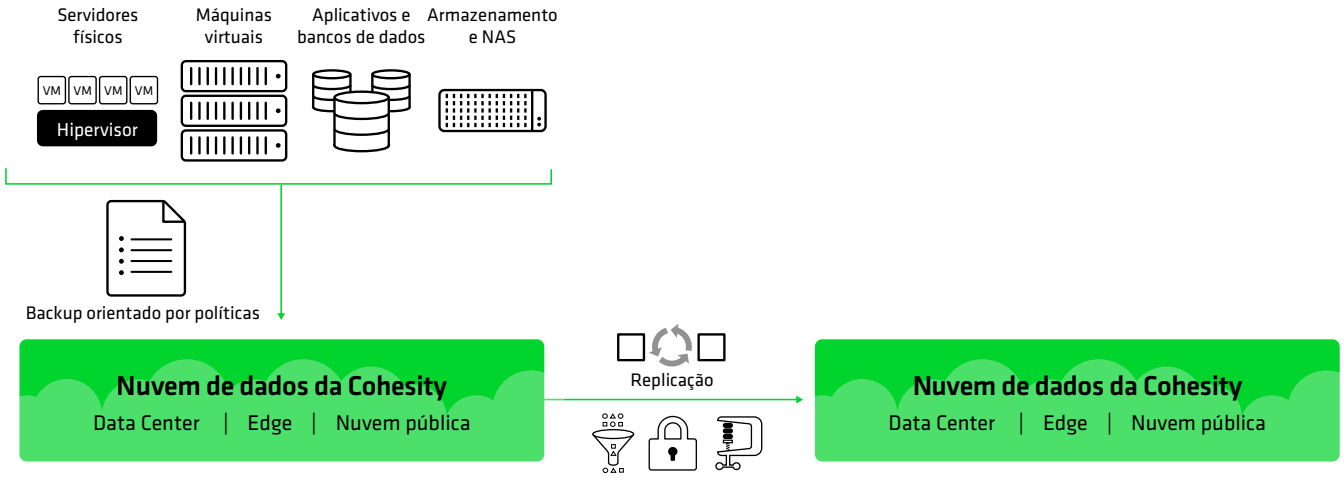
Básico: B2 – Backup e arquivamento (Ativo-Ativo)



Nesta topologia, temos um par de data centers de modelo Ativo-Ativo, cada um com seu próprio backup e arquivamento. Qualquer um dos data centers pode assumir as operações do outro em caso de indisponibilidade, e cada data center também tem um backup completo de seus dados e cargas de trabalho por meio do arquivamento.

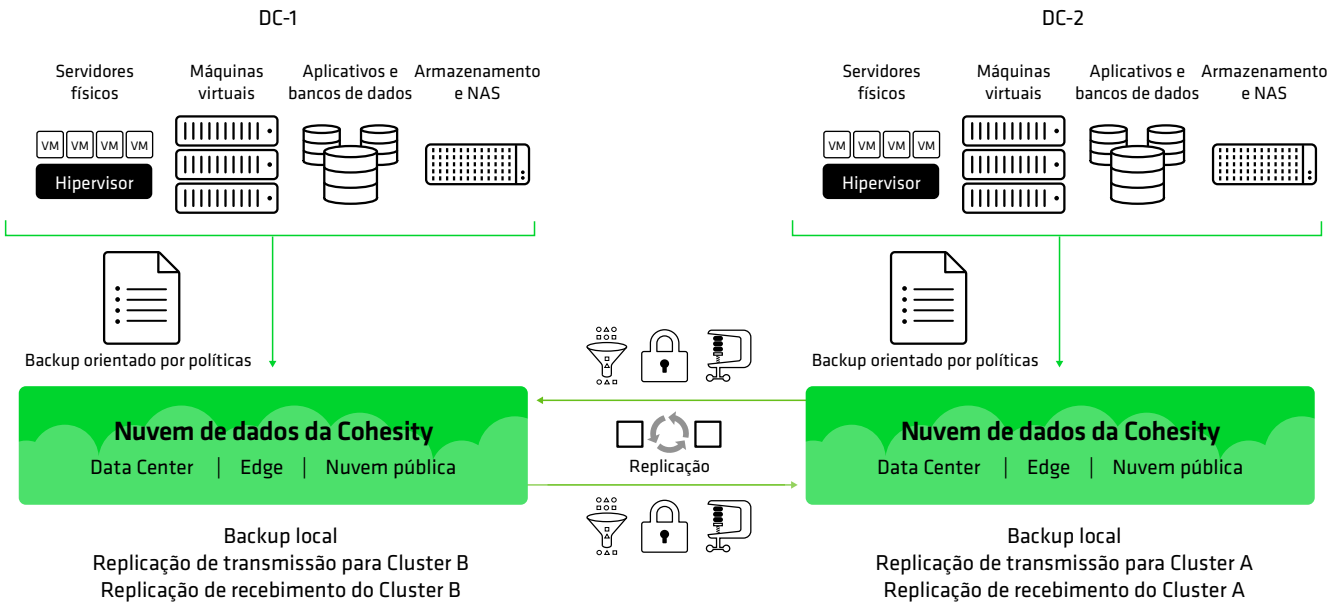
Toda replicação de cargas de trabalho e dados ocorre na camada de carga de trabalho, e é por isso que essa topologia não requer replicação. O FortKnox seria uma escolha útil para o arquivamento, considerando seu isolamento e segurança adicional.

Básico: B3 – Backup e replicação (recuperação de desastres)



Nesta topologia, o backup e a réplica mantêm equivalência temporal de retenção. A réplica é distribuída geograficamente e usada para recuperação de desastres. Para clientes com uma grande quantidade de largura de banda WAN disponível, até mesmo o backup pode ser geograficamente separado do data center para fornecer prevenção adicional em caso de desastres. O foco desta topologia é a continuidade dos negócios caso o backup não esteja disponível. As réplicas podem restaurar dados diretamente sem exigir o processo de duas etapas necessário quando um arquivo é usado.

Básico: B3 – Backup e replicação cruzada (ativo-ativo)



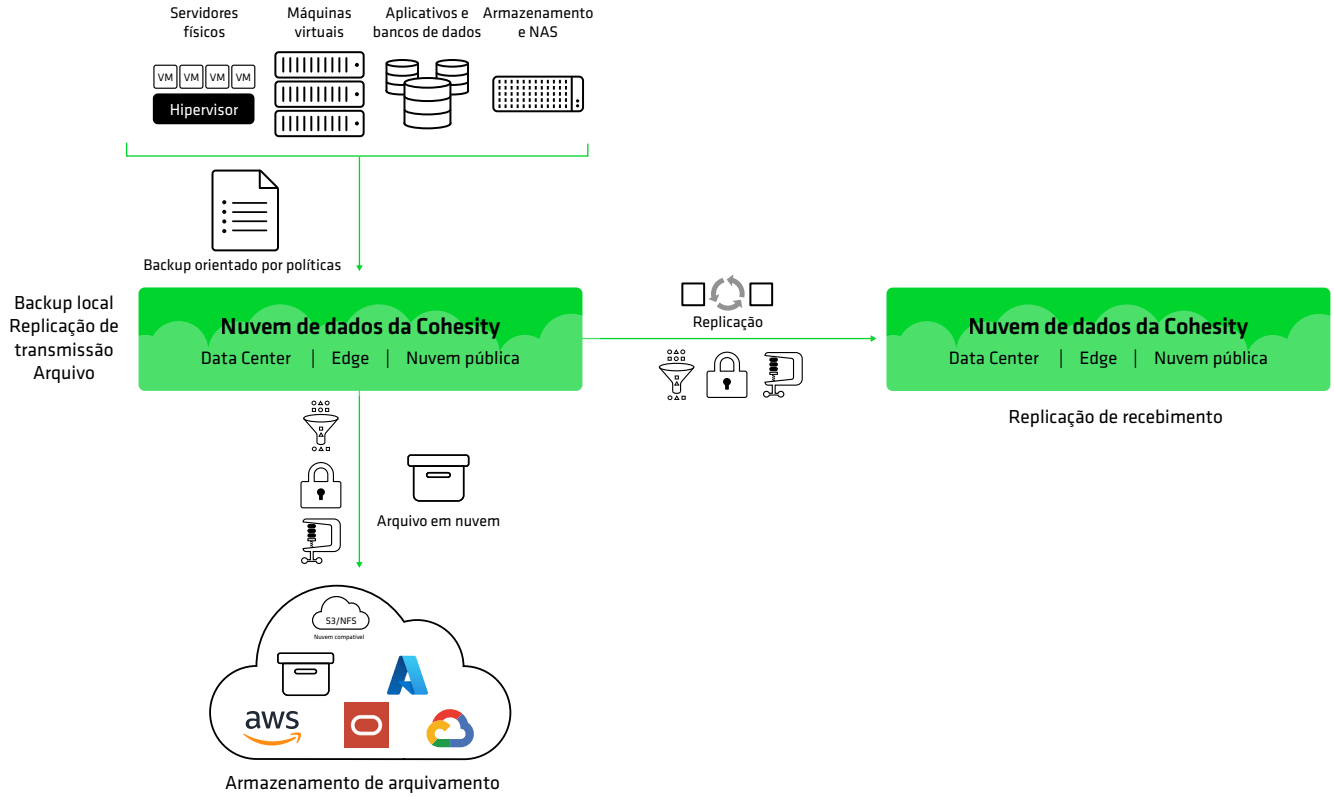
Nesse caso, os clusters de backup e replicação realizam replicação cruzada. O backup para o primeiro local é a réplica para o segundo local e vice-versa.

Topologias aprimoradas (incluindo adoção por setor)

Topologias aprimoradas são populares com dados de alto valor. Backup, replicação e arquivamento (E1) são os mais adotados, enquanto backup e replicação dupla (E2) são menos adotados. As topologias de uso comum estão marcadas abaixo, juntamente com os favoritos notáveis por setor.

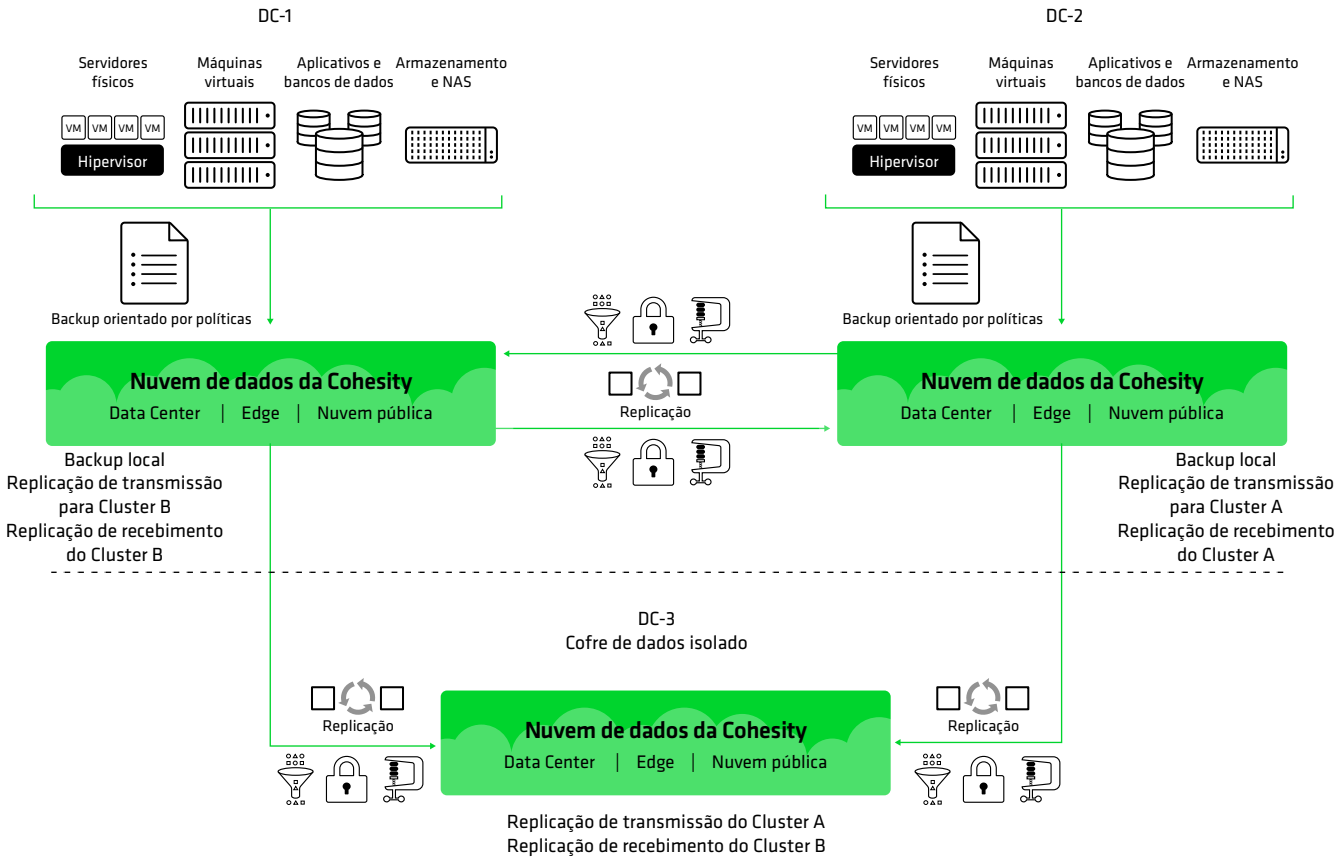
Topologia	Data Center Primário	Modelo Ativo-Ativo	Modelo Hub e Spoke
E1 – Backup, replicação, e arquivamento	✓ Todos os tipos	✓ Instituições Financeiras	
E2 – Backup e replicação dupla	✓ Órgãos governamentais	✓ Cadeias de varejo, alguns órgãos governamentais usando um modelo leste-oeste	

Aprimorado: E1 – Backup, replicação e arquivamento



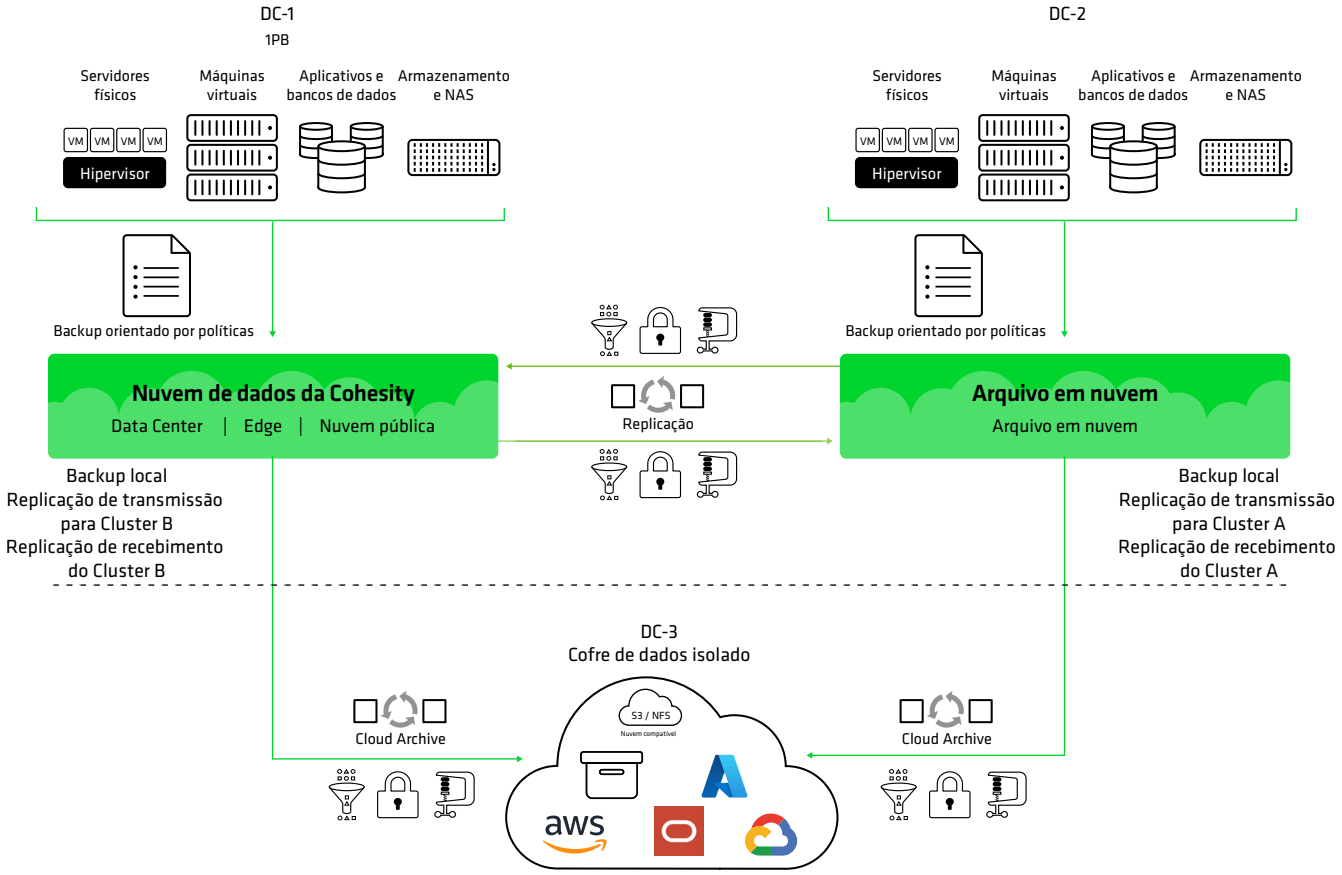
Backup e réplica mantêm uma equivalência temporal (por exemplo, duas vezes ao dia por 90 dias), enquanto o arquivamento pode cobrir meses ou até anos. A recuperação de um backup ou réplica é um processo de uma etapa, enquanto a recuperação do arquivo envolve duas etapas: uma leitura do arquivo e, em seguida, uma restauração dos dados. O arquivo pode ser em uma nuvem privada local/remota ou uma nuvem pública, como AWS, Google Cloud, Microsoft Azure, Oracle Cloud ou qualquer serviço em nuvem compatível com S3/NFS. O FortKnox também seria uma excelente escolha para essa topologia, considerando seu isolamento e segurança adicionais. Observe que com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário.

Aprimorado: E1 – Ativo-Ativo com um cofre de dados



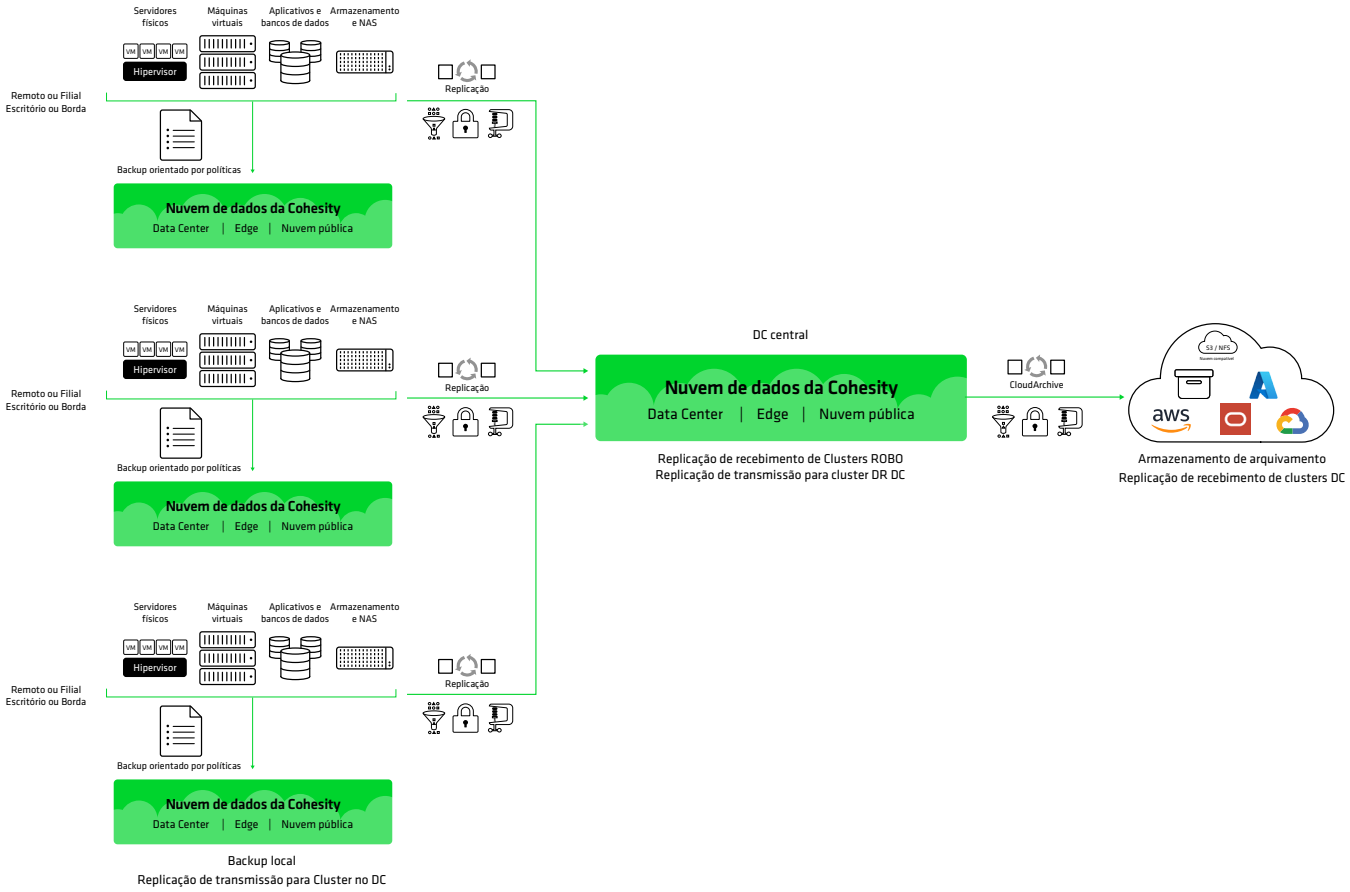
Essa topologia é outra abordagem **ativa-ativa**. Aqui, os data centers com replicação cruzada compartilham um único cofre de dados isolado. O isolamento é físico, com o cofre de dados desconectado da rede quando não está em uso. Observe que o cofre é uma réplica, permitindo uma recuperação de qualquer um dos data centers em uma única etapa a partir da réplica. Essa arquitetura também pode ser estendida, com vários pares com modelo ativo-ativo usando o mesmo cofre de dados.

Aprimorado: E1 – Ativo-Ativo com um arquivo isolado



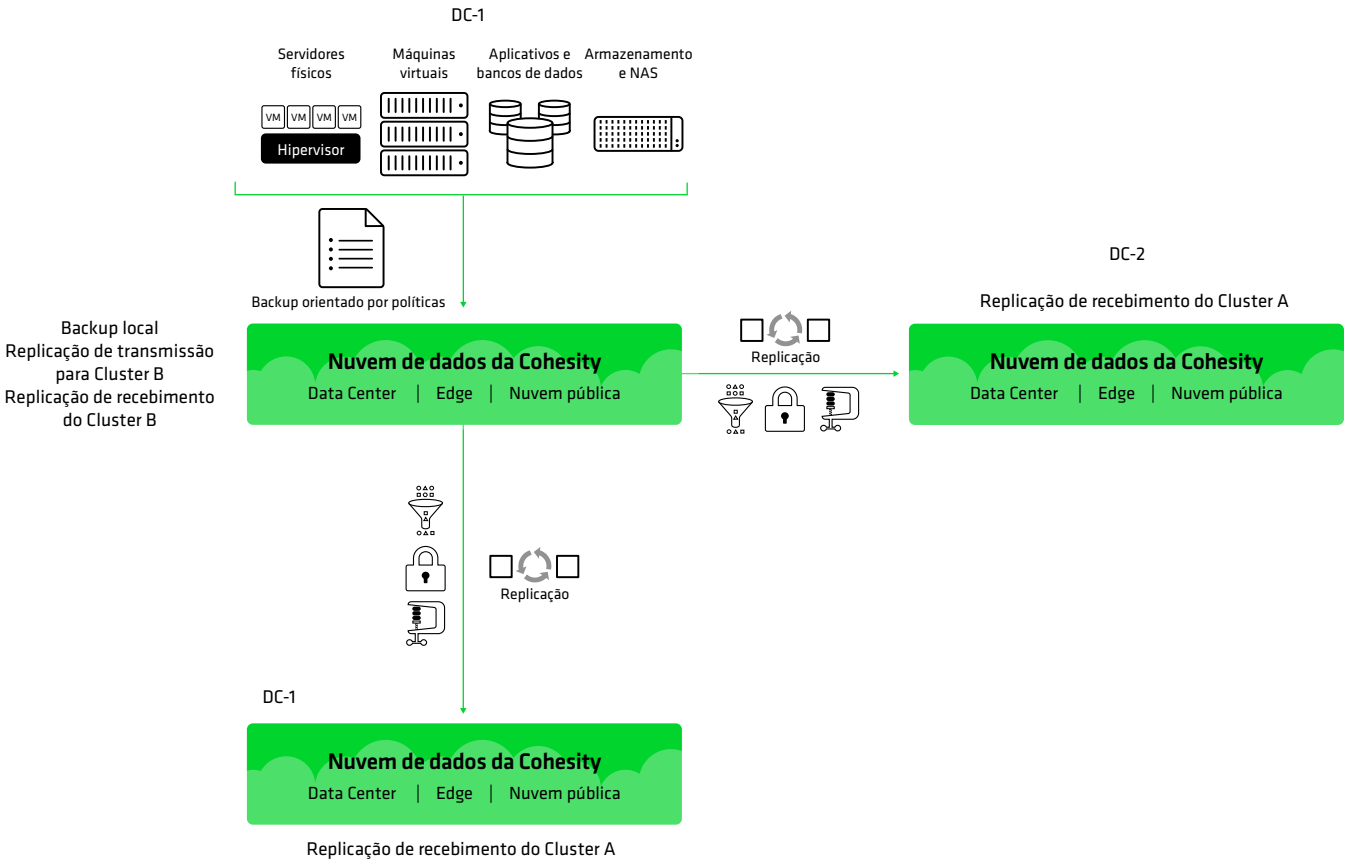
O gráfico acima é outra abordagem **ativo-ativo**. Nesse caso, os data centers com replicação cruzada compartilham um único arquivo isolado. Este caso de uso funcionaria bem com nossa abordagem de arquivamento FortKnox, considerando o isolamento e a segurança adicional que ele fornece. Essa arquitetura também pode ser estendida, com vários pares do modelo ativo-ativo usando o mesmo arquivo isolado. Com o Cohesity Data Cloud, um arquivo pode ser restaurado para qualquer um dos backups ou réplicas.

Aprimorado: E1 – Backup, replicação e arquivamento (Hub e Spoke)



Muitas topologias também podem ser estendidas para o modelo **hub e spoke**, que também é conhecido como topologia fan-in. No modelo hub e spoke, as filiais individuais têm seus próprios backups, e esses backups são replicados para uma única Cohesity Data Cloud integrada em um data center central. A partir do data center central, a réplica é arquivada por meio do FortKnox ou em outro arquivo privado ou público. O FortKnox seria uma ótima escolha neste cenário, pois oferece isolamento completo no caso de os backups e a réplica serem comprometidos. Com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário.

Aprimorado: E2 – Backup e replicação dupla



Essa topologia é para os casos em que o processo de restauração em duas etapas de um arquivo não fornece um objetivo de tempo de recuperação (RTO) suficientemente baixo. Todas as três cópias (o backup e as duas réplicas) podem ser usadas para restaurar os dados em um processo de uma etapa nesta configuração.

Aprimorado: E2 – Hub e Spoke com Hubs Ativo-Ativo

Essa topologia combina vários modelos diferentes. Cada filial remota faz seus próprios backups, e esses backups são replicados em um data center central. Esse data center central também tem um data center de recuperação de desastres como backup. Isso tudo é espelhado, com o data center principal à esquerda servindo como o local de recuperação de desastres para o data center à direita e vice-versa.

Missão crítica

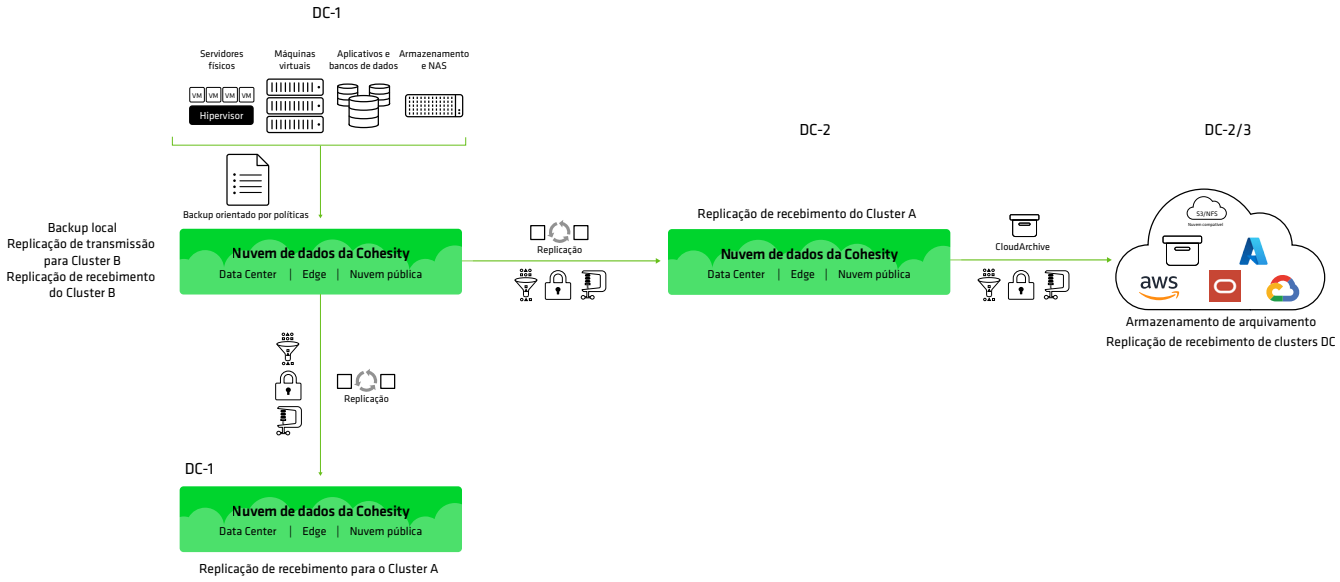
Topologia	Data center único	Modelo Ativo-Ativo	Modelo Hub e Spoke
Backup e réplica dupla com arquivamento	✓		✓
Backup, réplica e arquivamento duplo	✓	✓	
Backup, réplica dupla e arquivamento duplo		✓	

Missão crítica está surgindo como um tipo de topologia para os dados mais valiosos em uma determinada empresa. Estes são os dados necessários para a operação mínima viável da empresa (MVC).

Qual é a sua Empresa Mínima Viável?

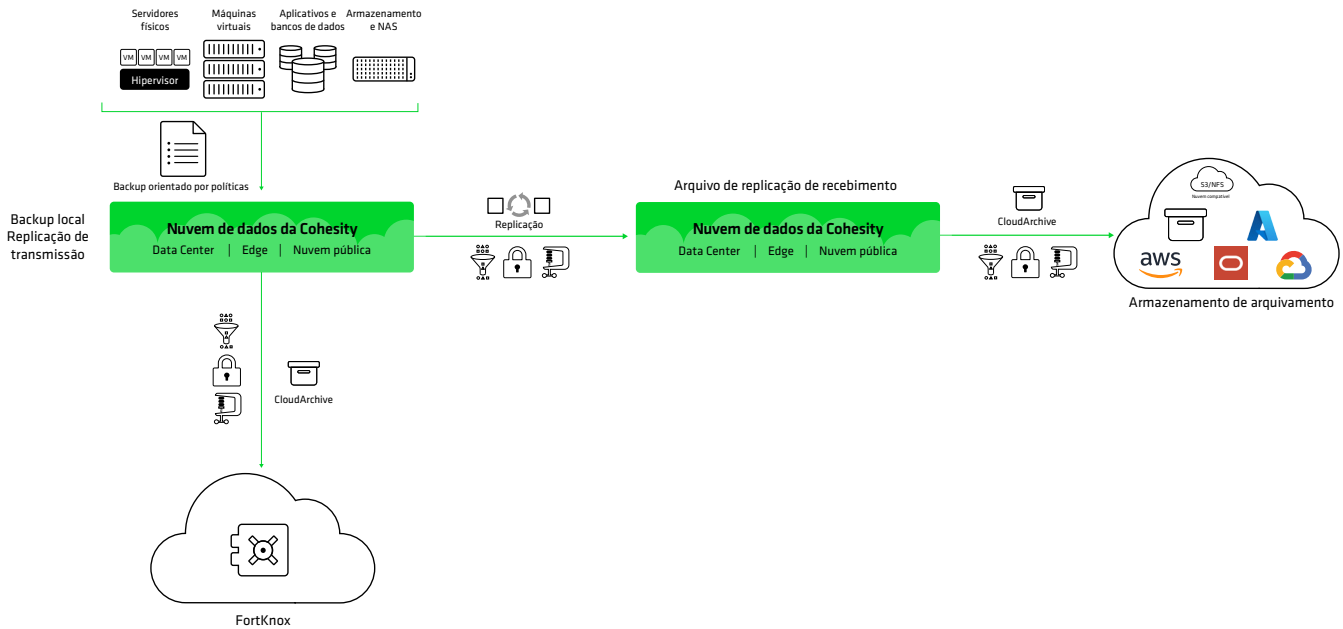
Uma MVC é o conjunto de aplicativos, infraestrutura e processos que precisam ser restaurados para que a empresa funcione em um nível minimamente viável. Esses sistemas devem ser colocados on-line primeiro; todos os outros sistemas são uma prioridade secundária. Os líderes de TI devem adotar o MVC ao planejar suas estratégias de resposta e recuperação de incidentes e sua topologia de dados.

Missão crítica: M1 – Backup e replicação dupla com arquivamento



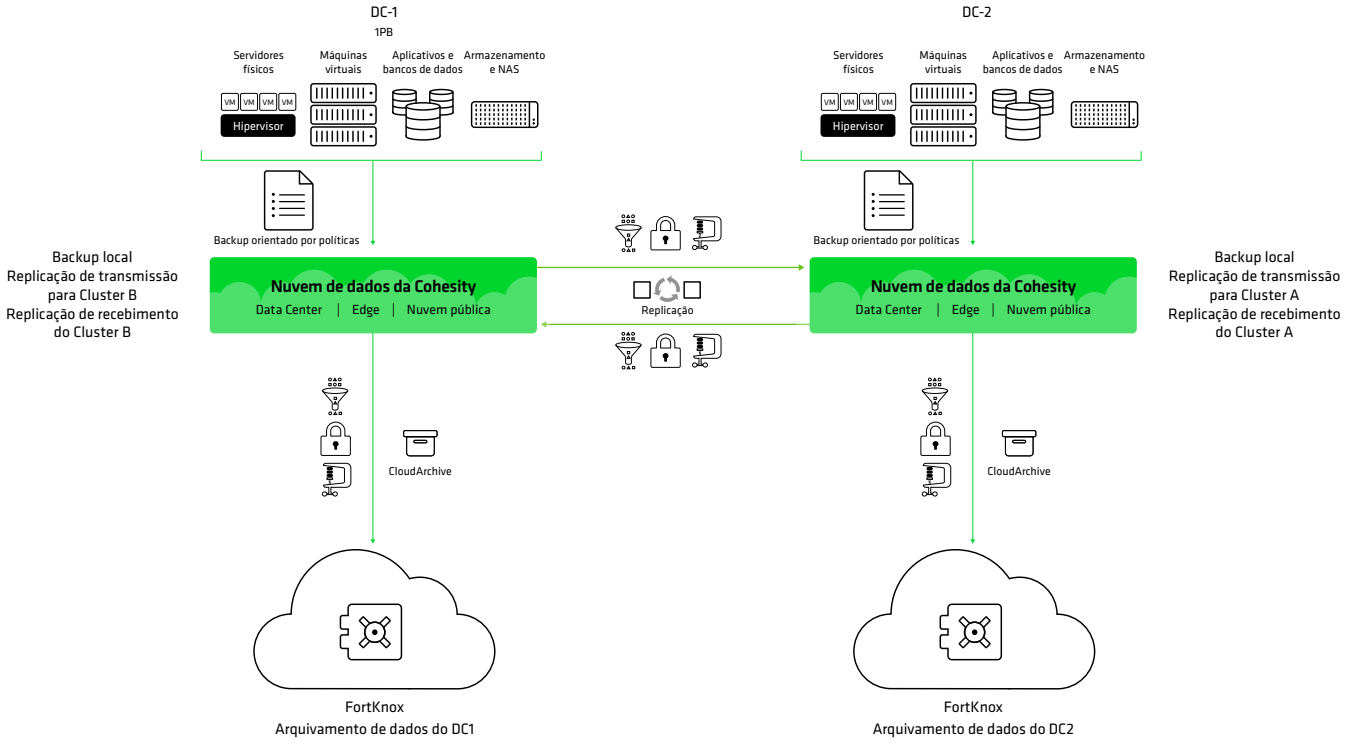
Essa arquitetura tolerante a falhas atende aos rigorosos requisitos de Objetivo de Tempo de Recuperação e Objetivo de Ponto de Recuperação e é associada a uma necessidade de retenção de longo prazo. A segunda réplica fornece recuperação de desastre adicional e proteção contra ransomware. Com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário. Adicionar uma air gap à segunda réplica aumenta a resiliência.

Missão crítica: M2 – Backup e replicação com arquivamento duplo usando FortKnox (a partir do backup local)



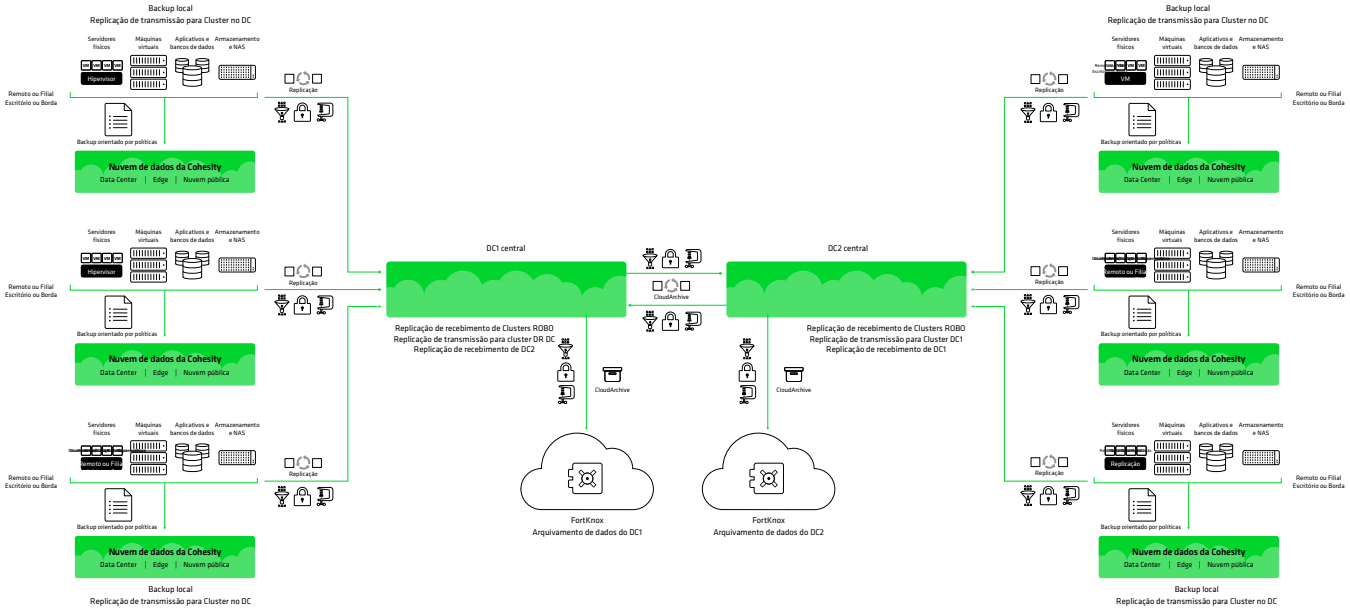
Essa arquitetura tolerante a falhas usa o FortKnox em vez de uma segunda réplica, pois o FortKnox fornece segurança e isolamento adicionais. O primeiro arquivo pode ser usado para atividades de conformidade, enquanto o arquivo FortKnox fornece resiliência contra ransomware adicional. Com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário.

Missão crítica: M2 – Replicação cruzada e arquivamento a partir do local com FortKnox



Este é o modelo **ativo-ativo** que vimos nas topologias **básicas,** com a adição de arquivos FortKnox duplos. Como cada cluster contém cópias de DC1 e DC2, cada instância FortKnox também contém cópias de DC1 e DC2. Com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário.

Missão crítica: M3 – Hub e Spoke com hubs ativo-ativo e arquivamento em FortKnox



Isso é semelhante ao que vimos nos tipos **aprimorados**, no entanto, nesse caso, cada uma das réplicas está conectada ao FortKnox como um arquivamento de longo prazo. Como as réplicas possuem cópias dos spokes esquerdo e direito, cada um dos arquivos FortKnox também contém ambos os conjuntos de cópias. Com o Cohesity Data Cloud, um arquivo pode ser restaurado por meio de um cluster primário ou secundário.

Conclusões e próximas etapas

Muitos líderes empresariais buscam fortalecer a proteção de seus dados críticos. Os modelos são essenciais para discutirmos novas abordagens com esses tomadores de decisão. Os projetos discutidos neste artigo técnico ajudarão os executivos a entender o que outros executivos fizeram em situações semelhantes com requisitos de proteção de dados semelhantes.

"Mais" nem sempre é melhor quando se trata de cópias de dados. Tanto a Cohesity quanto nossos clientes entendem que adicionar mais cópias de dados adiciona custos operacionais, de licenciamento e, muitas vezes, de hardware. Em alguns casos, não defendemos a adição de outra cópia, mas incentivamos o uso de diferentes tipos de cópias.

Com frequência, recomendamos o uso de arquivos para atividades de conformidade da empresa e para promover a resiliência cibernética. Portanto, nossos clientes geralmente optam por manter o mesmo número de cópias de dados, mas alteram o tipo das cópias que usam. Elas podem, por exemplo, substituir um arquivamento no local e não seguro por um arquivamento isolado, como o FortKnox, para fornecer cópias que possam ser usadas para fins de conformidade e resiliência contra ransomware.

Os modelos são poderosos porque permitem que você revise todas as opções relevantes e comprovadas e tome uma decisão informada sobre quais dessas opções usará em sua implantação.

O gráfico abaixo fornece uma visão simplificada e agregada do benefício de cada topologia no que se refere a domínios de falha, eventos de força maior e proteção cibernética.

Tipo	**Básico**		**Aprimorado**	**Missão Crítica**	
Cópias	**1**	**2**	**3**	**4**	**5**
Topologia	**Somente backup**	**Backup e repositório** (Réplica ou arquivamento)	**Backup e repositório duplo** (Réplica e arquivamento, ou réplica dupla)	**Backup, réplica dupla e arquivamento**	**Backup, réplica dupla e arquivamento duplo**
Proteção contra domínios de falha de HW e SW	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Proteção contra "Eventos de Força Maior"		★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★
Proteção cibernética	★	★ ★	★ ★ ★	★ ★ ★ ★	★ ★ ★ ★

A jornada para a segurança e o gerenciamento de dados modernos pode parecer assustadora. Reunimos essas informações de projeto para facilitar e ajudar a acelerar a rapidez com que você pode alcançar melhores resultados de negócios, reduzindo riscos e custos.

A partir daqui, recomendamos estas próximas etapas:

1. Determine quais planos são mais relevantes para a sua situação.
2. Avalie o Retorno sobre Investimento (ROI) e o Custo Total de Propriedade (TCO) de uma plataforma de dados moderna com relação à sua solução atual. Os principais pontos de comparação devem ser:
    a. Eficiência da proteção de dados
    b. Eficiência operacional
    c. Risco e conformidade
3. Selecione sua solução com base em demonstrações de produtos, cálculos comprovados de ROI e TCO e suporte às prioridades do planejamento.
4. Implemente a solução escolhida seguindo os modelos mais relevantes e prossiga para executar o planejamento a partir da etapa anterior.

Quando sua plataforma moderna estiver em vigor, gere um conjunto inicial de KPIs com relação à resiliência cibernética e meça regularmente seu progresso em relação a essa linha de base. A partir daí, você saberá quando avançar para a próxima fase da sua jornada.

Sobre a Cohesity

A Cohesity é líder em segurança de dados com tecnologia de inteligência artificial. Mais de 13.600 clientes corporativos, incluindo mais de 85 das empresas da Fortune 100 e quase 70% das empresas da Global 500, confiam na Cohesity para fortalecer sua resiliência e, ao mesmo tempo, fornecer insights de IA generativa em suas vastas quantidades de dados. Formadas a partir da combinação da Cohesity com o negócio de proteção de dados corporativos da Veritas, as soluções da empresa protegem os dados no local, na nuvem e na borda. Com o apoio da NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud e outros, a Cohesity tem sede em Santa Clara, Califórnia, e escritórios em todo o mundo. Para saber mais, siga a Cohesity no **LinkedIn**, no **X** e no **Facebook**.

Saiba mais sobre a Cohesity

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA,
Estados Unidos 95054

2000050-002 EN 4-2025