



Notas de lançamento

Astra Control Center

NetApp
August 11, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/astra-control-center-2310/release-notes/whats-new.html> on August 11, 2025. Always check docs.netapp.com for the latest.

Índice

Notas de lançamento	1
Novidades nesta versão do Astra Control Center	1
7 de novembro de 2023 (23.10.0)	1
31 de julho de 2023 (23.07.0)	2
18 de maio de 2023 (23.04.2)	2
25 de abril de 2023 (23.04.0)	3
22 de novembro de 2022 (22.11.0)	3
8 de setembro de 2022 (22.08.1)	3
10 de agosto de 2022 (22.08.0)	4
26 de abril de 2022 (22.04.0)	4
14 de dezembro de 2021 (21,12)	4
5 de agosto de 2021 (21,08)	5
Encontre mais informações	5
Problemas conhecidos	5
Backups e snapshots de aplicativos falharão se a <code>volumesnapshotclass</code> for adicionada após o gerenciamento de um cluster	6
O gerenciamento de um cluster com Astra Control Center falha quando o arquivo <code>kubeconfig</code> contém mais de um contexto	6
Um pod de monitoramento pode falhar em ambientes do Istio	6
As operações de gerenciamento de dados da aplicação falham com erro de serviço interno (500) quando o Astra Trident está off-line	7
As operações de restauração no local para as classes de storage de economia ONTAP nas falham	7
A restauração a partir de um backup ao usar a criptografia em trânsito Kerberos pode falhar	7
Os dados de backup permanecem no intervalo após a exclusão para buckets com política de retenção expirada	7
Encontre mais informações	8
Limitações conhecidas	8
O mesmo cluster não pode ser gerenciado por duas instâncias do Astra Control Center	8
O Astra Control Center não pode gerenciar dois clusters com nomes idênticos	9
Um usuário com restrições de namespace RBAC pode adicionar e desgerenciar um cluster	10
Um membro com restrições de namespace não pode acessar os aplicativos clonados ou restaurados até que o administrador adicione o namespace à restrição	10
Vários aplicativos em um único namespace não podem ser restaurados coletivamente para um namespace diferente	10
O Astra Control não é compatível com aplicações que usam várias classes de storage por namespace	10
O Astra Control não atribui automaticamente buckets padrão nas instâncias da nuvem	10
Clones de aplicativos instalados usando operadores pass-by-referência podem falhar	10
As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas	11
O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados	11
As aplicações implementadas com o Helm 2 não são suportadas	11
Os snapshots podem falhar no Kubernetes 1,25 ou em clusters posteriores com certas versões de	

controladora de snapshot	11
Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center	11
Limitações de usuário e grupo LDAP	12
Os buckets do S3 no Astra Control Center não relatam a capacidade disponível	12
O Astra Control Center não valida os detalhes inseridos para o servidor proxy	12
As conexões existentes com um pod Postgres causam falhas	12
A página atividade exibe até 100000 eventos	12
O SnapMirror não é compatível com aplicações que usam NVMe em TCP para back-ends de storage ..	12
Encontre mais informações	12

Notas de lançamento

Temos o prazer de anunciar a última versão do Astra Control Center.

- ["O que há nesta versão do Astra Control Center"](#)
- ["Problemas conhecidos"](#)
- ["Limitações conhecidas"](#)

Envie feedback sobre a documentação tornando-se um ["Colaborador do GitHub"](#) ou enviando um e-mail para NetApp.com.

Novidades nesta versão do Astra Control Center

Temos o prazer de anunciar a última versão do Astra Control Center.

7 de novembro de 2023 (23.10.0)

Novos recursos e suporte

- * Recursos de backup e restauração para aplicativos com backends de armazenamento com driver ONTAP-nas-Economy*: Ative operações de backup e restauração para `ontap-nas-economy` alguns ["passos simples"](#).
- * Backups imutáveis*: O Astra Control agora é compatível ["backups inalteráveis e somente leitura"](#) como uma camada de segurança adicional contra malware e outras ameaças.
- **Apresentamos o Astra Control Provisioner**

Com a versão 23,10, o Astra Control apresenta um novo componente de software chamado Astra Control Provisioner, que estará disponível para todos os usuários licenciados do Astra Control. O Astra Control Provisioner fornece acesso a um superconjunto de recursos avançados de gerenciamento e provisionamento de storage além daqueles fornecidos pelo Astra Trident. Esses recursos estão disponíveis para todos os clientes do Astra Control sem custo adicional.

- **Comece a usar o Astra Control Provisioner** você pode ["Habilite o Astra Control Provisioner"](#) se tiver instalado e configurado seu ambiente para usar o Astra Trident 23,10.
- **Funcionalidade do Astra Control Provisioner**

Os seguintes recursos estão disponíveis com o lançamento do Astra Control Provisioner 23,10:

- * Segurança de back-end de armazenamento aprimorada com criptografia Kerberos 5*: Você pode melhorar a segurança de armazenamento ["ativação da encriptação"](#) para o tráfego entre o cluster gerenciado e o back-end de armazenamento. O Astra Control Provisioner oferece suporte à criptografia Kerberos 5 em mais de NFSv4,1 conexões de clusters Red Hat OpenShift para volumes Azure NetApp Files e ONTAP locais
- **Recuperar dados usando um snapshot**: O Astra Control Provisioner fornece restauração rápida de volume no local a partir de um snapshot usando o `TridentActionSnapshotRestore` (TASR) CR.
- **Melhorias do SnapMirror**: Use o recurso de replicação de aplicativos em ambientes em que o Astra Control não tenha conectividade direta com um cluster ONTAP ou acesso às credenciais do ONTAP. Esse recurso permite que você use a replicação sem precisar gerenciar um back-end de storage ou suas credenciais no Astra Control.

- **Recursos de backup e restauração para aplicativos com ontap-nas-economy backends de armazenamento com backup de driver:** Como descrito [acima](#).

- **Suporte ao gerenciamento de aplicações que usam storage NVMe/TCP** o Astra Control agora pode gerenciar aplicações com suporte de volumes persistentes conectados por meio de NVMe/TCP.
- **Ganchos de execução desativados por padrão:** Começando com esta versão, a funcionalidade de ganchos de execução pode ser "[ativado](#)" ou desativada para segurança adicional (ela está desativada por padrão). Se você ainda não criou ganchos de execução para uso com o Astra Control, você precisa "[ative o recurso ganchos de execução](#)" começar a criar ganchos. Se você criou ganchos de execução antes desta versão, a funcionalidade ganchos de execução permanece ativada e você pode usar ganchos como faria normalmente.

Problemas e limitações conhecidos

- "[Problemas conhecidos para esta versão](#)"
- "[Limitações conhecidas para esta versão](#)"

31 de julho de 2023 (23.07.0)

Detalhes

Novos recursos e suporte

- "[Suporte para o uso do NetApp MetroCluster em uma configuração elástica como um back-end de storage](#)"
- "[Suporte para usar Longhorn como um back-end de armazenamento](#)"
- "[Agora, as aplicações podem ser replicadas entre os back-ends do ONTAP a partir do mesmo cluster do Kubernetes](#)"
- "[O Astra Control Center agora suporta 'userPrincipalName' como um atributo de login alternativo para usuários remotos \(LDAP\)](#)"
- "[O novo tipo de gancho de execução 'pós-failover' pode ser executado após failover de replicação com o Astra Control Center](#)"
- Os workflows do clone agora são compatíveis apenas com clones ativos (o estado atual da aplicação gerenciada). Para clonar de um snapshot ou backup, use o "[restaure o fluxo de trabalho](#)".

Problemas e limitações conhecidos

- "[Problemas conhecidos para esta versão](#)"
- "[Limitações conhecidas para esta versão](#)"

18 de maio de 2023 (23.04.2)

Detalhes

Esta versão de patch (23.04.2) para Astra Control Center (23.04.0) fornece suporte "[Snapshotter externo do Kubernetes v6,1.0](#)" e corrige o seguinte:

- Um bug com restauração de aplicativos no local ao usar ganchos de execução
- Problemas de conexão com o serviço do balde

25 de abril de 2023 (23.04.0)

Detalhes

Novos recursos e suporte

- ["Licença de avaliação de 90 dias habilitada por padrão para novas instalações do Astra Control Center"](#)
- ["Funcionalidade aprimorada de ganchos de execução com opções de filtragem adicionais"](#)
- ["Agora, os ganchos de execução podem ser executados após failover de replicação com o Astra Control Center"](#)
- ["Suporte para migrar volumes da classe 'ONTAP-nas-economy storage' para a classe de armazenamento 'ONTAP-nas'"](#)
- ["Suporte para incluir ou excluir recursos de aplicativos durante operações de restauração"](#)
- ["Suporte para gerenciamento de aplicações somente de dados"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

22 de novembro de 2022 (22.11.0)

Detalhes

Novos recursos e suporte

- ["Suporte para aplicações que abrangem vários namespaces"](#)
- ["Suporte para incluir recursos de cluster em uma definição de aplicativo"](#)
- ["Autenticação LDAP aprimorada com integração com controle de acesso baseado em função \(RBAC\)"](#)
- ["Adicionado suporte para Kubernetes 1,25 e admissão de segurança de Pod \(PSA\)"](#)
- ["Relatórios de progresso aprimorados para suas operações de backup, restauração e clone"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

8 de setembro de 2022 (22.08.1)

Detalhes

Esta versão de patch (22.08.1) para o Centro de Controle Astra (22.08.0) corrige pequenos bugs na replicação de aplicativos usando o NetApp SnapMirror.

10 de agosto de 2022 (22.08.0)

Detalhes

Novos recursos e suporte

- ["Replicação de aplicativos usando a tecnologia NetApp SnapMirror"](#)
- ["Fluxo de trabalho de gerenciamento de aplicativos aprimorado"](#)
- ["Funcionalidade aprimorada de ganchos de execução provide-your-own"](#)



O NetApp forneceu ganchos de execução pré e pós-snapshot padrão para aplicativos específicos foram removidos nesta versão. Se você atualizar para esta versão e não fornecer seus próprios ganchos de execução para snapshots, o Astra Control tirará somente snapshots consistentes com falhas. Visite o ["NetApp Verda"](#) repositório do GitHub para scripts de gancho de execução de exemplo que você pode modificar para se adequar ao seu ambiente.

- ["Suporte para o VMware Tanzu Kubernetes Grid Integrated Edition \(TKGI\)"](#)
- ["Suporte para Google Anthos"](#)
- ["Configuração LDAP \(via API Astra Control\)"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

26 de abril de 2022 (22.04.0)

Detalhes

Novos recursos e suporte

- ["Controles de acesso baseados em função do namespace \(RBAC\)"](#)
- ["Suporte para Cloud Volumes ONTAP"](#)
- ["Capacitação genérica de ingresso para Astra Control Center"](#)
- ["Remoção do balde do Astra Control"](#)
- ["Suporte ao portfólio VMware Tanzu"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

14 de dezembro de 2021 (21,12)

Detalhes

Novos recursos e suporte

- ["Restauração de aplicativo"](#)
- ["Ganchos de execução"](#)
- ["Suporte para aplicativos implantados com operadores com escopo de namespace"](#)
- ["Suporte adicional para Kubernetes e Rancher upstream"](#)
- ["Atualizações do Astra Control Center"](#)
- ["Opção Red Hat OperatorHub para instalação"](#)

Problemas resolvidos

- ["Problemas resolvidos para esta versão"](#)

Problemas e limitações conhecidos

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)

5 de agosto de 2021 (21,08)

Detalhes

Lançamento inicial do Astra Control Center.

- ["O que é"](#)
- ["Compreender a arquitetura e os componentes"](#)
- ["O que é preciso para começar"](#)
- ["Instale" e "configuração"](#)
- ["Gerenciar" e "proteger" aplicações](#)
- ["Gerenciar buckets" e "back-ends de armazenamento"](#)
- ["Gerenciar contas"](#)
- ["Automatize com API"](#)

Encontre mais informações

- ["Problemas conhecidos para esta versão"](#)
- ["Limitações conhecidas para esta versão"](#)
- ["Versões anteriores da documentação do Astra Control Center"](#)

Problemas conhecidos

Problemas conhecidos identificam problemas que podem impedi-lo de usar esta versão do produto com sucesso.

Os seguintes problemas conhecidos afetam a versão atual:

- Backups e snapshots de aplicativos falharão se a `volumesnapshotclass` for adicionada após o gerenciamento de um cluster
- O gerenciamento de um cluster com Astra Control Center falha quando o arquivo `kubeconfig` contém mais de um contexto
- Um pod de monitoramento pode falhar em ambientes do Istio
- As operações de gerenciamento de dados da aplicação falham com erro de serviço interno (500) quando o Astra Trident está off-line
- As operações de restauração no local para as classes de storage de economia ONTAP nas falham
- A restauração a partir de um backup ao usar a criptografia em trânsito Kerberos pode falhar
- Os dados de backup permanecem no intervalo após a exclusão para buckets com política de retenção expirada

Backups e snapshots de aplicativos falharão se a `volumesnapshotclass` for adicionada após o gerenciamento de um cluster

Backups e snapshots falham UI 500 error nesse cenário. Como solução alternativa, atualize a lista de aplicativos.

O gerenciamento de um cluster com Astra Control Center falha quando o arquivo `kubeconfig` contém mais de um contexto

Você não pode usar um `kubeconfig` com mais de um cluster e contexto nele. Consulte ["artigo da base de conhecimento"](#) para obter mais informações.

Um pod de monitoramento pode falhar em ambientes do Istio

Se você emparelhar o Astra Control Center com o Cloud Insights em um ambiente Istio, o `telegraf-rs` pod poderá falhar. Como solução alternativa, execute as seguintes etapas:

1. Encontre o pod avariado:

```
kubectl -n netapp-monitoring get pod | grep Error
```

Você deve ver saída semelhante ao seguinte:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-fhhrh 1/2 Error 2 (26s ago) 32s
```

2. Reinicie o pod avariado, substituindo `<pod_name_from_output>` pelo nome do pod afetado:

```
kubectl -n netapp-monitoring delete pod <pod_name_from_output>
```

Você deve ver saída semelhante ao seguinte:

```
pod "telegraf-rs-fhhrh" deleted
```

3. Verifique se o pod foi reiniciado e não está em um estado de erro:

```
kubectl -n netapp-monitoring get pod
```

Você deve ver saída semelhante ao seguinte:

```
NAME READY STATUS RESTARTS AGE
telegraf-rs-rrnsb 2/2 Running 0 11s
```

As operações de gerenciamento de dados da aplicação falham com erro de serviço interno (500) quando o Astra Trident está off-line

Se o Astra Trident em um cluster de aplicações ficar offline (e for colocado novamente online) e se forem encontrados 500 erros de serviço interno ao tentar o gerenciamento de dados de aplicações, reinicie todos os nós do Kubernetes no cluster de aplicações para restaurar a funcionalidade.

As operações de restauração no local para as classes de storage de economia ONTAP nas falham

Se você executar uma restauração no local de um aplicativo (restaurar o aplicativo para seu namespace original) e a classe de armazenamento do aplicativo usar o `ontap-nas-economy` driver, a operação de restauração poderá falhar se o diretório instantâneo não estiver oculto. Antes de restaurar no local, siga as instruções em ["Habilite o backup e a restauração de operações de economia de ONTAP nas"](#) para ocultar o diretório de instantâneos.

A restauração a partir de um backup ao usar a criptografia em trânsito Kerberos pode falhar

Quando você restaura um aplicativo de um backup para um back-end de armazenamento que esteja usando a criptografia em trânsito Kerberos, a operação de restauração pode falhar. Esse problema não afeta a restauração de um snapshot ou a replicação dos dados do aplicativo usando o NetApp SnapMirror.



Ao usar a criptografia em trânsito Kerberos com volumes NFSv4, verifique se os volumes NFSv4 estão usando as configurações corretas. Consulte a seção Configuração de domínio do NetApp NFSv4 (página 13) do ["Guia de práticas recomendadas e aprimoramentos do NetApp NFSv4"](#).

Os dados de backup permanecem no intervalo após a exclusão para buckets com política de retenção expirada

Se você excluir o backup imutável de um aplicativo após a política de retenção do bucket expirar, o backup será excluído do Astra Control, mas não do bucket. Esse problema será corrigido em um lançamento futuro.

Encontre mais informações

- ["Limitações conhecidas"](#)

Limitações conhecidas

As limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportadas por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações com cuidado.

Limitações do gerenciamento de clusters

- [O mesmo cluster não pode ser gerenciado por duas instâncias do Astra Control Center](#)
- [O Astra Control Center não pode gerenciar dois clusters com nomes idênticos](#)

Limitações de controle de acesso baseado em função (RBAC)

- [Um usuário com restrições de namespace RBAC pode adicionar e desgerenciar um cluster](#)
- [Um membro com restrições de namespace não pode acessar os aplicativos clonados ou restaurados até que o administrador adicione o namespace à restrição](#)

Limitações de gerenciamento de aplicativos

- [Vários aplicativos em um único namespace não podem ser restaurados coletivamente para um namespace diferente](#)
- [O Astra Control não é compatível com aplicações que usam várias classes de storage por namespace](#)
- [O Astra Control não atribui automaticamente buckets padrão nas instâncias da nuvem](#)
- [Clones de aplicativos instalados usando operadores pass-by-referência podem falhar](#)
- [As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas](#)
- [O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados](#)
- [As aplicações implementadas com o Helm 2 não são suportadas](#)
- [25 ou em clusters posteriores com certas versões de controladora de snapshot](#)
- [Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center](#)

Limitações gerais

- [Limitações de usuário e grupo LDAP](#)
- [Os buckets do S3 no Astra Control Center não relatam a capacidade disponível](#)
- [O Astra Control Center não valida os detalhes inseridos para o servidor proxy](#)
- [As conexões existentes com um pod Postgres causam falhas](#)
- [A página atividade exibe até 100000 eventos](#)
- [O SnapMirror não é compatível com aplicações que usam NVMe em TCP para back-ends de storage](#)

O mesmo cluster não pode ser gerenciado por duas instâncias do Astra Control Center

Se você quiser gerenciar um cluster em outra instância do Astra Control Center, primeiro você deve ["desgerenciar o cluster"](#) usar a instância na qual ele é gerenciado antes de gerenciá-lo em outra instância.

Depois de remover o cluster do gerenciamento, verifique se o cluster não é gerenciado executando este comando:

```
oc get pods -n netapp-monitoring
```

Não deve haver pods em execução nesse namespace ou o namespace não deve existir. Se qualquer um deles for verdadeiro, o cluster não será gerenciado.

O Astra Control Center não pode gerenciar dois clusters com nomes idênticos

Se você tentar adicionar um cluster com o mesmo nome de um cluster que já existe, a operação falhará. Esse problema ocorre na maioria das vezes em um ambiente padrão do Kubernetes se você não tiver alterado o nome padrão do cluster nos arquivos de configuração do Kubernetes.

Como solução alternativa, faça o seguinte:

1. Edite seu kubeadm-config ConfigMap:

```
kubectl edit configmaps -n kube-system kubeadm-config
```

2. Altere o `clusterName` valor do campo `kubernetes` de (o nome padrão do Kubernetes) para um nome personalizado exclusivo.
3. Editar `kubeconfig` (`.kube/config`).
4. Atualizar nome do cluster de `kubernetes` para um nome personalizado exclusivo (`xyz-cluster` é usado nos exemplos abaixo). Faça a atualização em ambas as seções e contextos, conforme mostrado neste exemplo:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcJZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
    name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
    name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

Um usuário com restrições de namespace RBAC pode adicionar e desgerenciar um cluster

Um usuário com restrições de namespace RBAC não deve ter permissão para adicionar ou desgerenciar clusters. Devido a uma limitação atual, o Astra não impede que tais usuários desgerenciem clusters.

Um membro com restrições de namespace não pode acessar os aplicativos clonados ou restaurados até que o administrador adicione o namespace à restrição

Qualquer `member` usuário com restrições RBAC por nome/ID de namespace pode clonar ou restaurar um aplicativo para um novo namespace no mesmo cluster ou para qualquer outro cluster na conta da organização. No entanto, o mesmo usuário não pode acessar o aplicativo clonado ou restaurado no novo namespace. Após uma operação de clone ou restauração criar um novo namespace, o administrador/proprietário da conta pode editar a `member` conta de usuário e atualizar as restrições de função para o usuário afetado conceder acesso ao novo namespace.

Vários aplicativos em um único namespace não podem ser restaurados coletivamente para um namespace diferente

Se você gerenciar várias aplicações em um único namespace (criando várias definições de aplicações no Astra Control), não poderá restaurar todas as aplicações para um namespace único diferente. Você precisa restaurar cada aplicativo para seu próprio namespace separado.

O Astra Control não é compatível com aplicações que usam várias classes de storage por namespace

O Astra Control é compatível com aplicações que usam uma única classe de storage por namespace. Ao adicionar um aplicativo a um namespace, verifique se o aplicativo tem a mesma classe de armazenamento que outros aplicativos no namespace.

O Astra Control não atribui automaticamente buckets padrão nas instâncias da nuvem

O Astra Control não atribui automaticamente um bucket padrão a nenhuma instância de nuvem. Você precisa definir manualmente um intervalo padrão para uma instância de nuvem. Se um bucket padrão não estiver definido, você não poderá executar operações de clone de aplicativo entre dois clusters.

Clones de aplicativos instalados usando operadores pass-by-referência podem falhar

O Astra Control é compatível com aplicativos instalados com operadores com escopo de namespace. Esses operadores são geralmente projetados com uma arquitetura "pass-by-value" em vez de "pass-by-reference". A seguir estão alguns aplicativos de operador que seguem estes padrões:

- ["Apache K8ssandra"](#)



Para K8ssandra, são suportadas as operações de restauração no local. Uma operação de restauração para um novo namespace ou cluster requer que a instância original do aplicativo seja removida. Isto destina-se a garantir que as informações do grupo de pares transportadas não conduzam à comunicação entre instâncias. A clonagem da aplicação não é suportada.

- ["Jenkins CI"](#)
- ["Cluster Percona XtraDB"](#)

O Astra Control pode não ser capaz de clonar um operador projetado com uma arquitetura "pass-by-reference" (por exemplo, o operador CockroachDB). Durante esses tipos de operações de clonagem, o operador clonado tenta consultar os segredos do Kubernetes do operador de origem, apesar de ter seu próprio novo segredo como parte do processo de clonagem. A operação de clone pode falhar porque o Astra Control não conhece os segredos do Kubernetes no operador de origem.



Durante as operações de clone, os aplicativos que precisam de um recurso do IngressClass ou webhooks para funcionar corretamente não devem ter esses recursos já definidos no cluster de destino.

As operações de restauração no local de aplicativos que usam um gerenciador de certificados não são suportadas

Esta versão do Astra Control Center não oferece suporte à restauração local de aplicativos com gerentes de certificados. Operações de restauração para um namespace diferente e operações de clone são compatíveis.

O operador habilitado para OLM e com escopo de cluster implantaram aplicativos não suportados

O Astra Control Center não oferece suporte a atividades de gerenciamento de aplicações com operadores com escopo de cluster.

As aplicações implementadas com o Helm 2 não são suportadas

Se você usar o Helm para implantar aplicativos, o Astra Control Center precisará do Helm versão 3. O gerenciamento e clonagem de aplicativos implantados com o Helm 3 (ou atualizados do Helm 2 para o Helm 3) é totalmente compatível. Para obter mais informações, ["Requisitos do Astra Control Center"](#) consulte .

Os snapshots podem falhar no Kubernetes 1,25 ou em clusters posteriores com certas versões de controladora de snapshot

Os snapshots para clusters do Kubernetes que executam a versão 1,25 ou posterior podem falhar se a versão v1beta1 das APIs do controlador de snapshot estiver instalada no cluster.

Como solução alternativa, faça o seguinte ao atualizar instalações existentes do Kubernetes 1,25 ou posteriores:

1. Remova quaisquer CRDs de Snapshot existentes e qualquer controladora de snapshot existente.
2. ["Desinstale o Astra Trident"](#).
3. ["Instale as CRDs de snapshot e o controlador de snapshot"](#).
4. ["Instale a versão mais recente do Astra Trident"](#).
5. ["Crie um VolumeSnapshotClass"](#).

Backups e snapshots podem não ser retidos durante a remoção de uma instância do Astra Control Center

Se você tiver uma licença de avaliação, certifique-se de armazenar o ID da conta para evitar perda de dados

em caso de falha do Astra Control Center se você não estiver enviando ASUPs.

Limitações de usuário e grupo LDAP

O Astra Control Center é compatível com até 5.000 grupos remotos e 10.000 usuários remotos.

O Astra Control não suporta uma entidade LDAP (utilizador ou grupo) que tenha um DN contendo um RDN com um espaço de saída ou de saída.

Os buckets do S3 no Astra Control Center não relatam a capacidade disponível

Antes de fazer backup ou clonar aplicativos gerenciados pelo Astra Control Center, verifique as informações do bucket no sistema de gerenciamento ONTAP ou StorageGRID.

O Astra Control Center não valida os detalhes inseridos para o servidor proxy

Certifique-se de que você ["introduza os valores corretos"](#) ao estabelecer uma conexão.

As conexões existentes com um pod Postgres causam falhas

Quando você executa operações nos pods Postgres, você não deve se conectar diretamente dentro do pod para usar o comando psql. O Astra Control requer acesso psql para congelar e descongelar os bancos de dados. Se houver uma conexão pré-existente, o snapshot, o backup ou o clone falhará.

A página atividade exibe até 100000 eventos

A página atividade do Astra Control pode exibir até 100.000 eventos. Para ver todos os eventos registrados, recupere os eventos utilizando o ["API Astra Control"](#).

O SnapMirror não é compatível com aplicações que usam NVMe em TCP para back-ends de storage

O Astra Control Center não oferece suporte à replicação NetApp SnapMirror para back-ends de storage que usam o protocolo NVMe em TCP.

Encontre mais informações

- ["Problemas conhecidos"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.