Red Hat Enterprise Linux 8

Gerenciamento de Identidade de Planejamento

Documentação para planejamento Gerenciamento de Identidade e estabelecimento de controle de acesso

Last Updated: 2021-03-07

Red Hat Enterprise Linux 8 Gerenciamento de Identidade de Planejamento

Documentação para planejamento Gerenciamento de Identidade e estabelecimento de controle de acesso

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

Nota Legal

Resumo

Este documento descreve o planejamento dos serviços de Gerenciamento de Identidade no Red Hat Enterprise Linux 8. A versão atual do documento contém apenas histórias prévias selecionadas de usuários.

Índice

TORNANDO O CÓDIGO ABERTO MAIS INCLUSIVO

A Red Hat tem o compromisso de substituir a linguagem problemática em nosso código, documentação e propriedades da web. Estamos começando com estes quatro termos: master, slave, blacklist e whitelist. Por causa da enormidade deste esforço, estas mudanças serão implementadas gradualmente ao longo de vários lançamentos futuros. Para mais detalhes, veja a mensagem de nosso CTO Chris Wright.

FORNECENDO FEEDBACK SOBRE A DOCUMENTAÇÃO DA RED HAT

Agradecemos sua contribuição em nossa documentação. Por favor, diga-nos como podemos melhorá-la. Para fazer isso:

- Para comentários simples sobre passagens específicas:
  1. Certifique-se de que você está visualizando a documentação no formato *Multi-page HTML*. Além disso, certifique-se de ver o botão **Feedback** no canto superior direito do documento.
  2. Use o cursor do mouse para destacar a parte do texto que você deseja comentar.
  3. Clique no pop-up **Add Feedback** que aparece abaixo do texto destacado.
  4. Siga as instruções apresentadas.
- Para enviar comentários mais complexos, crie um bilhete Bugzilla:
  1. Ir para o site da Bugzilla.
  2. Como Componente, use **Documentation**.
  3. Preencha o campo **Description** com sua sugestão de melhoria. Inclua um link para a(s) parte(s) relevante(s) da documentação.
  4. Clique em **Submit Bug**.

CAPÍTULO 1. VISÃO GERAL DO PLANEJAMENTO PARA IDM E CONTROLE DE ACESSO NA RHEL

As seções seguintes fornecem uma visão geral das opções para gerenciamento de identidade (IdM) e controle de acesso no Red Hat Enterprise Linux. Após ler estas seções, você poderá se aproximar da etapa de planejamento de seu ambiente.

1.1. INTRODUÇÃO À IDM

Este módulo explica o propósito do Gerenciamento de Identidade (IdM) no Red Hat Enterprise Linux. Ele também fornece informações básicas sobre o domínio IdM, incluindo as máquinas clientes e servidores que fazem parte do domínio.

O objetivo do IdM no Red Hat Enterprise Linux

O IdM no Red Hat Enterprise Linux fornece uma forma centralizada e unificada de gerenciar lojas de identidade, autenticação, políticas e políticas de autorização em um domínio baseado no Linux. O IdM reduz significativamente a sobrecarga administrativa de gerenciar diferentes serviços individualmente e usar diferentes ferramentas em diferentes máquinas.

IdM é uma das poucas soluções centralizadas de software de identidade, política e autorização que suportam:

- Características avançadas dos ambientes do sistema operacional Linux
- Unificando grandes grupos de máquinas Linux
- Integração nativa com o Active Directory

IdM cria um domínio baseado em Linux e controlado por Linux:

- IdM se baseia em ferramentas e protocolos Linux existentes e nativos. Tem seus próprios processos e configurações, mas suas tecnologias subjacentes são bem estabelecidas em sistemas Linux e confiáveis pelos administradores Linux.
- Os servidores e clientes da IdM são máquinas Red Hat Enterprise Linux. Os clientes IdM também podem ser outras distribuições Linux e UNIX se eles suportarem protocolos padrão. O cliente Windows não pode ser um membro do domínio IdM mas o usuário logado em sistemas Windows gerenciados pelo Active Directory (AD) pode se conectar a clientes Linux ou acessar serviços gerenciados pelo IdM. Isto é conseguido através do estabelecimento de confiança florestal entre os domínios AD e IdM.

Gerenciando identidades e políticas em múltiplos servidores Linux

Without IdM: Cada servidor é administrado separadamente. Todas as senhas são salvas nas máquinas locais. O administrador de TI gerencia os usuários em cada máquina, define as políticas de autenticação e autorização separadamente e mantém as senhas locais. Entretanto, mais freqüentemente os usuários confiam em outra solução centralizada, por exemplo, integração direta com AD. Os sistemas podem ser integrados diretamente com o AD usando várias soluções diferentes:

- Ferramentas Legacy Linux (não é recomendado o uso)
- Solução baseada em Samba winbind (recomendada para casos específicos de uso)
- Solução baseada em um software de terceiros (geralmente requer uma licença de outro fornecedor)

- Solução baseada em SSSD (Linux nativo e recomendado para a maioria dos casos de uso)

With IdM: O administrador de TI pode:

- Manter as identidades em um lugar central: o servidor IdM
- Aplicar as políticas de maneira uniforme a múltiplos de máquinas ao mesmo tempo
- Estabelecer diferentes níveis de acesso para os usuários usando controle de acesso baseado em host, delegação, e outras regras
- Administrar de forma centralizada as regras de escalada de privilégios
- Definir como os diretórios residenciais são montados

SSO Empresarial

No caso da IdM Enterprise, o single sign-on (SSO) é implementado alavancando o protocolo Kerberos. Este protocolo é popular no nível de infra-estrutura e permite SSO com serviços como SSH, LDAP, NFS, CUPS, ou DNS. Serviços web que utilizam diferentes pilhas web (Apache, EAP, Django, e outros) também podem ser habilitados para usar o Kerberos para SSO. Entretanto, a prática mostra que o uso de OpenID Connect ou SAML baseado em SSO é mais conveniente para aplicações web. Para fazer a ponte entre as duas camadas, recomenda-se implantar uma solução Identity Provider (IdP) que seria capaz de converter a autenticação Kerberos em um bilhete OpenID Connect ou afirmação SAML. A tecnologia SSO da Red Hat baseada no projeto de código aberto Keycloak é um exemplo de tal IdP

Without IdM: Os usuários acessam o sistema e são solicitados a obter uma senha toda vez que acessam um serviço ou aplicativo. Estas senhas podem ser diferentes, e os usuários têm que lembrar qual credencial usar para qual aplicação.

With Idm: Após o login dos usuários no sistema, eles podem acessar vários serviços e aplicações sem serem repetidamente solicitados por suas credenciais. Isto ajuda a:

- Melhorar a usabilidade
- Reduzir o risco de segurança de senhas escritas ou armazenadas de forma insegura
- Aumentar a produtividade do usuário

Gerenciando um ambiente Linux e Windows misto

Without IdM: Os sistemas Windows são gerenciados em uma floresta AD, mas o desenvolvimento, produção e outras equipes têm muitos sistemas Linux. Os sistemas Linux são excluídos do ambiente AD.

With IdM: O administrador de TI pode:

- Gerenciar os sistemas Linux usando ferramentas nativas Linux
- Integrar os sistemas Linux nos ambientes gerenciados centralmente pelo Active Directory, preservando assim uma loja de usuários centralizada.
- Implantar facilmente novos sistemas Linux em escala ou conforme a necessidade.
- Reagir rapidamente às necessidades comerciais e tomar decisões relacionadas ao gerenciamento da infra-estrutura Linux sem depender de outras equipes, evitando atrasos.

Contrastando o IdM com um Diretório LDAP padrão

Um diretório LDAP padrão, como o Red Hat Directory Server, é um diretório de uso geral: ele pode ser personalizado para se adequar a uma ampla gama de casos de uso.

- Esquema: um esquema flexível que pode ser personalizado para uma vasta gama de entradas, tais como usuários, máquinas, entidades de rede, equipamentos físicos ou edifícios.
- Tipicamente utilizado como: um diretório back-end para armazenar dados para outras aplicações, tais como aplicações comerciais que fornecem serviços na Internet.

IdM tem um propósito específico: gerenciar as identidades internas, internas à empresa, bem como as políticas de autenticação e autorização que se relacionam com essas identidades.

- Esquema: um esquema específico que define um conjunto particular de entradas relevantes para sua finalidade, tais como entradas para identidades de usuários ou máquinas.
- Normalmente utilizado como: o servidor de identidade e autenticação para gerenciar identidades dentro dos limites de uma empresa ou de um projeto.

A tecnologia subjacente do servidor de diretório é a mesma tanto para o Red Hat Directory Server quanto para o IdM. Entretanto, o IdM é otimizado para gerenciar as identidades dentro da empresa. Isto limita sua extensibilidade geral, mas também traz certos benefícios: configuração mais simples, melhor automação do gerenciamento de recursos e maior eficiência no gerenciamento de identidades empresariais.

Recursos adicionais

- Gerenciamento de Identidade ou Red Hat Directory Server - Qual Devo Usar? no Blog do Red Hat Enterprise Linux.
- Artigo da Base de Conhecimento sobre protocolos padrão.
- Notas de Lançamento do Red Hat Enterprise Linux 8 Beta

1.2. INTRODUÇÃO AOS SERVIDORES E CLIENTES DA IDM

O domínio de Gerenciamento de Identidade (IdM) inclui os seguintes tipos de sistemas:

Servidores IdM

Os servidores IdM são sistemas Red Hat Enterprise Linux que respondem a pedidos de identidade, autenticação e autorização dentro de um domínio IdM. Na maioria das implementações, uma autoridade de certificação integrada (CA) também é instalada com o servidor IdM.
Os servidores IdM são os repositórios centrais para informações de identidade e políticas. Os servidores IdM também podem hospedar qualquer um dos serviços opcionais utilizados pelos membros do domínio:

- Autoridade Certificadora (CA)
- Autoridade de Recuperação Chave (KRA)
- DNS
- Controlador de confiança Active Directory (AD)
- Agente fiduciário do Active Directory (AD)

O primeiro servidor instalado para criar o domínio é o *IdM master* ou *master server*. O master IdM não deve ser confundido com o servidor *master CA*: eles podem funcionar em duas máquinas diferentes.

Clientes da IdM

Os clientes IdM são sistemas Red Hat Enterprise Linux inscritos nos servidores e configurados para usar os serviços IdM nestes servidores.
Os clientes interagem com os servidores da IdM para acessar os serviços por eles prestados. Por exemplo, os clientes utilizam o protocolo Kerberos para realizar a autenticação e adquirir bilhetes para o single sign-on empresarial (SSO), utilizar o LDAP para obter informações de identidade e políticas, utilizar o DNS para detectar onde os servidores e serviços estão localizados e como se conectar a eles.

Os servidores da IdM também são clientes da IdM embutidos. Como clientes inscritos com eles mesmos, os servidores oferecem a mesma funcionalidade que outros clientes.

Para fornecer serviços para um grande número de clientes, bem como para redundância e disponibilidade, a IdM permite a implantação em vários servidores IdM em um único domínio. É possível implantar até 60 servidores. Este é o número máximo de servidores IdM, também chamados de réplicas, que é atualmente suportado no domínio IdM. Os servidores IdM fornecem diferentes serviços para o cliente. Nem todos os servidores precisam fornecer todos os serviços possíveis. Alguns componentes de servidor como Kerberos e LDAP estão sempre disponíveis em todos os servidores. Outros serviços como CA, DNS, Trust Controller ou Vault são opcionais. Isto significa que servidores diferentes em geral desempenham papéis diferentes na implantação.

Se sua topologia IdM contém uma CA integrada, um servidor também tem o papel de mestre de geração da lista de revogação de certificados (CRL) e o mestre de renovação da CA . Este servidor é o *master CA*.

ATENÇÃO

O servidor *master CA* é crítico para sua implantação do IdM porque é o único sistema no domínio responsável pelo rastreamento de certificados e chaves do subsistema CA, e pela geração da CRL. Para detalhes sobre como se recuperar de um desastre que afete sua implantação de IdM, consulte Realizando a recuperação de desastres com Gerenciamento de Identidade.

Para redundância e equilíbrio de carga, os administradores criam servidores adicionais criando um *replica* de qualquer servidor existente, seja o servidor mestre ou outra réplica. Ao criar uma réplica, a IdM clona a configuração do servidor existente. Uma réplica compartilha com o servidor inicial sua configuração principal, incluindo informações internas sobre usuários, sistemas, certificados e políticas configuradas.

NOTA

Uma réplica e o servidor de onde ela foi criada são funcionalmente idênticos, exceto pelo papel do mestre da geração CRL. Portanto, os termos *server* e *replica* são utilizados de forma intercambiável aqui, dependendo do contexto.

1.3. IDM E CONTROLE DE ACESSO EM RHEL: CENTRAL VS. LOCAL

No Red Hat Enterprise Linux, você pode gerenciar identidades e políticas de controle de acesso usando ferramentas centralizadas para todo um domínio de sistemas, ou usando ferramentas locais para um único sistema.

Gerenciando identidades e políticas em múltiplos servidores Red Hat Enterprise Linux: Com e sem IdM

Com a Identity Management IdM, o administrador de TI pode:

- Manter as identidades e os mecanismos de agrupamento em um lugar central: o servidor IdM
- Gerenciar centralmente diferentes tipos de credenciais, como senhas, certificados PKI, tokens OTP ou chaves SSH
- Aplicar as políticas de maneira uniforme a múltiplos de máquinas ao mesmo tempo
- Gerenciar o POSIX e outros atributos para usuários externos do Active Directory
- Estabelecer diferentes níveis de acesso para os usuários usando controle de acesso baseado em host, delegação, e outras regras
- Gerenciar centralmente as regras de escalonamento de privilégios (sudo) e controle de acesso obrigatório (mapeamento de usuários SELinux)
- Manter a infra-estrutura central PKI e a loja de segredos
- Definir como os diretórios residenciais são montados

Sem IdM:

- Cada servidor é administrado separadamente.
- Todas as senhas são salvas nas máquinas locais.
- O administrador de TI gerencia os usuários em cada máquina, estabelece políticas de autenticação e autorização separadamente, e mantém senhas locais.

1.4. TERMINOLOGIA DA IDM

Active Directory floresta

Uma floresta Active Directory (AD) é um conjunto de uma ou mais árvores de domínio que compartilham um catálogo global comum, esquema de diretório, estrutura lógica e configuração de diretório. A floresta representa a fronteira de segurança dentro da qual usuários, computadores, grupos e outros objetos são acessíveis. Para mais informações, consulte o documento da Microsoft sobre Florestas.

Catálogo global do Active Directory

O catálogo global é uma característica do Active Directory (AD) que permite que um controlador de domínio forneça informações sobre qualquer objeto na floresta, independentemente de o objeto ser um membro do domínio do controlador de domínio. Os controladores de domínio com o recurso de catálogo global ativado são referidos como servidores de catálogo global. O catálogo global fornece um catálogo pesquisável de todos os objetos em cada domínio em um Active Directory Domain Services (AD DS) multi-domínio.

Identificador de segurança do Active Directory

Um identificador de segurança (SID) é um número de identificação único atribuído a um objeto no Active Directory, tal como um usuário, grupo ou host. É o equivalente funcional dos UIDs e GIDs no Linux.

Jogo possível

As peças de teatro possíveis são os blocos de construção dos Livros de Brinquedos Ansíveis . O objetivo de uma peça de teatro é mapear um grupo de anfitriões para alguns papéis bem definidos, representados por Tarefas Possível.

Livro de jogo possível

Um livro de jogo possível é um arquivo que contém uma ou mais peças de teatro possíveis. Para mais informações, consulte a documentação oficial de um livro-jogo .

Tarefa possível

As tarefas possíveis são unidades de ação em Ansible. Um jogo possível pode conter várias tarefas. O objetivo de cada tarefa é executar um módulo, com argumentos muito específicos. Uma tarefa possível é um conjunto de instruções para alcançar um estado definido, em seus termos gerais, por uma função ou módulo específico de Possível, e afinado pelas variáveis dessa função ou módulo. Para mais informações, consulte a documentação oficial das Tarefas Ansíveis .

Certificado

Um certificado é um documento eletrônico utilizado para identificar um indivíduo, um servidor, uma empresa ou outra entidade e para associar essa identidade a uma chave pública. Tal como uma carteira de motorista ou passaporte, um certificado fornece uma prova geralmente reconhecida da identidade de uma pessoa. A criptografia de chave pública utiliza certificados para resolver o problema da personificação.

Autoridades Certificadoras (CA) em IdM

Uma entidade que emite certificados digitais. Na Red Hat Identity Management, a principal CA é **ipa**, a IdM CA. O certificado da CA **ipa** é um dos seguintes tipos:

- Auto-assinado. Neste caso, a CA **ipa** é a CA de raiz.
- Assinado externamente. Neste caso, o **ipa** CA está subordinado ao CA externo.

Na IdM, você também pode criar múltiplos **sub-CAs**. Sub-CAs são CAs IdM cujos certificados são um dos seguintes tipos:

- Assinado pela CA **ipa**.
- Assinado por qualquer uma das ACs intermediárias entre si e **ipa** CA. O certificado de uma sub-CA não pode ser autoassinado.

Confiança na floresta cruzada

Um trust estabelece uma relação de acesso entre dois reinos Kerberos, permitindo que usuários e serviços em um domínio acessem recursos em outro domínio.
Com uma confiança cruzada entre um domínio raiz florestal Active Directory (AD) e um domínio IdM, os usuários dos domínios florestais AD podem interagir com máquinas e serviços Linux do domínio IdM. Da perspectiva do AD, o Gerenciamento da Identidade representa uma floresta AD separada com um único domínio AD. Para mais informações, veja Como funciona a confiança.

Registros DNS PTR

Os registros DNS pointer (PTR) resolvem um endereço IP de um host para um domínio ou nome de host. Os registros PTR são o oposto dos registros DNS A e AAAA, que resolvem nomes de host para endereços IP. Os registros DNS PTR permitem a pesquisa inversa do DNS. Os registros PTR são armazenados no servidor DNS.

Registros DNS SRV

Um registro de serviço DNS (SRV) define o nome do host, número da porta, protocolo de transporte, prioridade e peso de um serviço disponível em um domínio. Você pode usar registros SRV para localizar servidores IdM e réplicas.

Controlador de domínio (DC)

Um controlador de domínio (DC) é um host que responde a solicitações de autenticação de segurança dentro de um domínio e controla o acesso a recursos nesse domínio. Os servidores IdM funcionam como DCs para o domínio IdM. Um CD autentica usuários, armazena informações de contas de usuários e reforça a política de segurança para um domínio. Quando um usuário faz login em um domínio, o CD autentica e valida suas credenciais e permite ou nega o acesso.

Nome de domínio totalmente qualificado

Um nome de domínio totalmente qualificado (FQDN) é um nome de domínio que especifica a localização exata de um host dentro da hierarquia do Sistema de Nomes de Domínio (DNS). Um dispositivo com o hostname **myhost** no domínio pai **example.com** tem o FQDN **myhost.example.com**. O FQDN distingue exclusivamente o dispositivo de qualquer outro host chamado **myhost** em outros domínios.
Se você estiver instalando um cliente IdM no host **machine1** usando o DNS autodiscovery e seus registros DNS estiverem corretamente configurados, a FQDN de **machine1** é tudo o que você precisa. Para mais informações, consulte o nome do host e os requisitos DNS para IdM .

Réplica oculta

Uma réplica oculta é uma réplica IdM que tem todos os serviços funcionando e disponíveis, mas suas funções de servidor estão desativadas, e os clientes não podem descobrir a réplica porque ela não tem registros SRV no DNS.
As réplicas ocultas são projetadas principalmente para serviços tais como backups, importação e exportação em massa, ou ações que requerem o fechamento dos serviços IdM. Como nenhum cliente utiliza uma réplica oculta, os administradores podem fechar temporariamente os serviços neste host sem afetar nenhum cliente. Para mais informações, consulte O modo de réplica oculta .

Faixas de identificação

Uma faixa de ID é uma faixa de números de ID atribuídos à topologia IdM ou a uma réplica específica. Você pode usar intervalos de ID para especificar o intervalo válido de UIDs e GIDs para novos usuários, hosts e grupos. As faixas de ID são usadas para evitar conflitos de números de ID. Há dois tipos distintos de faixas de ID no IdM:

- *IdM ID range*
  Use esta faixa de ID para definir as UIDs e GIDs para usuários e grupos em toda a topologia da IdM. A instalação do primeiro mestre IdM cria a faixa de ID do IdM. Não é possível modificar o intervalo de ID do IdM após criá-lo. Entretanto, você pode criar uma faixa de IDM adicional, por exemplo, quando a faixa original estiver próxima do esgotamento.

- *Distributed Numeric Assignment (DNA) ID range*
  Use esta faixa de ID para definir os UIDs e GIDs que uma réplica usa ao criar novos usuários. Adicionar uma nova entrada de usuário ou host a uma réplica IdM pela primeira vez atribui uma faixa de ID de DNA a essa réplica. Um administrador pode modificar a faixa de ID de DNA, mas a nova definição deve caber dentro de uma faixa de ID de IdM existente.

  Observe que a faixa IdM e a faixa de DNA correspondem, mas não estão interligadas. Se você mudar um intervalo, certifique-se de mudar o outro para coincidir.

Para mais informações, consulte as faixas de identificação.

Vistas de identificação

As visualizações de ID permitem especificar novos valores para os atributos do usuário ou grupo POSIX, e definir em qual cliente hospedar ou hospedar os novos valores serão aplicados. Por exemplo, você pode usar as visões de ID para:

- Definir diferentes valores de atributos para diferentes ambientes.
- Substituir um valor de atributo gerado anteriormente por um valor diferente.

Em uma configuração de confiança IdM-AD, o **Default Trust View** é uma visão de ID aplicada a usuários e grupos AD. Usando o **Default Trust View**, você pode definir atributos POSIX personalizados para usuários e grupos de AD, anulando assim os valores definidos no AD.

Para mais informações, consulte Utilizando uma visualização de ID para anular um valor de atributo de usuário em um cliente IdM.

Servidor IdM CA

Um servidor IdM no qual está instalado e funcionando o serviço da Autoridade de Certificação IdM (CA).
Nomes alternativos **CA server**

Implantação da IdM

Um termo que se refere à totalidade de sua instalação IdM. Você pode descrever sua implantação do IdM respondendo as seguintes perguntas:

- Sua implantação de IdM é uma implantação de teste ou de produção?
  - Quantos servidores IdM você tem?
- Sua implantação de IdM contém uma CA integrada?
  - Se sim, o CA integrado é autoassinado ou assinado externamente?
  - Se sim, em que servidores está disponível o papel de CA? Em quais servidores o papel da KRA está disponível?
- Sua implantação de IdM contém um DNS integrado?
  - Se sim, em quais servidores o papel do DNS está disponível?
- Sua implantação de IdM está em um acordo de confiança com uma floresta AD?
  - Se for, em quais servidores está disponível o papel de controlador do AD trust ou agente do AD trust?

IdM mestre e réplicas

O primeiro servidor instalado usando o comando **ipa-server-install**, usado para criar o domínio IdM, é conhecido como o **master server** ou **IdM master**.
Os administradores podem usar o comando **ipa-replica-install** para instalar **replicas**, além do mestre. Por padrão, a instalação de uma réplica cria um acordo de replicação com o servidor IdM a partir do qual ela foi criada, permitindo receber e enviar atualizações para o resto da IdM.

Não há diferença funcional entre um mestre e uma réplica. Ambos são servidores IdM totalmente funcionais.

Nomes alternativos: **master**, **master server**, **IdM master server**

Servidor principal do IdM CA

Se sua topologia IdM contém uma autoridade de certificação integrada (CA), um servidor tem o papel de mestre de geração da lista de revogação de certificados (CRL) e o mestre de renovação da CA. Este servidor é o **master CA server**. Em uma implantação sem CA integrada, não há um servidor CA mestre.
Nomes alternativos **master CA**

IMPORTANTE

IdM master e **master CA server** são dois termos diferentes. Por exemplo, no cenário de implantação a seguir, o primeiro servidor é o mestre da IdM e a réplica é o servidor mestre da CA:

1. Você instala o primeiro servidor IdM em seu ambiente sem CA integrada.
2. Você instala uma réplica.
3. Você instala um CA na réplica.

Neste cenário, o primeiro servidor é o master IdM e a réplica é o servidor CA master.

Topologia IdM

Um termo que se refere à estrutura de sua solução IdM , especialmente os acordos de replicação entre e dentro de centros de dados e clusters individuais.

Indicadores de autenticação Kerberos

Os indicadores de autenticação são anexados aos bilhetes Kerberos e representam o método de autenticação inicial utilizado para adquirir um bilhete:

- **otp** para autenticação de dois fatores (senha One-Time Password)
- **radius** para autenticação Remote Authentication Dial-In User Service (RADIUS) (comumente para autenticação 802.1x)
- **pkinit** para criptografia de chave pública para autenticação inicial em Kerberos (PKINIT), smart card, ou autenticação de certificado
- **hardened** para senhas endurecidas contra tentativas de força bruta

Para mais informações, consulte os indicadores de autenticação Kerberos.

Kerberos keytab

Enquanto uma senha é o método padrão de autenticação para um usuário, as fitas-chave são o método padrão de autenticação para hosts e serviços. Uma chave Kerberos keytab é um arquivo que contém uma lista dos principais Kerberos e suas chaves de criptografia associadas, de modo que um serviço pode recuperar sua própria chave Kerberos e verificar a identidade de um usuário.
Por exemplo, cada cliente IdM tem um arquivo **/etc/krb5.keytab** que armazena informações sobre o principal **host**, que representa a máquina cliente no reino de Kerberos.

Kerberos principal

Os diretores exclusivos da Kerberos identificam cada usuário, serviço e hospedeiro em um reino Kerberos:

Entidade	Convenção de nomenclatura	Exemplo
Usuários	**identifier@REALM**	**admin@EXAMPLE.COM**
Serviços	**service/fully-qualified-hostname@REALM**	**http/master.example.com@EXAMPLE.COM**
Anfitriões	**host/fully-qualified-hostname@REALM**	**host/client.example.com@EXAMPLE.COM**

Protocolo Kerberos

Kerberos é um protocolo de autenticação de rede que fornece autenticação forte para aplicações cliente e servidor, utilizando criptografia de chave secreta. IdM e Active Directory usam Kerberos para autenticação de usuários, hosts e serviços.

Reino de Kerberos

Um reino Kerberos abrange todos os principais administrados por um Centro de Distribuição de Chaves Kerberos (KDC). Em uma implantação IdM, o reino Kerberos inclui todos os usuários, hosts e serviços da IdM.

Políticas de bilhetes Kerberos

O Kerberos Key Distribution Center (KDC) reforça o controle de acesso aos bilhetes através de políticas de conexão, e gerencia a duração dos bilhetes Kerberos através de políticas de ciclo de vida dos bilhetes. Por exemplo, a duração padrão global do bilhete é de um dia, e a idade máxima de renovação padrão global é de uma semana. Para mais informações, consulte os tipos de políticas de bilhetes da IdM Kerberos.

Centro de Distribuição de Chaves (KDC)

O Kerberos Key Distribution Center (KDC) é um serviço que atua como a autoridade central e confiável que gerencia as informações de credenciais Kerberos. O KDC emite bilhetes Kerberos e garante a autenticidade dos dados provenientes de entidades dentro da rede IdM.
Para mais informações, veja O papel da IdM KDC .

Sub-CA leve

Na IdM, uma sub-CA leve é uma autoridade certificadora (AC) cujo certificado é assinado por uma AC raiz da IdM ou uma das ACs que lhe estão subordinadas. Uma sub-CA leve emite certificados somente para uma finalidade específica, por exemplo, para assegurar uma conexão VPN ou HTTP.
Para mais informações, consulte Restringindo um pedido para confiar apenas um subconjunto de certificados.

Política de senhas

Uma política de senha é um conjunto de condições que as senhas de um determinado grupo de usuários da IdM devem cumprir. As condições podem incluir os seguintes parâmetros:

- O comprimento da senha
- O número de classes de caracteres utilizados
- A vida útil máxima de uma senha.

Para mais informações, veja O que é uma política de senha .

Atributos POSIX

Os atributos POSIX são atributos do usuário para manter a compatibilidade entre os sistemas operacionais.
Em um ambiente de Gerenciamento de Identidade da Red Hat, os atributos POSIX para os usuários incluem:

- **cn**, o nome do usuário
- **uid**, o nome da conta (login)
- **uidNumber**, um número de usuário (UID)
- **gidNumber**, o número do grupo primário (GID)
- **homeDirectory**, o diretório pessoal do usuário

Em um ambiente de Gerenciamento de Identidade da Red Hat, os atributos POSIX para grupos incluem:

- **cn**, o nome do grupo
- **gidNumber**, o número do grupo (GID)

Esses atributos identificam usuários e grupos como entidades separadas.

Acordo de replicação

Um acordo de replicação é um acordo entre dois servidores IdM na mesma implantação da IdM. O acordo de replicação garante que os dados e a configuração sejam continuamente replicados entre os dois servidores.
IdM usa dois tipos de acordos de replicação: *domain replication* acordos, que replicam informações de identidade, e *certificate replication* acordos, que replicam informações de certificado.

Para mais informações, veja:

- Acordos de replicação
- Determinando o número apropriado de réplicas
- Conectando as réplicas em uma topologia
- Exemplos de topologia de réplicas

Cartão inteligente

Um cartão inteligente é um dispositivo removível ou cartão usado para controlar o acesso a um recurso. Eles podem ser cartões plásticos do tamanho de um cartão de crédito com um chip de circuito integrado (IC) incorporado, pequenos dispositivos USB como um Yubikey, ou outros dispositivos similares. Os Cartões Smart Card podem fornecer autenticação permitindo aos usuários conectar um Cartão Smart Card a um computador host, e o software nesse computador host interage com o material chave armazenado no Cartão Smart Card para autenticar o usuário.

SSSD

O System Security Services Daemon (SSSD) é um serviço de sistema que gerencia a autenticação do usuário e a autorização do usuário em um host RHEL. O SSSD opcionalmente mantém um cache de identidades e credenciais de usuários recuperadas de provedores remotos para autenticação offline. Para mais informações, consulte Entendendo o SSSD e seus benefícios .

Backend SSSD

Um backend SSSD, freqüentemente também chamado de provedor de dados, é um processo SSSD infantil que gerencia e cria o cache SSSD. Este processo se comunica com um servidor LDAP, realiza diferentes consultas de busca e armazena os resultados no cache. Ele também realiza autenticação on-line contra LDAP ou Kerberos e aplica a política de acesso e senha para o usuário que está fazendo o login.

Ticket-granting ticket (TGT)

Após a autenticação em um Centro de Distribuição de Chaves Kerberos (KDC), um usuário recebe um ticket de concessão de ingressos (TGT), que é um conjunto temporário de credenciais que pode ser usado para solicitar ingressos de acesso a outros serviços, tais como websites e e-mail.
O uso de um TGT para solicitar acesso adicional proporciona ao usuário uma experiência de Single Sign-On, já que o usuário só precisa se autenticar uma vez para poder acessar vários serviços. Os TGTs são renováveis, e as políticas de bilhetes Kerberos determinam os limites de renovação de bilhetes e controle de acesso.

Para mais informações, consulte as políticas de bilhetes da Kerberos Managing Kerberos.

Glossários adicionais

Se você não conseguir encontrar um termo de Gerenciamento de Identidade neste glossário, consulte os glossários do Servidor de Diretório e do Sistema de Certificados:

- Servidor de Diretório 11 Glossário
- Sistema de Certificado 9 Glossário

1.5. RECURSOS ADICIONAIS

- Para informações gerais sobre a Red Hat IdM, consulte a página do produto Red Hat Identity Management no Portal do Cliente da Red Hat.

CAPÍTULO 2. PLANEJAMENTO DA TOPOLOGIA DA RÉPLICA

As seções seguintes fornecem conselhos para determinar a topologia apropriada da réplica para seu caso de uso.

2.1. MÚLTIPLOS SERVIDORES DE RÉPLICAS COMO SOLUÇÃO PARA ALTO DESEMPENHO E RECUPERAÇÃO DE DESASTRES

A funcionalidade contínua e a alta disponibilidade dos serviços de Gerenciamento de Identidade (IdM) é vital para os usuários que acessam recursos. Uma das soluções integradas para a realização de funcionalidade contínua e alta disponibilidade da infra-estrutura de IdM através do balanceamento de carga é a replicação do diretório central através da criação de servidores réplicas do servidor mestre.

IdM permite colocar servidores adicionais em centros de dados geograficamente dispersos para refletir a estrutura organizacional de sua empresa. Desta forma, o caminho entre os clientes IdM e o servidor acessível mais próximo é encurtado. Além disso, a existência de múltiplos servidores permite a expansão da carga e o escalonamento para mais clientes.

Manter vários servidores IdM redundantes e deixá-los replicar uns com os outros também é um mecanismo de backup comum para mitigar ou prevenir a perda do servidor. Por exemplo, se um servidor falhar, os outros servidores continuam fornecendo serviços para o domínio. Você também pode recuperar o servidor perdido criando uma nova réplica baseada em um dos servidores restantes.

2.2. INTRODUÇÃO AOS SERVIDORES E CLIENTES DA IDM

O domínio de Gerenciamento de Identidade (IdM) inclui os seguintes tipos de sistemas:

Servidores IdM

Os servidores IdM são sistemas Red Hat Enterprise Linux que respondem a pedidos de identidade, autenticação e autorização dentro de um domínio IdM. Na maioria das implementações, uma autoridade de certificação integrada (CA) também é instalada com o servidor IdM.
Os servidores IdM são os repositórios centrais para informações de identidade e políticas. Os servidores IdM também podem hospedar qualquer um dos serviços opcionais utilizados pelos membros do domínio:

- Autoridade Certificadora (CA)
- Autoridade de Recuperação Chave (KRA)
- DNS
- Controlador de confiança Active Directory (AD)
- Agente fiduciário do Active Directory (AD)

O primeiro servidor instalado para criar o domínio é o *IdM master* ou *master server*. O master IdM não deve ser confundido com o servidor *master CA*: eles podem funcionar em duas máquinas diferentes.

Clientes da IdM

Os clientes IdM são sistemas Red Hat Enterprise Linux inscritos nos servidores e configurados para usar os serviços IdM nestes servidores.
Os clientes interagem com os servidores da IdM para acessar os serviços por eles prestados. Por exemplo, os clientes utilizam o protocolo Kerberos para realizar a autenticação e adquirir bilhetes para o single sign-on empresarial (SSO), utilizar o LDAP para obter informações de identidade e

políticas, utilizar o DNS para detectar onde os servidores e serviços estão localizados e como se conectar a eles.

Os servidores da IdM também são clientes da IdM embutidos. Como clientes inscritos com eles mesmos, os servidores oferecem a mesma funcionalidade que outros clientes.

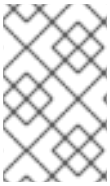
Para fornecer serviços para um grande número de clientes, bem como para redundância e disponibilidade, a IdM permite a implantação em vários servidores IdM em um único domínio. É possível implantar até 60 servidores. Este é o número máximo de servidores IdM, também chamados de réplicas, que é atualmente suportado no domínio IdM. Os servidores IdM fornecem diferentes serviços para o cliente. Nem todos os servidores precisam fornecer todos os serviços possíveis. Alguns componentes de servidor como Kerberos e LDAP estão sempre disponíveis em todos os servidores. Outros serviços como CA, DNS, Trust Controller ou Vault são opcionais. Isto significa que servidores diferentes em geral desempenham papéis diferentes na implantação.

Se sua topologia IdM contém uma CA integrada, um servidor também tem o papel de mestre de geração da lista de revogação de certificados (CRL) e o mestre de renovação da CA . Este servidor é o *master CA*.

ATENÇÃO

O servidor *master CA* é crítico para sua implantação do IdM porque é o único sistema no domínio responsável pelo rastreamento de certificados e chaves do subsistema CA, e pela geração da CRL. Para detalhes sobre como se recuperar de um desastre que afete sua implantação de IdM, consulte Realizando a recuperação de desastres com Gerenciamento de Identidade.

Para redundância e equilíbrio de carga, os administradores criam servidores adicionais criando um *replica* de qualquer servidor existente, seja o servidor mestre ou outra réplica. Ao criar uma réplica, a IdM clona a configuração do servidor existente. Uma réplica compartilha com o servidor inicial sua configuração principal, incluindo informações internas sobre usuários, sistemas, certificados e políticas configuradas.



NOTA

Uma réplica e o servidor de onde ela foi criada são funcionalmente idênticos, exceto pelo papel do mestre da geração CRL. Portanto, os termos *server* e *replica* são utilizados de forma intercambiável aqui, dependendo do contexto.

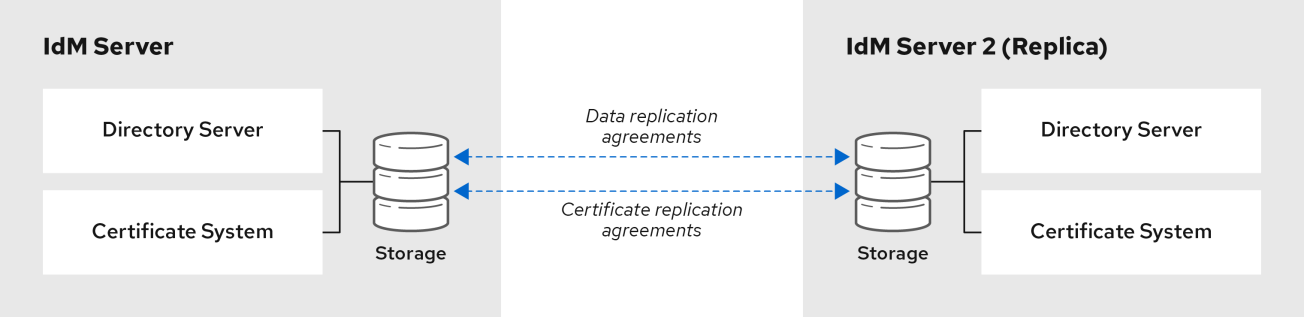
2.3. ACORDOS DE REPLICAÇÃO

Quando um administrador cria uma réplica baseada em um servidor existente, o Gerenciamento de Identidade (IdM) cria um *replication agreement* entre o servidor inicial e a réplica. O acordo de replicação garante que os dados e a configuração sejam continuamente replicados entre os dois servidores.

Os acordos de replicação são sempre bilaterais: os dados são replicados de um servidor para o outro, assim como do outro servidor para o primeiro servidor.

IdM usa *multi-master replication*. Na replicação multi-mestre, todas as réplicas unidas em um acordo de replicação recebem atualizações e, portanto, são consideradas mestres de dados.

Figura 2.1. Acordos de servidor e réplicas



A IdM usa dois tipos de acordos de replicação:

Acordos de replicação de domínio

Estes acordos replicam as informações de identidade.

Acordos de replicação de certificados

Estes acordos replicam as informações do certificado.

Os dois canais de replicação são independentes. Dois servidores podem ter um ou ambos os tipos de acordos de replicação configurados entre eles. Por exemplo, quando o servidor A e o servidor B têm apenas um acordo de replicação de domínio configurado, apenas as informações de identidade são replicadas entre eles, não as informações do certificado.

2.4. DETERMINANDO O NÚMERO APROPRIADO DE RÉPLICAS

Montar pelo menos duas réplicas em cada centro de dados (não é uma exigência difícil)

Um centro de dados pode ser, por exemplo, um escritório principal ou uma localização geográfica.

Configure um número suficiente de servidores para atender a seus clientes

Um servidor de Gerenciamento de Identidade (IdM) pode fornecer serviços a 2000 - 3000 clientes. Isto pressupõe que os clientes consultem os servidores várias vezes ao dia, mas não, por exemplo, a cada minuto. Se você espera consultas mais freqüentes, planeje mais servidores.

Estabelecer um número suficiente de réplicas da Autoridade Certificadora (CA)

Somente réplicas com a função CA instalada podem replicar os dados do certificado. Se você usar o IdM CA, certifique-se de que seu ambiente tenha pelo menos duas réplicas CA com acordos de replicação de certificados entre elas.

Configurar um máximo de 60 réplicas em um único domínio IdM

A Red Hat suporta ambientes com até 60 réplicas.

2.5. CONECTANDO AS RÉPLICAS EM UMA TOPOLOGIA

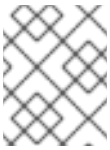
Conecte cada réplica a pelo menos duas outras réplicas

A configuração de acordos de replicação adicionais garante que as informações sejam replicadas não apenas entre a réplica inicial e o servidor mestre, mas também entre outras réplicas.

Conectar uma réplica a um máximo de quatro outras réplicas (não é uma exigência difícil)

Um grande número de acordos de replicação por servidor não acrescenta benefícios significativos.

Uma réplica receptora só pode ser atualizada por uma outra réplica de cada vez e, enquanto isso, os outros acordos de replicação são ociosos. Mais de quatro acordos de replicação por réplica tipicamente significa um desperdício de recursos.



NOTA

Esta recomendação se aplica tanto aos acordos de replicação de certificados quanto aos acordos de replicação de domínios.

Há duas exceções para o limite de quatro acordos de replicação por réplica:

- Você quer caminhos de falha se certas réplicas não estiverem online ou não responderem.
- Em implantações maiores, você quer ligações diretas adicionais entre nós específicos.

A configuração de um alto número de acordos de replicação pode ter um impacto negativo no desempenho geral: quando múltiplos acordos de replicação na topologia estão enviando atualizações, certas réplicas podem experimentar uma alta contenção no arquivo do banco de dados changelog entre as atualizações recebidas e as atualizações enviadas.

Se você decidir usar mais acordos de replicação por réplica, certifique-se de não ter problemas de replicação e latência. Entretanto, observe que grandes distâncias e altos números de nós intermediários também podem causar problemas de latência.

Conectar as réplicas em um centro de dados umas com as outras

Isto garante a replicação de domínio dentro do centro de dados.

Conectar cada centro de dados a pelo menos dois outros centros de dados

Isto garante a replicação de domínio entre os centros de dados.

Conectar centros de dados usando pelo menos um par de acordos de replicação

Se os centros de dados A e B tiverem um acordo de replicação de A1 a B1, ter um acordo de replicação de A2 a B2 garante que, se um dos servidores estiver desligado, a replicação pode continuar entre os dois centros de dados.

2.6. EXEMPLOS DE TOPOLOGIA DE RÉPLICAS

As figuras abaixo mostram exemplos de topologias de Gerenciamento de Identidade (IdM) baseadas nas diretrizes para a criação de uma topologia confiável.

Figura 2.2, “Réplica Topologia Exemplo 1” mostra quatro centros de dados, cada um com quatro servidores. Os servidores são conectados com acordos de replicação.

Figura 2.2. Réplica Topologia Exemplo 1

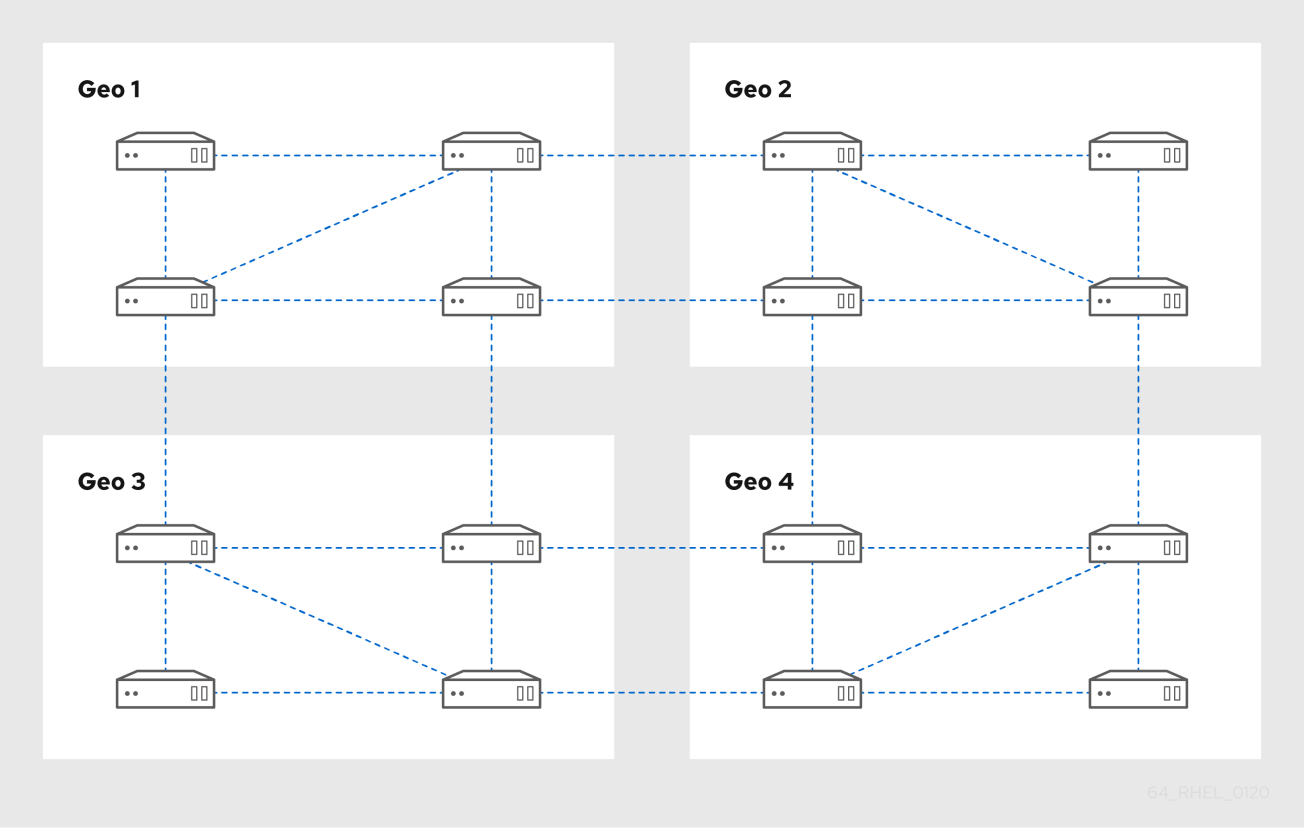
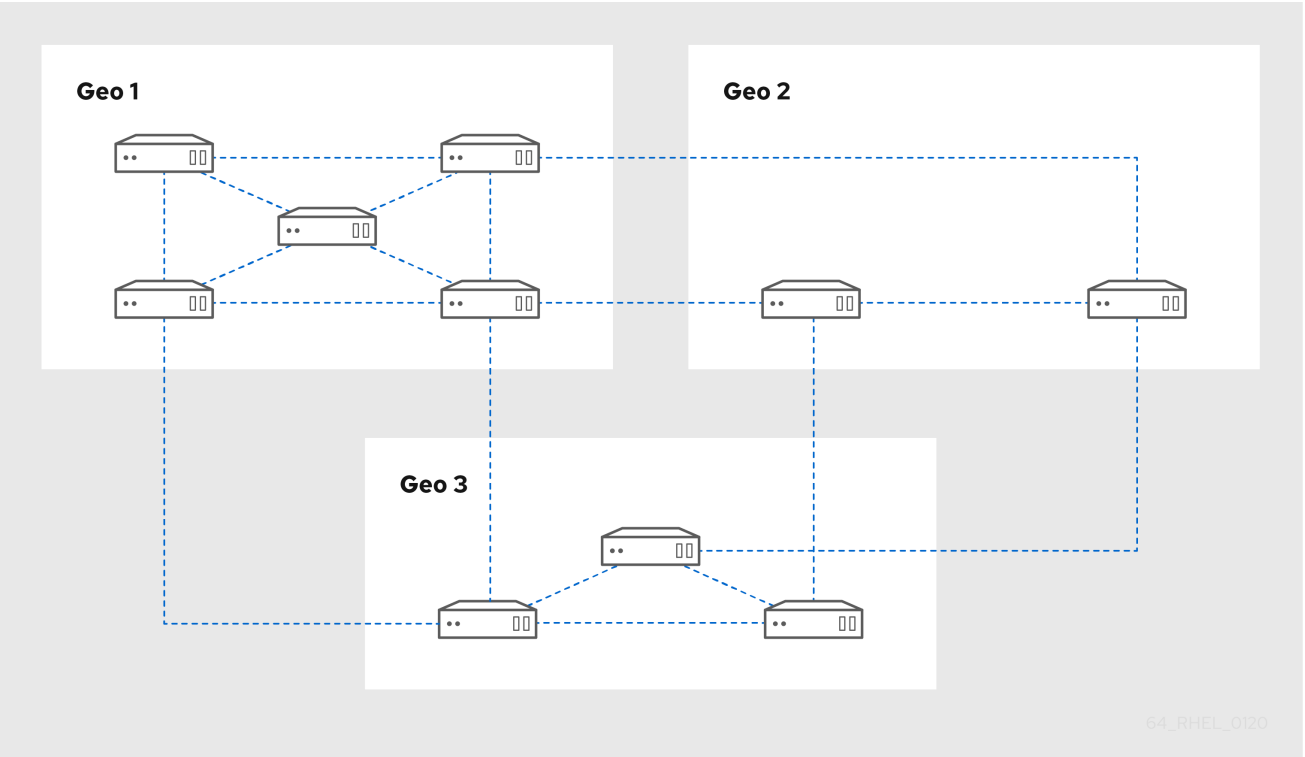


Figura 2.3, "Réplica Topologia Exemplo 2" mostra três centros de dados, cada um com um número diferente de servidores. Os servidores são conectados com acordos de replicação.

Figura 2.3. Réplica Topologia Exemplo 2



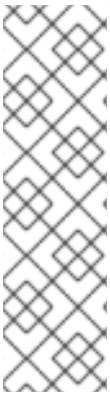
2.7. O MODO DE RÉPLICA OCULTA

Por padrão, quando você configura uma nova réplica, o instalador cria automaticamente registros de recursos de serviço (SRV) no DNS. Estes registros permitem aos clientes auto-descobrir a réplica e seus serviços. Uma réplica oculta é um servidor IdM que tem todos os serviços funcionando e disponíveis. Entretanto, não possui registros SRV no DNS e as funções do servidor LDAP não estão habilitadas. Portanto, os clientes não podem usar a descoberta de serviços para detectar estas réplicas ocultas.

NOTA

O recurso de réplica oculta está disponível no Red Hat Enterprise Linux 8.1 e, mais tarde, como uma Pré-visualização Tecnológica e, portanto, não é suportado.

As réplicas ocultas são projetadas principalmente para serviços dedicados que de outra forma podem perturbar os clientes. Por exemplo, um backup completo da IdM requer o encerramento de todos os serviços da IdM no master ou réplica. Como nenhum cliente usa uma réplica oculta, os administradores podem fechar temporariamente os serviços neste host sem afetar nenhum cliente.



NOTA

- Restaurar um backup de uma réplica escondida em um novo host sempre resulta em uma réplica não escondida (regular).
- Todas as funções de servidor usadas em um cluster, especialmente a função de Autoridade Certificadora se a CA integrada for usada, devem ser instaladas na réplica oculta para que o backup seja capaz de restaurar esses serviços.
- Para mais informações sobre como criar e trabalhar com backups IdM, veja Backing Up and Restoring IdM .

Outros casos de uso incluem operações de alta carga no IdM API ou no servidor LDAP, tais como uma importação em massa ou consultas extensivas. Para instalar uma réplica como oculta, passe o parâmetro **--hidden-replica** para o comando **ipa-replica-install**.

Para mais detalhes sobre a instalação de uma réplica, consulte Instalando uma réplica de Gerenciamento de Identidade.

Alternativamente, você pode mudar o estado de uma réplica existente. Para detalhes, consulte Demonstração e Promoção de réplicas ocultas .

CAPÍTULO 3. PLANEJANDO SEUS SERVIÇOS DNS E NOMES DE HOST

O Gerenciamento de Identidade (IdM) fornece diferentes tipos de configurações de DNS no servidor IdM. As seções seguintes as descrevem e fornecem conselhos sobre como determinar qual é o melhor para seu caso de uso.

3.1. SERVIÇOS DNS DISPONÍVEIS EM UM SERVIDOR IDM

Você pode instalar um servidor de Gerenciamento de Identidade (IdM) com ou sem DNS integrado.

Tabela 3.1. Comparando IdM com DNS integrado e sem DNS integrado

	Com DNS integrado	Sem DNS integrado
Visão geral:	IdM executa seu próprio serviço DNS para o domínio IdM.	IdM utiliza os serviços DNS fornecidos por um servidor DNS externo.
Limitações:	O servidor DNS integrado fornecido pela IdM suporta apenas recursos relacionados à implantação e manutenção da IdM. Ele não suporta alguns dos recursos avançados do DNS. Não foi projetado para ser usado como um servidor DNS de uso geral.	O DNS não está integrado com ferramentas nativas da IdM. Por exemplo, o IdM não atualiza os registros DNS automaticamente após uma mudança na topologia.
Funciona melhor para:	Uso básico dentro da implantação da IdM. Quando o servidor IdM gerencia o DNS, o DNS é fortemente integrado com ferramentas nativas da IdM, o que permite automatizar algumas das tarefas de gerenciamento de registros DNS.	Ambientes onde são necessários recursos avançados de DNS além do escopo do DNS da IdM. Ambientes com uma infra-estrutura DNS bem estabelecida onde você quer continuar usando um servidor DNS externo.

Mesmo que um servidor de Gerenciamento de Identidade seja usado como servidor DNS primário, outros servidores DNS externos ainda podem ser usados como servidores secundários. Por exemplo, se seu ambiente já estiver usando outro servidor DNS, como um servidor DNS integrado ao Active Directory (AD), você pode delegar apenas o domínio principal da IdM ao DNS integrado à IdM. Não é necessário migrar as zonas DNS para o DNS do IdM.

NOTA

Se você precisar emitir certificados para clientes IdM com um endereço IP na extensão Subject Alternative Name (SAN), você deve usar o serviço DNS integrado da IdM.

3.2. DIRETRIZES PARA O PLANEJAMENTO DO NOME DE DOMÍNIO DNS E DO NOME DO REINO KERBEROS

Ao instalar o primeiro servidor de Gerenciamento de Identidade (IdM), a instalação solicita um nome DNS primário do domínio IdM e o nome do reino Kerberos. As diretrizes nesta seção podem ajudá-lo a definir os nomes corretamente.

ATENÇÃO

Você não poderá mudar o nome de domínio primário do IdM e o nome do reino Kerberos depois que o servidor já estiver instalado. Não espere ser capaz de passar de um ambiente de teste para um ambiente de produção mudando os nomes, por exemplo, de ***lab.example.com*** para ***production.example.com***.

Um domínio DNS separado para registros de serviço

Garantir que o *primary DNS domain* utilizado para a IdM não seja compartilhado com nenhum outro sistema. Isto ajuda a evitar conflitos no nível do DNS.

Delegação apropriada de nomes de domínio DNS

Assegure-se de ter uma delegação válida na árvore pública do DNS para o domínio DNS. Não utilize um nome de domínio que não seja delegado a você, nem mesmo em uma rede privada.

Domínio DNS multi-label

Não utilize nomes de domínio com rótulo único, por exemplo **.company**. O domínio IdM deve ser composto por um ou mais subdomínios e um domínio de nível superior, por exemplo **example.com** ou **company.example.com**.

Um nome único do reino de Kerberos

Garantir que o nome do reino não esteja em conflito com nenhum outro nome existente do reino Kerberos, como um nome usado pelo Active Directory (AD).

Nome do reino Kerberos como uma versão em maiúsculas do nome DNS primário

Considere definir o nome do reino para uma maiúscula (***EXAMPLE.COM***) versão do nome de domínio DNS primário (***example.com***).

ATENÇÃO

Se você não definir o nome do reino Kerberos como a versão em maiúsculas do nome DNS primário, você não poderá usar os trusts AD.

Notas adicionais sobre o planejamento do nome de domínio DNS e do nome do reino Kerberos

- Uma implantação da IdM sempre representa um reino Kerberos.
- Você pode se juntar a clientes da IdM a partir de vários domínios DNS distintos (***example.com***, ***example.net***, ***example.org***) para um único reino de Kerberos (***EXAMPLE.COM***).

- Os clientes da IdM não precisam estar no domínio DNS primário. Por exemplo, se o domínio IdM for ***idm.example.com***os clientes podem estar no ***clients.example.com*** mas um mapeamento claro deve ser configurado entre o domínio DNS e o reino de Kerberos.

NOTA

O método padrão para criar o mapeamento é usar os registros DNS do **_kerberos** TXT. O DNS integrado do IdM adiciona estes registros automaticamente.

CAPÍTULO 4. PLANEJANDO SEUS SERVIÇOS DE CA

O Gerenciamento de Identidade (IdM) no Red Hat Enterprise Linux fornece diferentes tipos de configurações de autoridade de certificado (CA). As seções seguintes descrevem diferentes cenários e fornecem conselhos para ajudá-lo a determinar qual configuração é a melhor para seu caso de uso.

4.1. SERVIÇOS CA DISPONÍVEIS EM UM SERVIDOR IDM

Você pode instalar um servidor de Gerenciamento de Identidade (IdM) com uma autoridade de certificado IdM integrada (CA) ou sem uma CA.

Tabela 4.1. Comparação entre IdM com CA integrada e sem CA

	CA integrada	Sem um CA
Visão geral:	IdM usa seu próprio serviço de infra-estrutura de chave pública (PKI) com um *CA signing certificate* para criar e assinar os certificados no domínio IdM. ● Se a CA de raiz é a CA integrada, a IdM usa um certificado CA autoassinado. ● Se a CA raiz for uma CA externa, a CA IdM integrada é subordinada à CA externa. O certificado CA usado pelo IdM é assinado pela CA externa, mas todos os certificados para o domínio do IdM são emitidos pela instância do Sistema de Certificado integrado. ● A CA integrada também é capaz de emitir certificados para usuários, anfitriões ou serviços. A AC externa pode ser uma AC corporativa ou uma AC de terceiros.	A IdM não cria sua própria CA, mas utiliza certificados de host assinados por uma CA externa. A instalação de um servidor sem CA exige que você solicite os seguintes certificados a uma autoridade terceirizada: ● Um certificado de servidor LDAP ● Um certificado de servidor Apache ● Um certificado PKINIT ● Cadeia completa de certificados CA da CA que emitiu os certificados de servidor LDAP e Apache

	CA integrada	Sem um CA
Limitações:	Se a CA integrada estiver subordinada a uma CA externa, os certificados emitidos dentro do domínio IdM estão potencialmente sujeitos a restrições estabelecidas pela CA externa para vários atributos de certificado, como por exemplo: ● O período de validade. ● Restrições sobre quais nomes de assuntos podem aparecer nos certificados emitidos pela IDM CA ou por seus subordinados. ● Restrições sobre se a IDM CA pode ela mesma, emitir certificados CA subordinados, ou como "profunda" a cadeia de certificados subordinados pode ir.	O gerenciamento de certificados fora da IdM causa muitas atividades adicionais, tais como : ● A criação, o carregamento e a renovação de certificados é um processo manual. ● O serviço **certmonger** não rastreia os certificados IPA (servidor LDAP, servidor Apache e certificados PKINIT) e não o notifica quando os certificados estão prestes a expirar. Os administradores devem configurar manualmente as notificações para certificados emitidos externamente, ou definir pedidos de rastreamento para esses certificados se quiserem que **certmonger** os rastreie.
Funciona melhor para:	Ambientes que lhe permitem criar e utilizar sua própria infra-estrutura de certificados.	Casos muito raros quando as restrições dentro da infra-estrutura não permitem a instalação de serviços de certificado integrados ao servidor.

NOTA

A mudança da CA autoassinada para uma CA com assinatura externa, ou o contrário, assim como a mudança de qual CA externa emite o certificado da IdM CA, é possível mesmo após a instalação. Também é possível configurar uma CA integrada mesmo depois de uma instalação sem uma CA.

4.2. ASSUNTO CA DN

O assunto Autoridade Certificadora (CA) nome distinto (DN) é o nome da CA. Ele deve ser globalmente único na infra-estrutura de Gerenciamento de Identidade (IdM) da CA e não pode ser alterado após a instalação. Caso você precise que o IdM CA seja assinado externamente, você pode precisar consultar o administrador da CA externa sobre a forma que seu IDM CA Subject DN deve tomar.

4.3. DIRETRIZES PARA DISTRIBUIÇÃO DE SERVIÇOS DE AC

Os seguintes passos fornecem diretrizes para a distribuição de seus serviços de autoridade certificadora (CA).

- Instalar os serviços da CA em mais de um servidor na topologia

As réplicas configuradas sem uma CA encaminham todas as solicitações de operações de certificado para os servidores da CA em sua topologia.

ATENÇÃO

Se você perder todos os servidores com uma CA, você perderá toda a configuração da CA sem qualquer chance de recuperação. Neste caso, você precisa configurar uma nova CA e emitir e instalar novos certificados.

- Mantenha um número suficiente de servidores CA para lidar com as solicitações da CA em sua implantação

Para recomendações, consulte a tabela a seguir:

Tabela 4.2. Diretrizes para a criação do número apropriado de servidores CA

Descrição do desdobramento	Número sugerido de servidores CA
Uma implantação com um número muito grande de certificados emitidos	Três ou quatro servidores CA
Uma implantação com problemas de largura de banda ou disponibilidade entre múltiplas regiões	Um servidor CA por região, com um mínimo de três servidores no total para a implantação
Todas as outras implantações	Dois servidores CA

CAPÍTULO 5. INTEGRAÇÃO DO PLANEJAMENTO COM AD

As seções seguintes apresentam as opções de integração do Red Hat Enterprise Linux com o Active Directory (AD).

- Para uma visão geral da integração direta, veja Seção 5.1, “Integração direta”.
- Para uma visão geral da integração indireta, veja Seção 5.2, “Integração indireta”.
- Para conselhos sobre como decidir entre eles, ver Seção 5.3, “Decidindo entre integração indireta e direta”.

5.1. INTEGRAÇÃO DIRETA

Na integração direta, os sistemas Linux são conectados diretamente ao Active Directory (AD). Os seguintes tipos de integração são possíveis:

Integração com o Sistema de Serviços de Segurança Daemon (SSSD)

O SSSD pode conectar um sistema Linux com várias lojas de identidade e autenticação: AD, Identity Management (IdM), ou um servidor genérico LDAP ou Kerberos.
Requisitos notáveis para integração com SSSD:

- Ao integrar com o AD, o SSSD funciona apenas dentro de uma única floresta AD por padrão. Para configuração multifloresta, configure a enumeração manual de domínios.
- As florestas AD remotas devem confiar na floresta local para garantir que o plug-in **idmap_ad** manipule corretamente os usuários florestais remotos.

O SSSD apóia tanto a integração direta quanto a indireta. Ele também permite mudar de uma abordagem de integração para outra sem custos de migração significativos.

Integração com Samba Winbind

O componente Winbind da suíte Samba emula um cliente Windows em um sistema Linux e se comunica com servidores AD.
Requisitos notáveis para integração com Samba Winbind:

- A integração direta com Winbind em uma configuração AD multifloresta requer fundos bidirecionais.
- Um caminho bidirecional do domínio local de um sistema Linux deve existir para o domínio de um usuário em uma floresta AD remota para permitir que informações completas sobre o usuário do domínio AD remoto estejam disponíveis para o plug-in **idmap_ad**.

Recomendações

- O SSSD satisfaz a maioria dos casos de uso para integração de AD e fornece uma solução robusta como um gateway genérico entre um sistema cliente e diferentes tipos de provedores de identidade e autenticação - AD, IdM, Kerberos, e LDAP.
- Winbind é recomendado para implantação nos servidores membros do domínio AD nos quais você planeja implantar o Samba FS.

5.2. INTEGRAÇÃO INDIRETA

Na integração indireta, os sistemas Linux são primeiro conectados a um servidor central que depois é conectado ao Active Directory (AD). A integração indireta permite ao administrador gerenciar os sistemas e políticas Linux de forma centralizada, enquanto os usuários do AD podem acessar de forma transparente os sistemas e serviços Linux.

Integração baseada na confiança cruzada com a AD

O servidor de Gerenciamento de Identidade (IdM) atua como o servidor central para controlar os sistemas Linux. É estabelecida uma confiança cruzada da Kerberos com o AD, permitindo que os usuários do AD acessem os sistemas e recursos Linux. O IdM se apresenta ao AD como uma floresta separada e aproveita os trusts de nível florestal suportados pelo AD.
Ao utilizar um fundo de confiança:

- Os usuários AD podem acessar os recursos da IdM.
- Os servidores e clientes da IdM podem resolver as identidades dos usuários e grupos AD.
- Usuários e grupos AD acessam a IdM sob as condições definidas pela IdM, tais como o controle de acesso baseado em host.
- Os usuários e grupos AD continuam sendo administrados do lado AD.

Integração baseada na sincronização

Esta abordagem é baseada na ferramenta WinSync. Um acordo de replicação WinSync sincroniza as contas de usuário do AD para o IdM.

ATENÇÃO

WinSync não é mais desenvolvido ativamente no Red Hat Enterprise Linux 8. A solução preferida para integração indireta é a confiança cruzada das florestas.

As limitações da integração baseada na sincronização incluem:

- Os grupos não são sincronizados de IdM para AD.
- Os usuários são duplicados em AD e IdM.
- WinSync suporta apenas um único domínio AD.
- Apenas um controlador de domínio em AD pode ser usado para sincronizar dados com uma instância de IdM.
- As senhas de usuários devem ser sincronizadas, o que requer que o componente PassSync seja instalado em todos os controladores de domínio no domínio AD.
- Após configurar a sincronização, todos os usuários AD devem alterar manualmente as senhas antes que o PassSync possa sincronizá-las.

5.3. DECIDINDO ENTRE INTEGRAÇÃO INDIRETA E DIRETA

As diretrizes desta seção podem ajudar a decidir que tipo de integração se adequa ao seu caso de uso.

Número de sistemas a serem conectados ao Active Directory

Conexão de menos de 30-50 sistemas (não é um limite difícil)

Se você conectar menos de 30-50 sistemas, considere a integração direta. A integração indireta pode introduzir custos indiretos desnecessários.

Conexão de mais de 30-50 sistemas (não é um limite difícil)

Se você conectar mais de 30-50 sistemas, considere a integração indireta com a Gestão de Identidade. Com esta abordagem, você pode se beneficiar da gestão centralizada para sistemas Linux.

Gerenciando um pequeno número de sistemas Linux, mas esperando que o número cresça rapidamente

Neste cenário, considere a integração indireta para evitar ter que migrar o ambiente mais tarde.

Frequência de implantação de novos sistemas e seu tipo

Implantação de sistemas de metal nu em uma base irregular

Se você implanta novos sistemas raramente e eles geralmente são sistemas de metal nu, considere a integração direta. Nesses casos, a integração direta é geralmente mais simples e fácil.

Implantação de sistemas virtuais com freqüência

Se você implanta novos sistemas frequentemente e eles são geralmente sistemas virtuais provisionados sob demanda, considere a integração indireta. Com a integração indireta, você pode usar um servidor central para gerenciar os novos sistemas dinamicamente e integrá-los com ferramentas de orquestração, como o Red Hat Satellite.

O Active Directory é o fornecedor de autenticação necessário

Suas políticas internas estabelecem que todos os usuários devem se autenticar contra o Active Directory?

Você pode escolher entre integração direta ou indireta. Se você utiliza a integração indireta com uma confiança entre o Gerenciamento de Identidade e o Active Directory, os usuários que acessam os sistemas Linux se autenticam contra o Active Directory. As políticas que existem no Active Directory são executadas e aplicadas durante a autenticação.

CAPÍTULO 6. PLANEJANDO UMA CONFIANÇA FLORESTAL CRUZADA ENTRE IDM E AD

Active Directory (AD) e Gerenciamento de Identidade (IdM) são dois ambientes alternativos gerenciando uma variedade de serviços centrais, tais como Kerberos, LDAP, DNS, e serviços de certificados. Um relacionamento *cross-forest trust* integra de forma transparente estes dois ambientes diversos, permitindo que todos os serviços principais interajam de forma transparente. As seções seguintes fornecem conselhos sobre como planejar e projetar uma implantação de confiança entre florestas.

6.1. TRUSTS DE FLORESTAS CRUZADAS ENTRE IDM E AD

Em um ambiente de Active Directory (AD) puro, uma confiança florestal cruzada conecta dois domínios de raiz florestal AD separados. Quando você cria uma confiança florestal cruzada entre AD e IdM, o domínio IdM se apresenta ao AD como uma floresta separada com um único domínio. Uma relação de confiança é então estabelecida entre o domínio raiz da floresta de AD e o domínio IdM. Como resultado, os usuários da floresta AD podem acessar os recursos no domínio IdM.

IdM pode estabelecer uma confiança com uma floresta AD ou múltiplas florestas não relacionadas.

NOTA

Dois reinos Kerberos separados podem ser conectados em um *cross-realm trust*. Entretanto, um reino Kerberos diz respeito apenas à autenticação e não a outros serviços e protocolos envolvidos em operações de identidade e autorização. Portanto, estabelecer uma confiança cruzada Kerberos não é suficiente para permitir que usuários de um reino possam acessar recursos em outro reino.

Uma confiança externa para um domínio AD
Uma confiança externa é uma relação de confiança entre a IdM e um domínio do Active Directory. Enquanto um trust florestal sempre requer o estabelecimento de um trust entre o IdM e o domínio raiz de uma floresta do Active Directory, um trust externo pode ser estabelecido do IdM para qualquer domínio dentro de uma floresta.

6.2. CONTROLADORES DE CONFIANÇA E AGENTES DE CONFIANÇA

O Gerenciamento de Identidade (IdM) fornece os seguintes tipos de servidores IdM que suportam a confiança do Active Directory (AD):

Agentes de confiança

Servidores IdM que podem realizar buscas de identidade contra controladores de domínio AD.

Controladores de confiança

Agentes de confiança que também administram a suíte Samba. Os controladores de domínio AD entram em contato com os controladores de confiança quando estabelecem e verificam a confiança para AD.
O primeiro controlador de confiança é criado quando você configura o trust.

Os controladores de confiança executam mais serviços voltados para a rede do que os agentes de confiança, e assim apresentam uma superfície de ataque maior para intrusos potenciais.

Além dos agentes e controladores de confiança, o domínio IdM também pode incluir servidores IdM

padrão. No entanto, estes servidores não se comunicam com AD. Portanto, os clientes que se comunicam com os servidores padrão não podem resolver usuários e grupos AD ou autenticar e autorizar usuários AD.

Tabela 6.1. Comparando as capacidades suportadas pelos controladores de confiança e agentes de confiança

Capacidades	Agente de confiança	Controlador de confiança
Resolver usuários e grupos de AD	Sim	Sim
Inscrever clientes IdM que executam serviços acessíveis por usuários de florestas AD confiáveis	Sim	Sim
Gerenciar a confiança (por exemplo, adicionar acordos de confiança)	Não	Sim

Ao planejar a implantação de controladores de confiança e agentes de confiança, considere estas diretrizes:

- Configurar pelo menos dois controladores de confiança por implantação da IdM.
- Configurar pelo menos dois controladores de confiança em cada centro de dados.

Se você quiser criar controladores de confiança adicionais ou se um controlador de confiança existente falhar, crie um novo controlador de confiança, promovendo um agente de confiança ou um servidor padrão. Para fazer isso, use o utilitário **ipa-adtrust-install** no servidor da IdM.

IMPORTANTE

Não se pode rebaixar um controlador fiduciário existente para um agente fiduciário.

6.3. TRUSTS UNIDIRECIONAIS E TRUSTS BIDIRECIONAIS

De certa forma, a Gestão de Identidade (IdM) confia no Active Directory (AD), mas a AD não confia na IdM. Os usuários do AD podem acessar recursos no domínio do IdM, mas os usuários do IdM não podem acessar recursos dentro do domínio do AD. O servidor IdM se conecta ao AD usando uma conta especial, e lê informações de identidade que são então entregues aos clientes da IdM através do LDAP.

De duas maneiras, os usuários do IdM podem se autenticar no AD, e os usuários do AD podem se autenticar no IdM. Os usuários AD podem se autenticar e acessar recursos no domínio IdM, como no caso de um caso de confiança. Usuários do IdM podem autenticar mas não podem acessar a maioria dos recursos no AD. Eles só podem acessar os serviços Kerberized nas florestas do AD que não exigem nenhuma verificação de controle de acesso.

Para poder conceder acesso aos recursos AD, a IdM precisa implementar o serviço de Catálogo Global. Este serviço ainda não existe na versão atual do servidor da IdM. Por isso, uma confiança bidirecional entre IdM e AD é quase funcionalmente equivalente a uma confiança unidirecional entre IdM e AD.

6.4. GRUPOS EXTERNOS NÃO-POSIX E MAPEAMENTO SID

A Gestão de Identidade (IdM) utiliza o LDAP para a gestão de grupos. As entradas do Active Directory (AD) não são sincronizadas ou copiadas para o IdM, o que significa que os usuários e grupos do AD não possuem objetos LDAP no servidor LDAP, de modo que não podem ser usados diretamente para expressar a adesão de grupos ao IdM LDAP. Por esta razão, os administradores no IdM precisam criar grupos externos não-POSIX, referenciados como objetos LDAP normais do IdM para significar associação em grupo para usuários AD e grupos no IdM.

Os IDs de segurança (SIDs) para grupos externos não-POSIX são processados pelo SSSD, que mapeia os SIDs de grupos no Active Directory para grupos POSIX no IdM. No Active Directory, os SIDs são associados a nomes de usuários. Quando um nome de usuário AD é usado para acessar recursos do IdM, o SSSD usa o SID do usuário para construir uma informação completa de membros do grupo para o usuário no domínio do IdM.

6.5. CONFIGURANDO O DNS

Estas diretrizes podem ajudá-lo a obter a configuração DNS correta para estabelecer uma confiança cruzada entre o Gerenciamento de Identidade (IdM) e o Active Directory (AD).

Domínios DNS primários exclusivos

Assegurar que tanto o AD quanto o IdM tenham seus próprios domínios DNS primários exclusivos configurados. Por exemplo:

- ***ad.example.com*** para AD e ***idm.example.com*** para IdM
- ***example.com*** para AD e ***idm.example.com*** para IdM

A solução de gerenciamento mais conveniente é um ambiente onde cada domínio DNS é gerenciado por servidores DNS integrados, mas você também pode usar qualquer outro servidor DNS compatível com o padrão.

Sem sobreposição entre os domínios DNS IdM e AD

Os sistemas unidos à IdM podem ser distribuídos em vários domínios DNS. Assegurar que os domínios DNS que contêm clientes IdM não se sobreponham aos domínios DNS que contêm sistemas unidos à AD.

Registros SRV adequados

Assegurar que o domínio DNS principal da IdM tenha registros SRV adequados para suportar os trusts AD.
Para outros domínios DNS que fazem parte do mesmo domínio do IdM, os registros SRV não precisam ser configurados quando a confiança ao AD é estabelecida. A razão é que os controladores de domínio AD não usam os registros SRV para descobrir os centros de distribuição chave (KDCs) da Kerberos, mas baseiam a descoberta do KDC nas informações de roteamento do sufixo do nome para a confiança.

Registros DNS resolvíveis a partir de todos os domínios DNS do trust

Garantir que todas as máquinas possam resolver registros DNS de todos os domínios DNS envolvidos na relação de confiança:

- Ao configurar o DNS do IdM, siga as instruções descritas em Instalação de um servidor IdM com uma CA externa.
- Se você estiver usando IdM sem DNS integrado, siga as instruções descritas em Instalação de um servidor IdM sem DNS integrado.

Nomes do reino Kerberos como versões em caixa alta dos nomes de domínio DNS primários

Assegurar que os nomes do reino Kerberos sejam os mesmos que os nomes de domínio DNS primários, com todas as letras em maiúsculas. Por exemplo, se os nomes de domínio forem ***ad.example.com*** para AD e ***idm.example.com*** para a IdM, os nomes do reino Kerberos devem ser ***AD.EXAMPLE.COM*** e ***IDM.EXAMPLE.COM***.

6.6. NOMES NETBIOS

O nome NetBIOS é geralmente o componente de extrema esquerda do nome de domínio. Por exemplo, o nome NetBIOS:

- No nome de domínio ***linux.example.com***o nome NetBIOS é **linux**.
- No nome de domínio ***example.com***o nome NetBIOS é **example**.

Diferentes nomes NetBIOS para os domínios de Gerenciamento de Identidade (IdM) e Active Directory (AD)

Garantir que os domínios IdM e AD tenham nomes NetBIOS diferentes.
O nome NetBIOS é fundamental para identificar o domínio AD. Se o domínio IdM estiver dentro de um subdomínio do DNS AD, o nome NetBIOS também é crítico para a identificação do domínio e dos serviços IdM.

Limite de caracteres para os nomes NetBIOS

O comprimento máximo de um nome NetBIOS é de 15 caracteres.

6.7. VERSÕES SUPORTADAS DO WINDOWS SERVER

Você pode estabelecer uma relação de confiança com as florestas do Active Directory (AD) que utilizam os seguintes níveis funcionais de floresta e domínio:

- Faixa de nível funcional da floresta: Servidor Windows 2008 - Windows Servidor 2016
- Gama de níveis funcionais de domínio: Servidor Windows 2008 - Windows Servidor 2016

O Gerenciamento de Identidade (IdM) suporta os seguintes sistemas operacionais:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

6.8. CONFIGURAÇÃO DA DESCOBERTA E AFINIDADE DO SERVIDOR AD

A descoberta do servidor e a configuração de afinidade afetam os servidores do Active Directory (AD) com os quais um cliente de Gerenciamento de Identidade (IdM) se comunica. Esta seção fornece uma visão geral de como a descoberta e a afinidade funcionam em um ambiente com uma confiança florestal cruzada entre IdM e AD.

A configuração dos clientes para preferir servidores na mesma localização geográfica ajuda a evitar atrasos e outros problemas que ocorrem quando os clientes entram em contato com servidores de outro centro de dados remoto. Para garantir que os clientes se comuniquem com os servidores locais, é preciso garantir isso:

- Os clientes se comunicam com servidores locais IdM sobre LDAP e sobre Kerberos
- Os clientes se comunicam com os servidores AD locais através do Kerberos
- Clientes embutidos em servidores IdM comunicam-se com servidores AD locais sobre LDAP e sobre Kerberos

Opções de configuração do LDAP e Kerberos no cliente IdM para comunicação com servidores locais IdM

Ao utilizar IdM com DNS integrado

Por padrão, os clientes utilizam a busca automática de serviços com base nos registros DNS. Nesta configuração, você também pode usar o recurso *DNS locations* para configurar a descoberta de serviços baseados no DNS.
Para anular a busca automática, você pode desativar a descoberta do DNS de uma das seguintes maneiras:

- Durante a instalação do cliente IdM, fornecendo parâmetros de failover a partir da linha de comando
- Após a instalação do cliente, modificando a configuração do System Security Services Daemon (SSSD)

Ao utilizar IdM sem DNS integrado

Você deve configurar explicitamente os clientes de uma das seguintes maneiras:

- Durante a instalação do cliente IdM, fornecendo parâmetros de failover a partir da linha de comando
- Após a instalação do cliente, modificando a configuração do SSSD

Opções de configuração do Kerberos no cliente IdM para comunicação com os servidores AD locais

Os clientes da IdM são incapazes de descobrir automaticamente com quais servidores AD se comunicar. Para especificar os servidores de AD manualmente, modifique o arquivo **krb5.conf**:

- Adicionar as informações do reino AD
- Relacione explicitamente os servidores AD para se comunicar com

Por exemplo:

```
[realms]
AD.EXAMPLE.COM = {
kdc = server1.ad.example.com
kdc = server2.ad.example.com
}
```

Opções para configuração de clientes embarcados em servidores IdM para comunicação com servidores AD locais sobre Kerberos e LDAP

O cliente incorporado em um servidor IdM funciona também como cliente do servidor AD. Ele pode descobrir e usar automaticamente o site AD apropriado.

Quando o cliente incorporado realiza a descoberta, ele pode primeiro descobrir um servidor AD em um local remoto. Se a tentativa de contatar o servidor remoto levar muito tempo, o cliente pode parar a operação sem estabelecer a conexão. Use a opção **dns_resolver_timeout** no arquivo **sssd.conf** do cliente para aumentar o tempo pelo qual o cliente espera uma resposta do resolvedor DNS. Consulte a página de manual *sssd.conf(5)* para maiores detalhes.

Uma vez configurado o cliente incorporado para se comunicar com os servidores AD locais, o SSSD se lembra do site AD ao qual o cliente incorporado pertence. Graças a isto, o SSSD normalmente envia um ping LDAP diretamente a um controlador de domínio local para atualizar as informações de seu site. Se o site não existir mais ou o cliente tiver sido designado para um site diferente, o SSSD começa a procurar por registros SRV na floresta e passa por todo um processo de auto-descoberta.

Usando *trusted domain sections* em **sssd.conf**, você também pode anular explicitamente algumas das informações que são descobertas automaticamente por padrão.

6.9. OPERAÇÕES REALIZADAS DURANTE A INTEGRAÇÃO INDIRETA DA IDM À AD

Tabela 6.2, “Operações realizadas a partir de um controlador de confiança IdM para controladores de domínio AD” mostra quais operações e solicitações são realizadas durante a criação de uma confiança de Gerenciamento de Identidade (IdM) para o Active Directory (AD) do controlador de confiança da IdM para os controladores de domínio AD.

Tabela 6.2. Operações realizadas a partir de um controlador de confiança IdM para controladores de domínio AD

Operação	Protocolo utilizado	Objetivo
Resolução DNS con	DNS	Para descobrir os

Operação	Protocolo utilizado	Objetivo
lvedores DNS AD configurados em um controlador de confi		IP dos controladores de domínio AD

Operação	Protocolo utilizado	Objetivo
Pedidos à porta UDP/UDP 63389 em um ADDC	LDAP sem conexão (CLDAP)	Para realizar a descoberta do ADDC

Operação	Protocolo utilizado	Objetivo
Solicitações às portas TCP/TCP 636 8 9 e 3268 em um ADDC	LDAP	Para consultar informações de usuários e grupos AD

Operação	Protocolo utilizado	Objetivo
Solicitações às portas TCP/TCP 6389 e 32768 em um ADDC	DCE RPC e SMB	Para criar e apoiar a configuração cruzada das fl orestas p

Operação	Protocolo utilizado	Objetivo

Operação	Protocolo utilizado	Objetivo
Pedidos às portas TCP/TCP 6135, 139, 445 e um ADDC	DCE RPC e SMB	Para criar e apoiar a configuração cruzada das florestas p

Operação	Protocolo utilizado	Objetivo
Pedidos de abertura direcionados a uma porta em um ADDC, conforme	DCE RPC e SMB	Para responder às solicitações do mapeador de ponto final a

Operação	Protocolo utilizado	Objetivo
Comunicação do controlador de domínio Active Directory, provavelmente		porta 135 TCP/TCP6)

Operação	Protocolo utilizado	Objetivo
aixa de 49152-65535 (TCP/TCP6)		
Pedidos às portas 88 (T	Kerberos	Para obter um bilhete K

Operação	Protocolo utilizado	Objetivo
DP/UDP6), 464 (TCP/TCP6 e UDP/UDP6), e 749 (TCP/TCP6) e		dar uma senha Kerberos; administrar Kerberos remotam

Operação	Protocolo utilizado	Objetivo

Tabela 6.3, “Operações realizadas a partir de um controlador de domínio AD para controladores de confiança IdM” mostra quais operações e solicitações são realizadas durante a criação de uma confiança IdM para AD do controlador de domínio AD para os controladores de confiança IdM.

Tabela 6.3. Operações realizadas a partir de um controlador de domínio AD para controladores de confiança IdM

Operação	Protocolo utilizado	Objetivo
Resolução DNS contra os resolvedor	DNS	Para descobrir os endereços IP dos c

Operação	Protocolo utilizado	Objetivo
Configurados em um controlador de domínio AD		Usado para configuração de IdM

Operação	Protocolo utilizado	Objetivo
Pedidos à porta UDP/UDP 6389 em um controlador de identificação	CLDAP	Para realizar a descoberta do controlador de confiança

Operação	Protocolo utilizado	Objetivo
Pedidos para as portas TCP/TCP 6135, 139, 445 em um contr	DCE RPC e SMB	Para verificar a conf iança cruzada com a AD

Operação	Protocolo utilizado	Objetivo
Configuração do IdM		
Pedidos de abertura dinâmica de portas em	DCE RPC e SMB	Para responder às solicitações do mapead

Operação	Protocolo utilizado	Objetivo
um controlador fiduciário IdM, conforme orientação do controlad		or de pontos finais DCERPC (porta 135 TCP/TCP6)

Operação	Protocolo utilizado	Objetivo
Do IdM, provavelmente a faixa de 49152-65535 (TCP/TC		

Operação	Protocolo utilizado	Objetivo
Kerberos		Permitir obter um ticket Kerberos; mudar uma senha Kerberos; administrar

Operação	Protocolo utilizado	Objetivo
49 (TCP/TCP6) em um controlador de confiança IdM		Observe remotamente

CAPÍTULO 7. APOIO E RESTAURAÇÃO DO IDM

O Red Hat Enterprise Linux Identity Management fornece uma solução para fazer o backup manual e restaurar o sistema IdM. Isto pode ser necessário após um evento de perda de dados.

Durante o backup, o sistema cria um diretório contendo informações sobre sua configuração de IdM e as armazena. Durante a restauração, você pode usar este diretório de backup para trazer de volta sua configuração original do IdM.

NOTA

Os recursos de backup e restauração da IdM são projetados para ajudar a evitar a perda de dados. Para mitigar o impacto da perda de um servidor e garantir a operação contínua, fornecendo servidores alternativos aos clientes, assegure-se de ter uma topologia de réplica de acordo com Mitigating server loss with replication .

7.1. TIPOS DE BACKUP IDM

Com o utilitário **ipa-backup**, você pode criar dois tipos de backups:

Backup de servidor completo

- **Contains** todos os arquivos de configuração do servidor relacionados ao IdM, e dados LDAP em arquivos LDAP Data Interchange Format (LDIF)
- Os serviços da IdM devem ser **offline**.
- **Suitable for** reconstruindo uma implantação de IdM a partir do zero.

Cópia de segurança somente de dados

- **Contains** Dados LDAP em arquivos LDIF e o changelog de replicação
- Os serviços da IdM podem ser **online or offline**.
- **Suitable for** restaurando dados de IdM a um estado no passado

7.2. CONVENÇÕES DE NOMES PARA ARQUIVOS DE BACKUP DA IDM

Por padrão, a IdM armazena backups como arquivos **.tar** nos subdiretórios do diretório **/var/lib/ipa/backup/**.

Os arquivos e subdiretórios seguem estas convenções de nomenclatura:

Backup de servidor completo

Um arquivo chamado **ipa-full.tar** em um diretório chamado **ipa-full-*<YEAR-MM-DD-HH-MM-SS>***com a hora especificada na hora GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

Cópia de segurança somente de dados

Um arquivo chamado **ipa-data.tar** em um diretório chamado **ipa-data-*<YEAR-MM-DD-HH-MM-SS>***com a hora especificada na hora GMT.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```

NOTA

A desinstalação de um servidor IdM não remove automaticamente nenhum arquivo de backup.

7.3. CONSIDERAÇÕES AO CRIAR UM BACKUP

Esta seção descreve importantes comportamentos e limitações do comando **ipa-backup**.

- Por padrão, o utilitário **ipa-backup** roda em modo offline, o que interrompe todos os serviços da IdM. O utilitário reinicia automaticamente os serviços IdM após a finalização do backup.
- Um backup completo do servidor deve ser executado em **always** com serviços IdM offline, mas um backup somente de dados pode ser executado com serviços online.
- Por padrão, o utilitário **ipa-backup** cria backups no sistema de arquivos contendo o diretório **/var/lib/ipa/backup/**. A Red Hat recomenda criar backups regularmente em um sistema de arquivos separado do sistema de arquivos de produção usado pela IdM, e arquivar os backups em um meio fixo, como fita ou armazenamento óptico.
- Considere a realização de backups em réplicas ocultas. Os serviços da IdM podem ser fechados em réplicas ocultas sem afetar os clientes da IdM.
- A partir do RHEL 8.3.0, o utilitário **ipa-backup** verifica se todos os serviços utilizados em seu cluster IdM, tais como Autoridade Certificadora (CA), Sistema de Nomes de Domínio (DNS) e Agente de Recuperação de Chaves (KRA), estão instalados no servidor onde você está executando o backup. Se o servidor não tiver todos esses serviços instalados, o utilitário **ipa-backup** sai com um aviso, pois os backups realizados nesse host não seriam suficientes para uma restauração completa do cluster.
  Por exemplo, se sua implantação de IdM usa uma Autoridade Certificadora (CA) integrada, uma execução de backup em uma réplica não-CA não capturará os dados da CA. A Red Hat recomenda verificar se a réplica onde você realiza uma **ipa-backup** tem todos os serviços de IdM utilizados no cluster instalados.

  Você pode ignorar a verificação de funções do servidor IdM com o comando **ipa-backup --disable-role-check**, mas o backup resultante não conterá todos os dados necessários para restaurar completamente o IdM.

7.4. CRIANDO UM BACKUP IDM

Esta seção descreve como criar um servidor completo e backup somente de dados nos modos off-line e on-line usando o comando **ipa-backup**.

Pré-requisitos

- Você deve ter **root** privilégios para executar o utilitário **ipa-backup**.

Procedimento

- Para criar um backup completo do servidor em modo offline, use o utilitário **ipa-backup** sem opções adicionais.

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- Para criar uma cópia de segurança offline apenas de dados, especifique a opção **--data**.

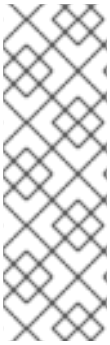
```
[root@server ~]# ipa-backup --data
```

- Para criar um backup completo do servidor que inclua arquivos de log IdM, use a opção **--logs**.

```
[root@server ~]# ipa-backup --logs
```

- Para criar um backup somente de dados enquanto os serviços da IdM estão sendo executados, especifique as opções **--data** e **--online**.

```
[root@server ~]# ipa-backup --data --online
```



NOTA

Se o backup falhar devido a espaço insuficiente no diretório /**tmp**, use a variável de ambiente **TMPDIR** para alterar o destino dos arquivos temporários criados pelo processo de backup:

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

Para obter mais detalhes, consulte o Comando ipa-backup Falha em Concluir .

Passos de verificação

- O diretório de backup contém um arquivo com o backup.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

7.5. CRIAÇÃO DE BACKUPS CRIPTOGRAFADOS DE IDM

Você pode criar backups criptografados usando a criptografia GNU Privacy Guard (GPG). Para criar backups criptografados IdM, você precisará primeiro criar uma chave GPG2.

7.5.1. Criação de uma chave GPG2 para criptografia de backups IdM

O procedimento a seguir descreve como gerar uma chave GPG2 para a utilidade **ipa-backup**.

Procedimento

1. Instalar e configurar o utilitário **pinentry**.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. Crie um arquivo **key-input** usado para gerar um par de chaves GPG com seus detalhes preferidos. Por exemplo:

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: IPA Backup
Name-Comment: IPA Backup
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. Por padrão, o GPG2 armazena seu chaveiro no arquivo **~/.gnupg**. Para usar um local personalizado do chaveiro, defina a variável de ambiente **GNUPGHOME** para um diretório acessível apenas pela raiz.

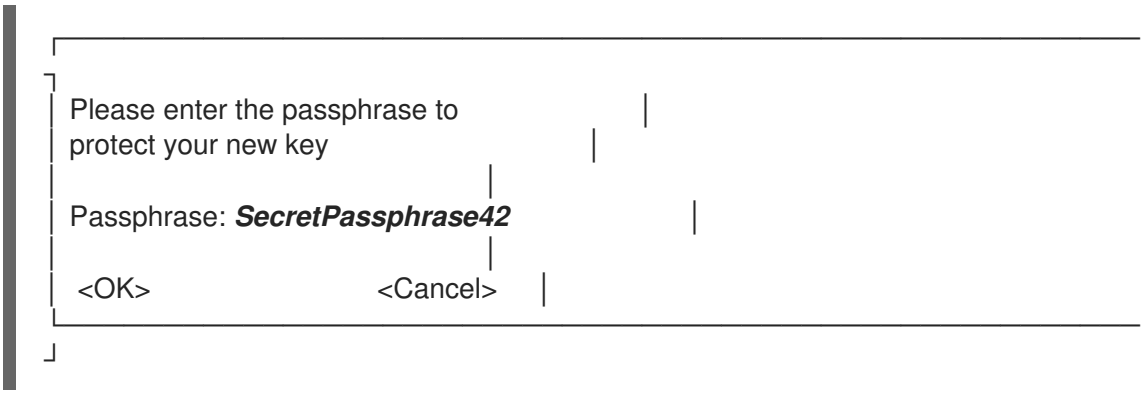
```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Comece a gerar uma nova chave GPG2 baseada no conteúdo de **key-input**.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

   a. Insira uma frase-chave para proteger a chave GPG2.



   b. Confirme a senha correta digitando-a novamente.

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: SecretPassphrase42                       │
│                                                      │
│  <OK>                          <Cancel>              │
└──────────────────────────────────────────────────────┘
```

c. A nova chave GPG2 é agora criada.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

Passos de verificação

- Liste as chaves GPG no servidor.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] IPA Backup (IPA Backup) <root@example.com>
```

Recursos adicionais

- Para mais informações sobre criptografia GPG e seus usos, consulte o site da GNU Privacy Guard.

7.5.2. Criação de um backup criptografado GPG2 IdM

O procedimento a seguir cria um backup IdM e o codifica usando uma chave GPG2.

Pré-requisitos

- Você criou uma chave GPG2. Veja Criando uma chave GPG2 para criptografar backups IdM .

Procedimento

- Crie um backup criptografado por GPG especificando a opção **--gpg**.

```
[root@server ~]# ipa-backup --gpg
```

```
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

Passos de verificação

- Certifique-se de que o diretório de backup contenha um arquivo criptografado com uma extensão de arquivo **.gpg**.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

Recursos adicionais

- Para informações gerais sobre como criar um backup, consulte Criando um backup.

7.6. QUANDO RESTAURAR A PARTIR DE UM BACKUP IDM

Você pode responder a vários cenários de desastre restaurando a partir de um backup IdM:

- **Undesirable changes were made to the LDAP content** As entradas foram modificadas ou excluídas, a replicação dessas mudanças foi realizada durante todo o desdobramento, e você deseja reverter essas mudanças. A restauração de um backup somente de dados retorna as entradas LDAP ao estado anterior sem afetar a configuração do IdM em si.
- **Total Infrastructure Loss, or loss of all CA instances** Se um desastre danificar todas as réplicas da Autoridade Certificadora, a implantação perdeu a capacidade de se reconstruir por meio da implantação de servidores adicionais. Nesta situação, restaurar um backup de uma Réplica CA e construir novas réplicas a partir dela.
- **An upgrade on an isolated server failed** O sistema operacional permanece funcional, mas os dados do IdM estão corrompidos, e é por isso que você quer restaurar o sistema IdM a um bom estado conhecido. A Red Hat recomenda trabalhar com Suporte Técnico a fim de diagnosticar e solucionar o problema. Se esses esforços falharem, restaure a partir de um servidor de backup completo.

IMPORTANTE

A solução preferida para falha de hardware ou atualização é reconstruir o servidor perdido a partir de uma réplica. Para mais informações, consulte Recuperando da perda do servidor com replicação .

7.7. CONSIDERAÇÕES AO RESTAURAR A PARTIR DE UM BACKUP IDM

Se você tiver um backup criado com o utilitário **ipa-backup**, você pode restaurar seu servidor IdM ou o conteúdo LDAP para o estado em que se encontravam quando o backup foi realizado.

As considerações a seguir são as principais, ao restaurar a partir de um backup IdM:

- Você só pode restaurar um backup em um servidor que corresponda à configuração do servidor onde o backup foi originalmente criado. O servidor **must** tem:
  - O mesmo hostname
  - O mesmo endereço IP
  - A mesma versão do software IdM
- Se um servidor IdM em um ambiente multi-mestre é restaurado, o servidor restaurado torna-se a única fonte de informação para a IdM. Todos os outros servidores mestre **must** serão reinicializados a partir do servidor restaurado.
- Como qualquer dado criado após o último backup será perdido, não use a solução de backup e restauração para manutenção normal do sistema.
- Se um servidor for perdido, a Red Hat recomenda a reconstrução do servidor, reinstalando-o como uma réplica, em vez de restaurá-lo a partir de um backup. A criação de uma nova réplica preserva os dados do ambiente de trabalho atual. Para mais informações, consulte Preparação para perda do servidor com replicação.
- Os recursos de backup e restauração só podem ser gerenciados a partir da linha de comando e não estão disponíveis na interface web do IdM.
- Você não pode restaurar a partir de arquivos de backup localizados nos diretórios **/tmp** ou **/var/tmp**. O Servidor de Diretórios IdM usa um diretório **PrivateTmp** e não pode acessar os diretórios **/tmp** ou **/var/tmp** comumente disponíveis para o sistema operacional.

DICA

A restauração a partir de um backup requer as mesmas versões de software (RPM) no host de destino que foram instaladas quando o backup foi realizado. Devido a isto, a Red Hat recomenda a restauração a partir de um instantâneo da máquina virtual em vez de um backup. Para mais informações, consulte Recuperando da perda de dados com instantâneos de VM .

7.8. RESTAURANDO UM SERVIDOR IDM A PARTIR DE UM BACKUP

O procedimento seguinte descreve a restauração de um servidor IdM, ou seus dados LDAP, a partir de um backup IdM.

Figura 7.1. Topologia de Replicação utilizada neste exemplo

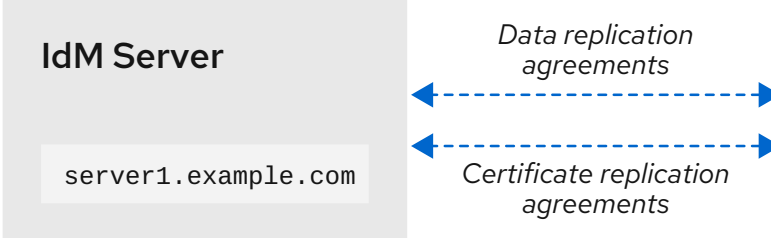


Tabela 7.1. Convenções de nomenclatura de servidores usadas neste exemplo

Nome do host do servidor	Função
server1.example.com	O servidor que precisa ser restaurado a partir do backup.
caReplica2.example.com	Uma réplica da Autoridade Certificadora (CA) conectada ao host **server1.example.com**.
replica3.example.com	Uma réplica conectada ao host **caReplica2.example.com**.

Pré-requisitos

- Você gerou um backup completo do servidor IdM ou apenas de dados com o utilitário **ipa-backup**. Veja Criando uma cópia de segurança .
- Seus arquivos de backup não estão nos diretórios **/tmp** ou **/var/tmp**.
- Antes de executar uma restauração do servidor completo a partir de um backup do servidor completo, desinstale o IdM do servidor e reinstale o IdM usando a mesma configuração do servidor anterior.

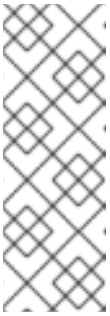
Procedimento

1. Use o utilitário **ipa-restore** para restaurar um servidor completo ou uma cópia de segurança somente de dados.
   - Se o diretório de backup estiver no local padrão **/var/lib/ipa/backup/**, digite apenas o nome do diretório:

     ```
     [root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
     ```

   - Se o diretório de backup não estiver no local padrão, digite seu caminho completo:

     ```
     [root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
     ```

     NOTA

     O utilitário **ipa-restore** detecta automaticamente o tipo de backup que o diretório contém, e executa o mesmo tipo de restauração por padrão. Para executar uma restauração somente de dados a partir de um backup de servidor completo, adicione a opção **--data** a **ipa-restore**:

     ```
     [root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
     ```

2. Digite a senha do Gerenciador de Diretório.

   ```
   Senha do gerenciador de diretórios (master existente):
   ```

3. Digite **yes** para confirmar a sobreposição dos dados atuais com o backup.

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. O utilitário **ipa-restore** desabilita a replicação em todos os servidores que estão disponíveis:

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

O utilitário então pára os serviços da IdM, restaura o backup, e reinicia os serviços:

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

5. Reinicializar todas as réplicas conectadas ao servidor restaurado:

   a. Liste todos os segmentos de topologia de replicação para o sufixo **domain**, tomando nota dos segmentos de topologia que envolvem o servidor restaurado.

```
[root@server1 ~]# ipa topologysegment-find domain
------------------
2 segments matched
------------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both

  Segment name: caReplica2.example.com-to-replica3.example.com
  Left node: caReplica2.example.com
  Right node: replica3.example.com
  Connectivity: both
```

```
----------------------------
Number of entries returned 2
----------------------------
```

b. Re-inicializar o sufixo **domain** para todos os segmentos de topologia com o servidor restaurado.
Neste exemplo, faça uma reinicialização de **caReplica2** com dados de **server1**.

```
[root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
Update in progress, 2 seconds elapsed
Update succeeded
```

c. Passando aos dados da Autoridade Certificadora, liste todos os segmentos de topologia de replicação para o sufixo **ca**.

```
[root@server1 ~]# ipa topologysegment-find ca
-----------------
1 segment matched
-----------------
  Segment name: server1.example.com-to-caReplica2.example.com
  Left node: server1.example.com
  Right node: caReplica2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------
```

d. Re-inicializar todas as réplicas CA conectadas ao servidor restaurado.
Neste exemplo, realize uma reinicialização do site **csreplica caReplica2** com dados de **server1**.

```
[root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
from=server1.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

6. Continue movendo-se para fora através da topologia de replicação, reinicializando sucessivas réplicas, até que todos os servidores tenham sido atualizados com os dados do servidor restaurado **server1.example.com**.
Neste exemplo, basta reinicializar o sufixo **domain** em **replica3** com os dados de **caReplica2**:

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. Limpar o cache do SSSD em cada servidor a fim de evitar problemas de autenticação devido a dados inválidos:

a. Parar o serviço SSSD:

```
[root@server ~]# systemctl stop sssd
```

b. Remover todo o conteúdo armazenado em cache do SSSD:

```
[root@server ~]# sss_cache -E
```

c. Iniciar o serviço SSSD:

```
[root@server ~]# systemctl start sssd
```

d. Reinicialize o servidor.

Recursos adicionais

- A página de manual **ipa-restore**(1) também cobre em detalhes como lidar com cenários complexos de replicação durante a restauração.

7.9. RESTAURANDO A PARTIR DE UM BACKUP CRIPTOGRAFADO

O utilitário **ipa-restore** detecta automaticamente se um backup IdM está criptografado, e o restaura usando o chaveiro raiz GPG2 e **gpg-agent** por padrão.

Pré-requisitos

- Uma cópia de segurança criptografada GPG IdM. Veja Criando backups criptografados de IdM .
- A senha do LDAP Directory Manager
- O **Passphrase** usado ao criar a chave GPG

Procedimento

1. Se você usou um local personalizado de chaveiro ao criar as chaves GPG2, certifique-se de que a variável de ambiente **$GNUPGHOME** esteja definida para esse diretório. Consulte Criando uma chave GPG2 para criptografar backups IdM.

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. Forneça ao utilitário **ipa-restore** a localização do diretório de backup.

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

a. Digite a senha do Gerenciador de Diretório.

```
Senha do gerenciador de diretórios (master existente):
```

b. Digite o endereço **Passphrase** que você usou ao criar a chave GPG.

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
```

```
| "IPA Backup (IPA Backup) <root@example.com>"                |
| 2048-bit RSA key, ID BF28FFA302EF4557,                      |
| created 2020-01-13.                                         |
|                                                             |
|                                                             |
| Passphrase: SecretPassPhrase42                              |
|                                                             |
|       <OK>                          <Cancel>                |
└─────────────────────────────────────────────────────────────
```

3. Reinicializar todas as réplicas conectadas ao servidor restaurado. Ver Restauração de um servidor IdM a partir do backup.