Versão 2.8.0.0

Technical Support Appliance
Guia de configuração

Nota

Antes de usar essas informações e o produto suportado por elas, leia as informações em “Avisos” na página 141.

Vigésima quarta edição (janeiro de 2021)

Esta edição se aplica à versão 2, liberação 8, modificação 0 do IBM® Technical Support Appliance e a todas as liberações e modificações subsequentes até que seja indicado o contrário em novas edições.

Índice

Figuras

Capítulo 1. Introdução

O Technical Support Appliance (TSA) é uma ferramenta fácil de usar que permite obter mais valor dos seus contratos do Suporte IBM. O TSA descobre os principais elementos de tecnologia da informação e seus relacionamentos na sua infraestrutura de TI e transmite os dados com segurança para o Suporte IBM para análise. Esses dados fornecem ao Suporte IBM insights sobre os relacionamentos complexos entre aplicativos, middleware, servidores e componentes de rede em seu data center.

O TSA inclui uma interface com o usuário (UI) baseada na web para configurar e customizar o acesso ao seu sistema e aos dados. A interface com o usuário também permite modificar planejamentos para descoberta e transmissão de dados.

Como parte do processo de descoberta, o TSA tenta detectar inicialmente terminais no escopo definido sem usar credenciais de descoberta. Isso envolve o uso do Nmap e tenta descobrir e classificar dispositivos com varredura intrusiva mínima de IP, impressões digitais de pilhas e mapeamento de portas. Geralmente, essa atividade não é significativa o suficiente para acionar um sistema de detecção de intrusão (IDS), porém, isso poderá ocorrer se houver configurações locais rigorosas.

Os conjuntos de escopos gerais permitem descobrir elementos individuais da rede de TI. O conjunto de escopos contém um ou mais escopos que identificam o local desses elementos de rede usando um endereço IP ou nome de host, um intervalo de endereços IP ou uma rede ou sub-rede.

Para HMCs e servidores VMware vCenter/ESXi, o uso de conjuntos de escopos dinâmicos é recomendado. Os conjuntos de escopos dinâmicos requerem muito menos esforço de configuração no TSA em comparação com a criação e o gerenciamento de escopos de descoberta para LPARs/máquinas virtuais individuais. Além disso, os conjuntos de escopos dinâmicos podem lidar com ambientes nos quais as LPARs ou máquinas virtuais são incluídas e excluídas ao longo do tempo sem a necessidade de nenhuma modificação.

Contas do usuário e grupos de usuários

Executar qualquer função do TSA requer um determinado nível de autoridade. Se um usuário autenticado tentar executar uma função sem o nível de autoridade apropriado, um erro será exibido e a função não será executada.

Dentro de uma organização, podem ser criados cargos para várias funções de trabalho. As permissões para executar determinadas operações são atribuídas a funções específicas. Usuários do TSA recebem funções específicas, e por meio dessas atribuições de função, têm as permissões necessárias para executar determinadas funções do sistema. Dessa forma, qualquer usuário atribuído a uma função terá os níveis de autoridade associados a essa função e será fácil incluir um usuário em uma função, mudar usuários de uma função para outra ou remover usuários de uma função.

No TSA, as funções são gerenciadas com grupos de usuários que possuem níveis de autoridade associados. Os usuários são gerenciados com contas de usuário. É possível atribuir associações a contas de usuário em um ou mais grupos de usuários e, por meio dessas associações, os usuários têm o nível de autoridade para executar funções específicas.

Além disso, os grupos de usuários podem ficar mais restritos aos conjuntos de escopos selecionados. Um conjunto de escopos é uma coleção de endereços IP ou nomes de host, intervalos de endereços ou sub-redes que identificam os elementos de TI que o TSA pode descobrir. Especificar restrições do conjunto de escopos para um grupo de usuários é uma maneira de limitar ainda mais o acesso dos membros desse grupo de usuários. Por exemplo, é possível criar grupos de usuários específicos da plataforma, como usuários responsáveis por manter os sistemas Linux®, através de uma combinação de restrições de nível de autoridade e conjunto de escopos associadas a um determinado grupo de usuários.

Escopos de descoberta e conjuntos de escopos

Os escopos de descoberta identificam os recursos que você deseja que o TSA descubra. Os escopos de descoberta são agrupados em conjuntos de escopos de descoberta.

É possível especificar escopos de descoberta usando um endereço IP ou nome de host, um intervalo de endereços IP ou uma rede ou sub-rede para definir os recursos que são acessados durante a descoberta. Um escopo de descoberta pode ser tão pequeno quanto um único endereço IP ou nome de host ou tão grande quanto um intervalo de endereços IP ou uma rede.

Para simplificar a criação de um conjunto de escopos, é possível usar um arquivo para importar uma lista contendo endereços IP e nomes de host. Para obter mais informações, consulte a seção "Importando um conjunto de escopos" na página 74.

Quanto mais endereços IP houver no escopo da descoberta, maior será a duração da descoberta. É possível modificar o tamanho da descoberta desativando ou ativando conjuntos de escopos de descoberta ou excluindo endereços IP, intervalos de endereços IP ou redes e sub-redes de um escopo dentro de um conjunto de escopos.

Nota: Para melhorar o desempenho, limite o número acumulativo de endereços IP (endereço IP, intervalos, sub-redes e exclusões) em um conjunto de escopos a 400 ou menos.

Nota: Escopos ou listas de importação que são definidas com nomes de host têm o nome do host resolvido para um endereço IP quando o escopo é criado ou editado. O TSA não usa o nome do host ao descobrir recursos da rede.

Tarefas relacionadas

Incluindo contas de usuário e grupos de usuários
É possível incluir contas e grupos de usuários para controlar o acesso às funções do TSA.

Credenciais de descoberta

As credenciais de descoberta são uma coleção de nomes de usuário, senhas ou chaves SSH e sequências de comunidades de Protocolo Simples de Gerenciamento de Rede (SNMP) que o TSA usa para acessar recursos durante a descoberta.

Deve-se configurar e manter credenciais de descoberta para os recursos que você deseja descobrir. As informações de acesso que você fornece variam de acordo com o tipo de credencial, mas geralmente incluem pelo menos nome de usuário e senha ou chave SSH.

Uma credencial de descoberta pode se aplicar a todos os conjuntos de escopos ou ser restrita a um único conjunto de escopos. Definir credenciais que se aplicam a um único conjunto de escopos melhora o desempenho e evita tentativas inválidas de login, o que pode resultar no bloqueio da conta.

Quando você acessa um recurso, o TSA usa sequencialmente cada credencial associada a um escopo específico na ordem listada na página **Credenciais de descoberta** até que o recurso habilite a permissão do TSA a acessá-lo. Por exemplo, quando você está acessando um sistema de computador, o TSA usa o primeiro nome de usuário e a senha especificados na lista de credenciais para sistemas de computador e que estão associados ao conjunto de escopos que o contém. Se o nome de usuário e a senha estiverem incorretos para um sistema de computador específico, o TSA usará automaticamente o próximo nome de usuário e senha especificados na lista de credenciais para sistemas de computador.

Dica: Antes de salvar as credenciais, é possível testar se você especificou credenciais válidas para os tipos de sistema, como **Sistema de computador**, **Sistema de computador (Windows)**, **SNMP** ou **SNMPV3**. Com esse teste, é possível garantir que as credenciais sejam definidas de forma válida.

Dica:

- Use uma conta de serviço com uma senha comum para todos os dispositivos de um determinado tipo, como AIX ou Windows. Uma única credencial pode ser definida para descobrir todas as instâncias desse tipo de dispositivo.
- Use contas com senhas que não expiram.

- Use chaves SSH, sempre que necessário.

Planejamento de descoberta

As descobertas são executadas em dias e horários planejados para garantir que os dados descobertos sejam sempre atuais e precisos. O TSA tem um planejamento padrão de "Descoberta Completa" que descobre todos os conjuntos de escopos definidos. Esse planejamento padrão pode ser modificado de acordo com suas necessidades. Também é possível criar planejamentos que permitam que a descoberta de conjuntos de escopos seja distribuída entre diferentes datas e horas. Também é possível visualizar os detalhes, o histórico e o estado da última descoberta que foi executada.

Ao modificar um planejamento de descoberta, especifique o nome, os conjuntos de escopos, a hora de início e a frequência das descobertas. Se o planejamento de descoberta for a descoberta padrão, será possível modificar apenas o horário de início e a frequência das descobertas. Também será possível executar descobertas sob demanda.

A duração da descoberta depende de vários fatores, que também incluem o número e a complexidade dos recursos e pode levar até 72 horas para ser concluída.

Planejamento de transmissão

Os dados descobertos são empacotados e transmitidos com segurança para o Suporte IBM nos dias e horários planejados para garantir que a IBM tenha as informações mais atuais e precisas. O TSA tem um planejamento de transmissão padrão que pode ser modificado para as suas necessidades. Também é possível executar transmissões sob demanda. Também é possível visualizar o estado da última transmissão que foi executada.

O tempo decorrido para uma transmissão varia dependendo da quantidade de dados descobertos.

Capítulo 2. Pré-requisitos

Para configurar e usar o TSA, é necessário garantir que você atenda aos pré-requisitos, como ter as credenciais necessárias para o ambiente de descoberta e os requisitos de configuração para conectar-se ao Suporte IBM.

Fazer download da imagem do TSA

As imagens do TSA estão disponíveis para os servidores Microsoft Hyper-V [*TSA-HYPERV-<version>*] e VMware [*TSA-VMWARE-<version>*] .

É possível obter instruções de download em: https://ibm.biz/TSAdemo

Requisitos para TSA

Antes de configurar e usar o TSA, verifique se você atende aos seguintes pré-requisitos.

Hardware x86 de 64 bits
O TSA deve ser carregado em sistemas x86 de 64 bits.

Hypervisor
O TSA requer o VMware ESXi ou o Microsoft Hyper-V

Nota: Use apenas versões do ESXi ou Hyper-V que são atualmente suportada pelo fabricante.

Processador
O TSA requer no mínimo um processador de quatro núcleos, 2.26 GHz.

CPU
O TSA requer quatro CPUs de 64 bits.

Memória
O TSA requer memória de 16 GB.

Dispositivo de armazenamento de acesso direto (DASD)
O TSA requer 150 GB de DASD.

Rede
O TSA requer um adaptador Ethernet de 1 Gigabit.

Navegadores da web obrigatórios

Uma interface com o usuário baseada na web é usada para configurar e monitorar a descoberta e a transmissão.

O TSA suporta os seguintes navegadores da Internet:

- Mozilla Firefox V78.4.0 Extended Support Release (ESR)
- Microsoft Edge V86.0.622.56 for Windows 10
- Google Chrome V86.0.4240.111 (64 bits)

É possível fazer download desses navegadores nos seguintes sites:

- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Microsoft Edge (https://www.microsoft.com/en-us/edge)
- Google Chrome (https://support.google.com/chrome/answer/95346?hl=en)

Requisitos de configuração para conexões com o Suporte IBM

O TSA pode conectar-se ao Suporte IBM através de uma conexão direta ou através de um proxy fornecido pelo usuário que deve ser configurado para permitir a comunicação com a IBM. Se você estiver usando um proxy, a inspeção TLS/SSL não será suportada. Qualquer solicitação por meio de um proxy deve ser permitida para fluir diretamente para a IBM sem terminação TLS/SSL.

Certifique-se de que seu firewall permita conexões com o nome do host e os endereços IP do servidor IBM, conforme explicado na tabela Conexões de rede. Se sua rede não permitir acesso aos servidores IBM, as transações do TSA para o Suporte IBM falharão.

Tabela 1. Conexões de rede

Nome DNS	Endereço IP	Porta	Protocolo
esupport.ibm.com	129.42.54.189	443	HTTPS (para a IBM)
	129.42.56.189		
	129.42.60.189		

O ambiente do servidor IBM é totalmente compatível com o NIST SP800-131A, suportando o protocolo TLS 1.2, o SHA-256 ou funções de hash mais fortes e chaves de força RSA com pelo menos 2048 bits.

Nota: A inspeção SSL não é suportada ao utilizá-la no proxy. Desative-a para esses fluxos.

Para proxies Blue Coat, desative a "detecção de protocolo" nos servidores IBM. Inclua estas regras de configuração:

- url.domain=esupport.ibm.com detect_protocol (nenhum)
- url.address=129.42.54.189 detect_protocol (nenhum)
- url.address=129.42.56.189 detect_protocol (nenhum)
- url.address=129.42.60.189 detect_protocol (nenhum)

Credencial e requisitos de software para o ambiente de descoberta

Para descobrir terminais ou recursos de descoberta em seu ambiente, o TSA deve ter acesso a esses recursos. É recomendado criar uma conta de serviço em cada recurso especificamente para o TSA usar ao acessar esse recurso.

Depois de criar uma conta de serviço em um recurso, deve-se definir e manter credenciais no TSA que correspondam às credenciais definidas no recurso para essa conta de serviço. O TSA usa essas credenciais para acessar o recurso. Os requisitos para credenciais variam de acordo com o ambiente e o tipo de recurso que você deseja descobrir, mas geralmente incluem um nome de usuário e senha ou chave SSH. Alguns recursos têm requisitos de software específicos também.

Tipo de credencial	Informações de acesso
Sistema de computador	**Nome do usuário:** Nome do usuário para acessar o dispositivo. **Senha/Passphrase:** A senha/passphrase para acessar o dispositivo. **Tipo de autenticação:** O tipo de autenticação para o dispositivo. • **Senha**: use a senha fornecida. • **PKI**: use a chave SSH associada com o conjunto de escopos específico.

Tipo de credencial	Informações de acesso
Sistema de computador (Windows)	**Nome do usuário:** Nome de usuário para acessar o sistema de computador Windows. **Senha:** A senha para acessar o sistema de computador Windows.
Elemento de rede (SNMP)	**Sequência de comunidades:** A sequência de comunidade para o dispositivo.
Elemento de rede (SNMPV3)	**Nome do usuário:** O nome do usuário para acessar o dispositivo. **Senha:** A senha para acessar o dispositivo. **Senha privada:** A senha que será usada se a criptografia de dados for configurada para SNMP. **Protocolo de autenticação:** O tipo do protocolo de autenticação usado pelo SNMP. • Nenhum • MD5 • SHA
Outro (dispositivo Cisco)	**Nome do usuário:** O nome do usuário para acessar o dispositivo Cisco. **Senha:** A senha do dispositivo Cisco. **Senha de ativação:** A senha de ativação para o dispositivo Cisco.
Outro (Cisco Works)	**Nome do usuário:** O nome do usuário para acessar o servidor CiscoWorks. **Senha:** A senha para acessar o servidor CiscoWorks.

Nota: Para obter mais informações sobre credenciais e requisitos de software, consulte o Guia do assistente de configuração.

Capítulo 3. Instalando o Technical Support Appliance

O TSA inclui software pré-instalado. Ele é empacotado e distribuído como uma imagem para instalações VMware ou como uma imagem VHDX para instalações do Microsoft Hyper-V. Para VMware, é possível instalar o TSA usando a interface da web do VMware (para ESXi). Para o Hyper-V, o TSA pode ser instalado usando o Hyper-V Manager. Esta seção fornece as etapas para instalar o TSA usando qualquer um desses métodos.

Instalando usando interface da web do VMware ESXi

Antes de Iniciar

O TSA requer que o VMware ESXi 6.5 ou superior seja carregado para controlar o hardware.

Sobre Esta Tarefa

Siga estas etapas para instalar a imagem do TSA.

Procedimento

1. Efetue login para se conectar ao sistema ESXi por meio da interface da web do VMware ESXi.
2. Clique em **Criar/Registrar VM**. O assistente **Nova máquina virtual** é exibido.

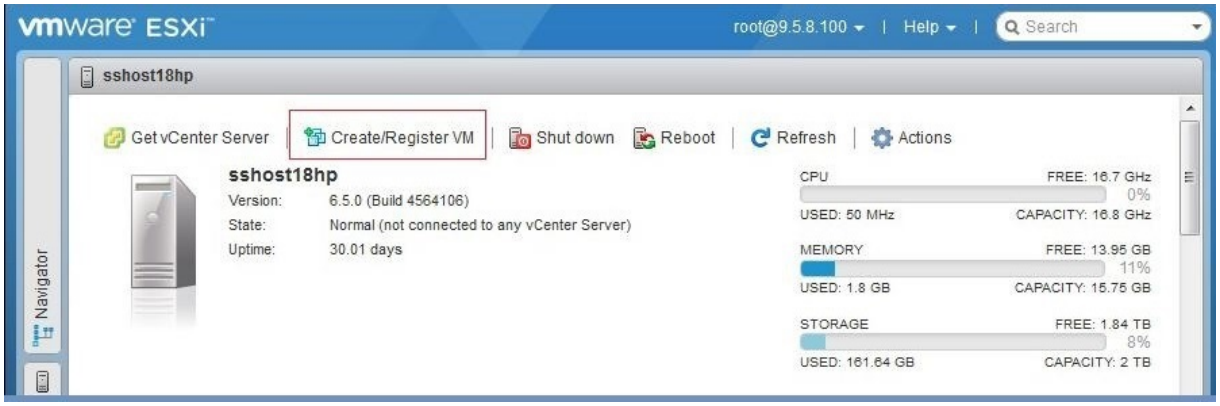

Figura 1. Criar/Registrar VM

3. Na tela **Selecionar tipo de criação**, selecione a opção **Implementar uma máquina virtual por meio de um arquivo OVF ou OVA** e clique em **Avançar**.

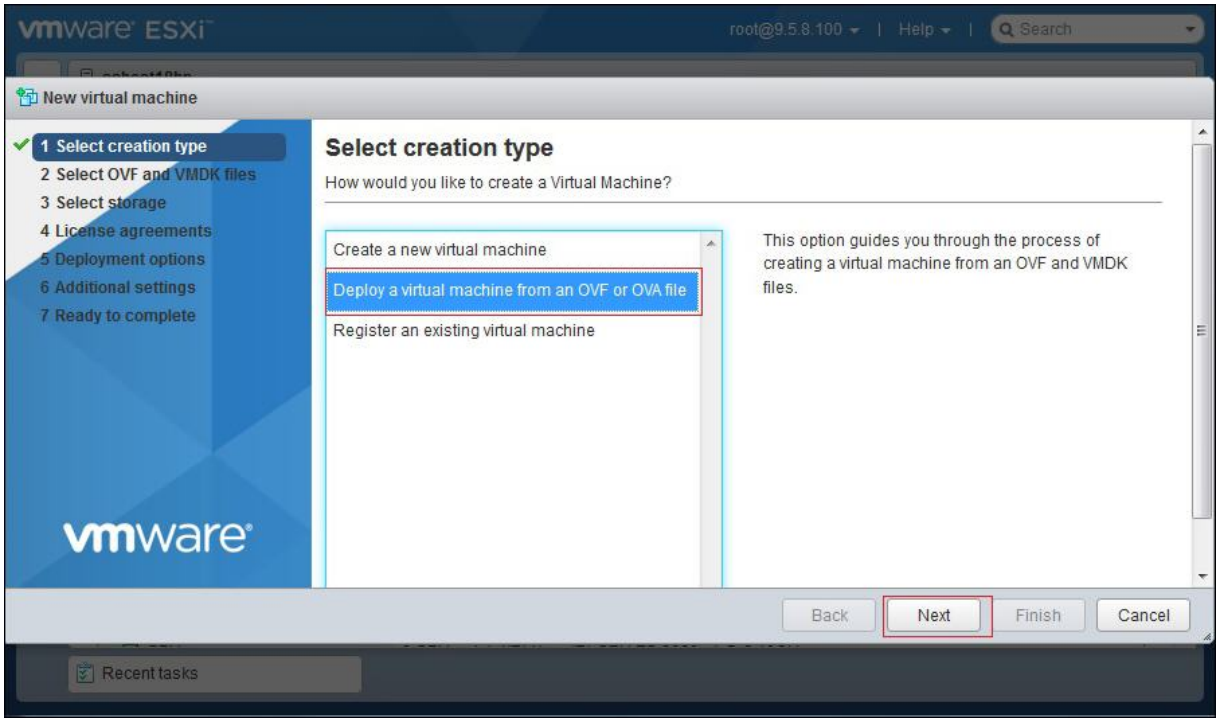

Figura 2. Selecionar tipo de criação

4. Na tela de arquivos **Selecionar OVF e VMDK**, clique dentro da caixa **Clicar para selecionar arquivos ou arrastar e soltar** e selecione o arquivo de imagem transferido por download do Fix Central. Insira um nome exclusivo para sua máquina virtual ou use o valor padrão, em seguida, clique em **Avançar**.

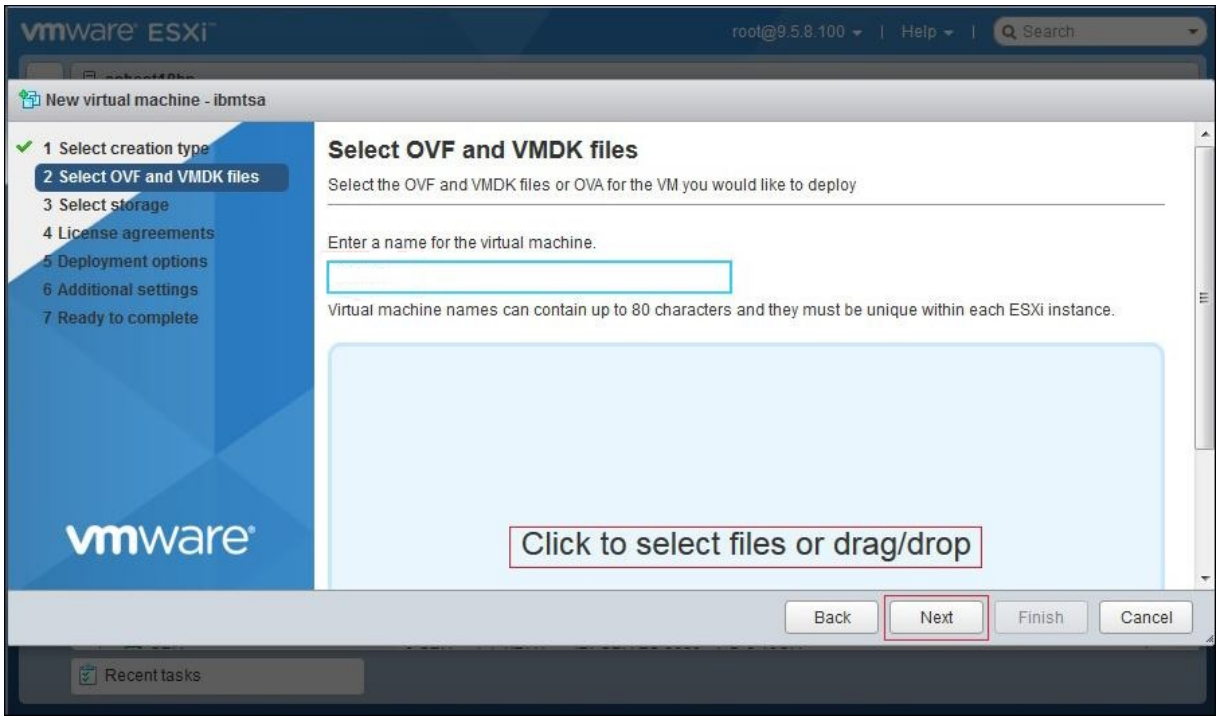

Figura 3. Selecionar os arquivos OVF e VMDK

5. Na tela **Selecionar armazenamento**, na lista exibida, selecione um armazenamento de dados no qual armazenar os arquivos de configuração e disco. Em seguida, clique em **Avançar**.

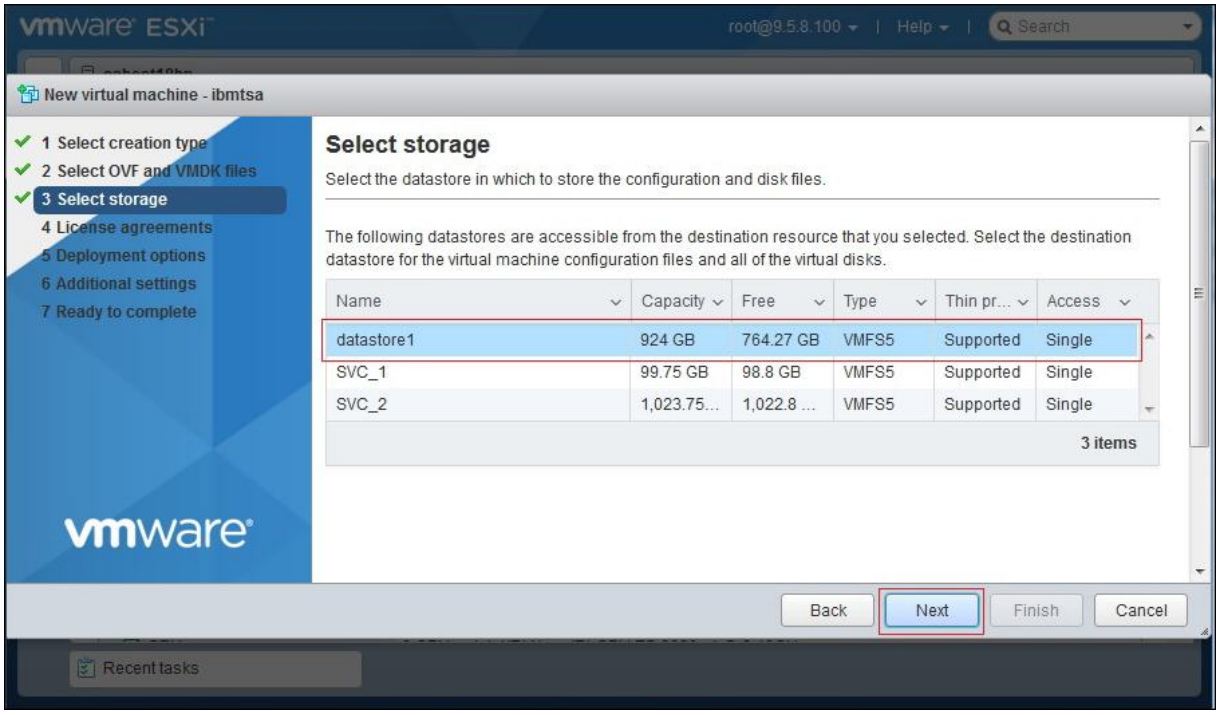

Figura 4. Selecionar armazenamento

6. Na tela **Opções de implementação**, selecione mapeamentos de rede na lista suspensa **Rede da VM**.

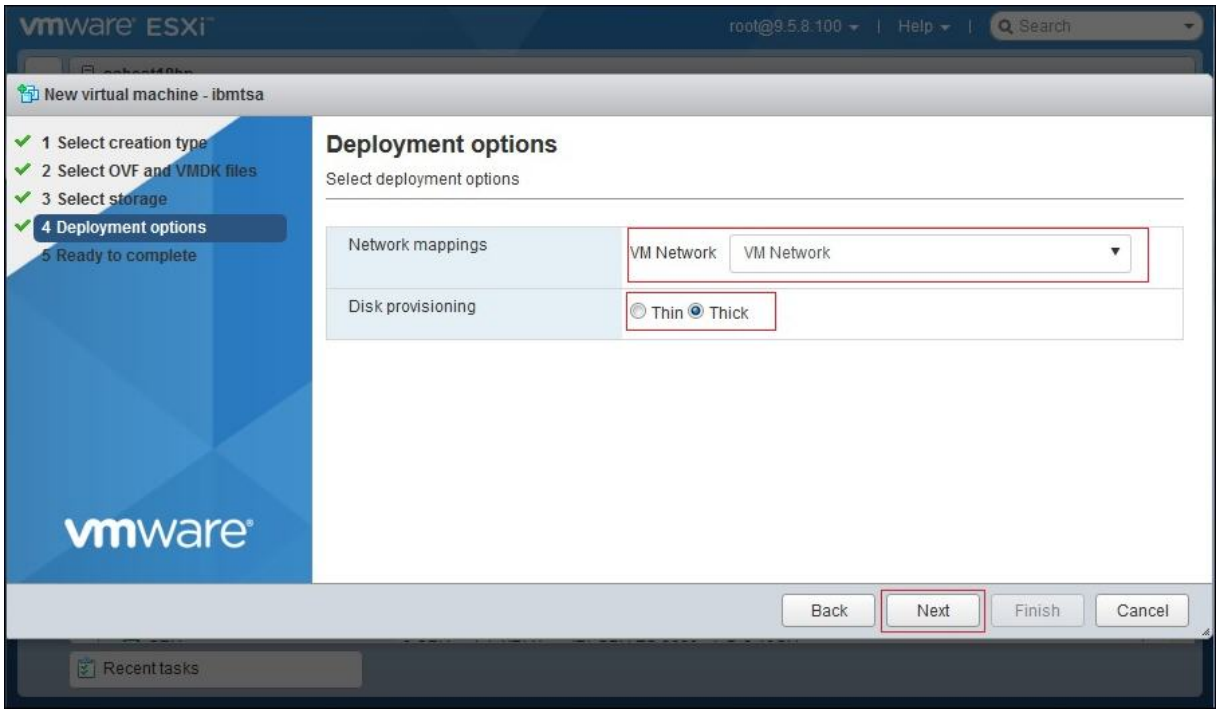

Figura 5. Opções de implementação

7. Selecione a opção **Thick** para o provisionamento de disco e, em seguida clique em **Avançar**.
8. Na tela **Pronto para conclusão**, revise todas as configurações especificadas. Se você quiser fazer mudanças, clique em **Voltar** e faça as mudanças nas opções relevantes. Se você estiver satisfeito, clique em **Concluir**.

Importante: Não atualize seu navegador enquanto a máquina virtual estiver sendo implementada.

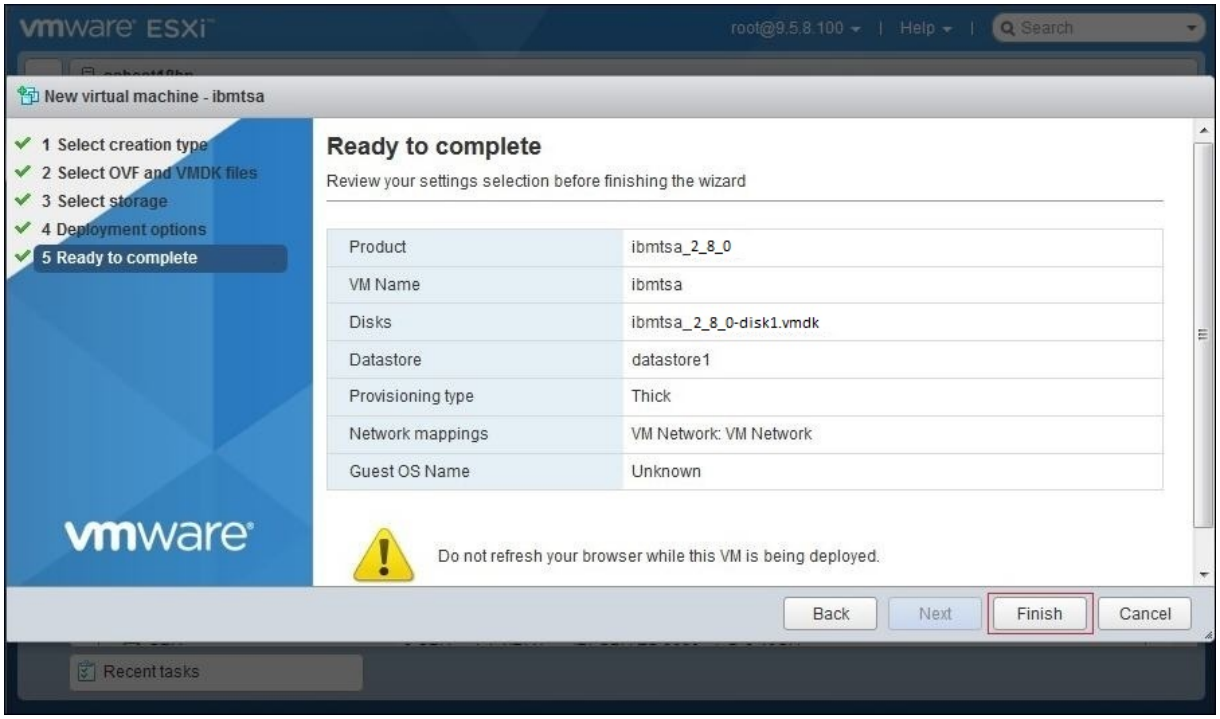

Figura 6. Revise a seleção de configurações

A máquina virtual do TSA está instalada em seu sistema.

9. No console do TSA, insira o **ibmtsa login** como **`tsausr`** e **Senha** como **`configTsa`**.
10. Necessário: Para mudar a senha de login, continue com as etapas listadas na seção "Mudando a senha tsausr (obrigatório)" na página 19.
11. Para concluir a instalação, continue com as etapas listadas na seção "Configurando os detalhes da rede" na página 19.

Instalando o TSA no Microsoft Hyper-V

Antes de Iniciar

Antes de configurar e usar o TSA no Hyper-V, assegure-se de atender aos seguintes pré-requisitos.

- Hyper-V Server 2016 ou 2019
- Hyper-V Manager
- O Virtual Network Switch foi criado por meio do Hyper-V Manager

Sobre Esta Tarefa

Siga estas etapas para instalar o TSA no Hyper-V.

Procedimento

Para instalar o TSA no Hyper-V, siga estas etapas:

1. Após fazer download da imagem do TSA, extraia o arquivo *ibmtsa_2800.vhdx* do arquivo *ibmtsa_2800.zip* do ibmtsa_2800.zip e mova-o para um diretório no servidor Hyper-V.
2. Incie o Hyper-V Manager e conecte ao servidor Hyper-V a partir do sistema do cliente.
3. Clique em **Procurar** e selecione a imagem que é salva em seu sistema.

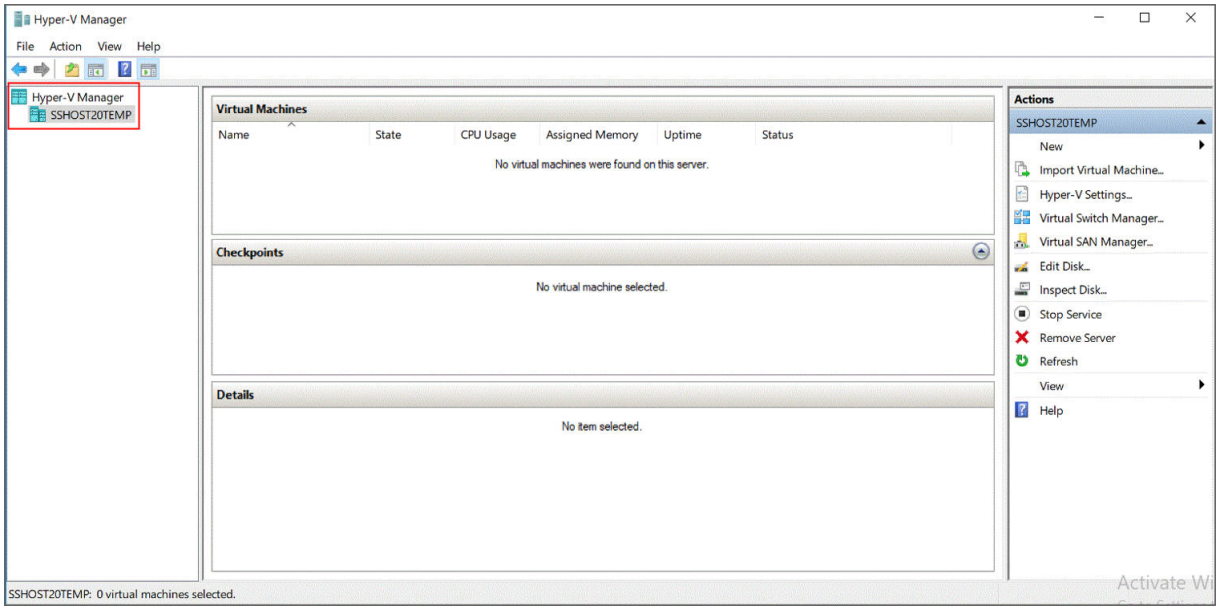

Figura 7. Hyper-V Manager

4. No menu **Ação**, selecione **Novo** → **Máquina virtual**. O **Novo assistente da máquina virtual** é exibido.
5. Insira o **Nome** para a nova máquina virtual e clique em **Avançar**.

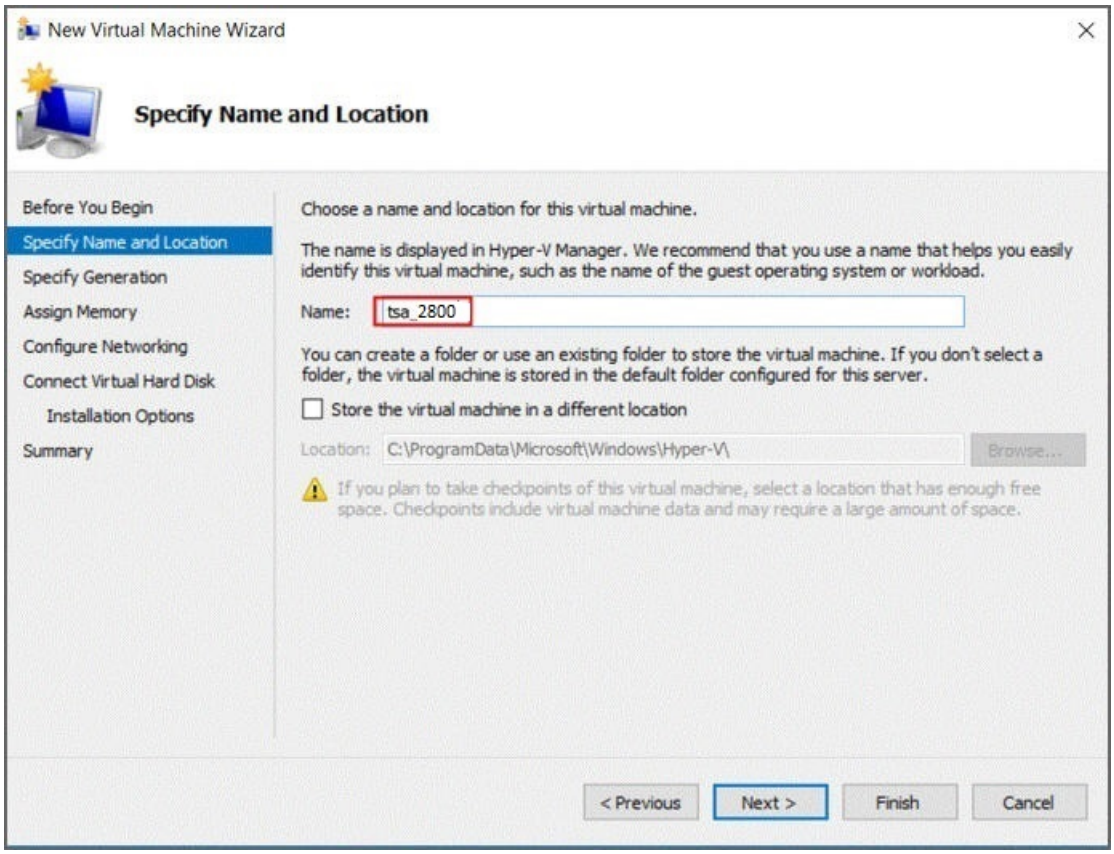

Figura 8. Nome da máquina virtual

6. Selecione **Geração 1** como a geração da máquina virtual e clique em **Avançar**.

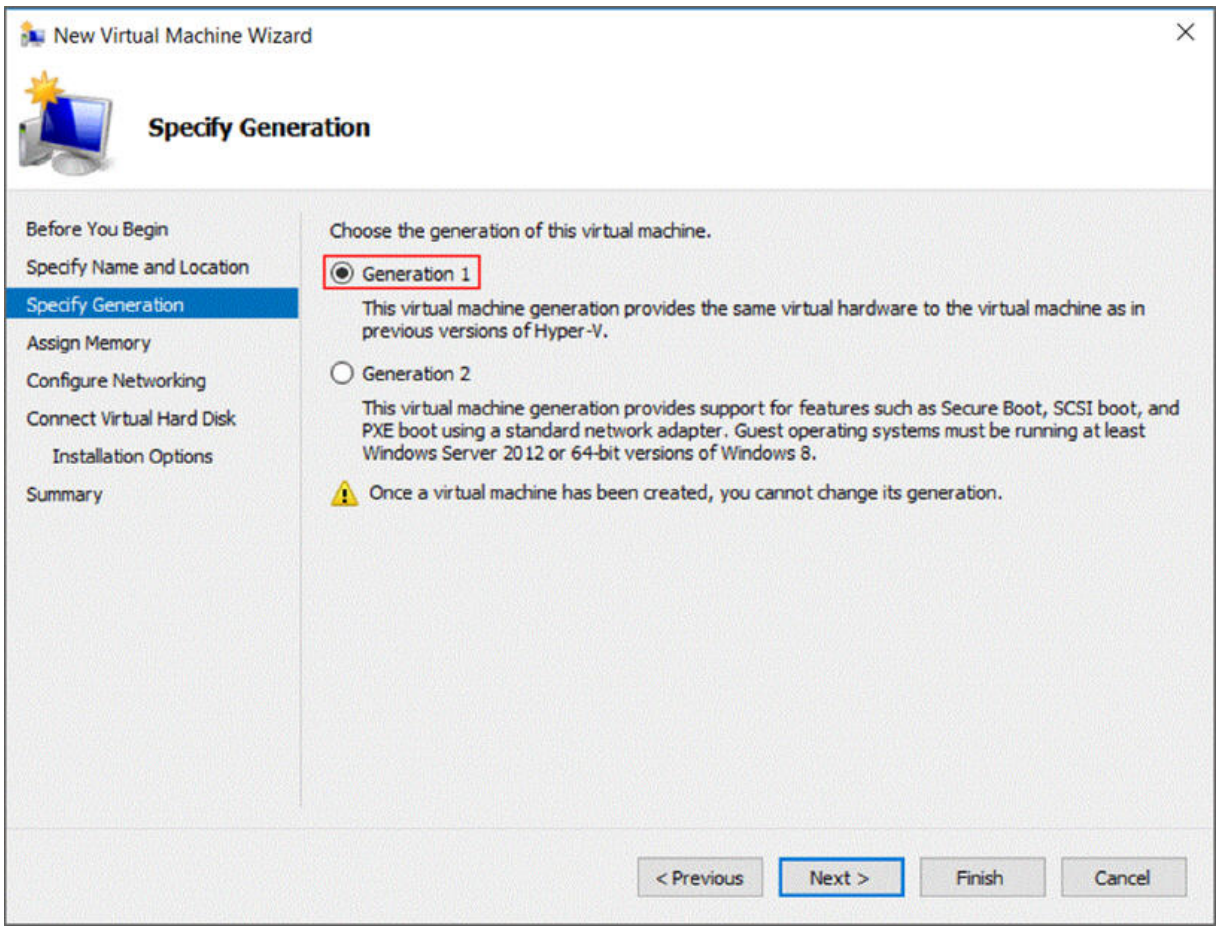

Figura 9. Especifique a geração

7. Insira **Memória da inicialização** como *16384* MB e clique em **Avançar**.

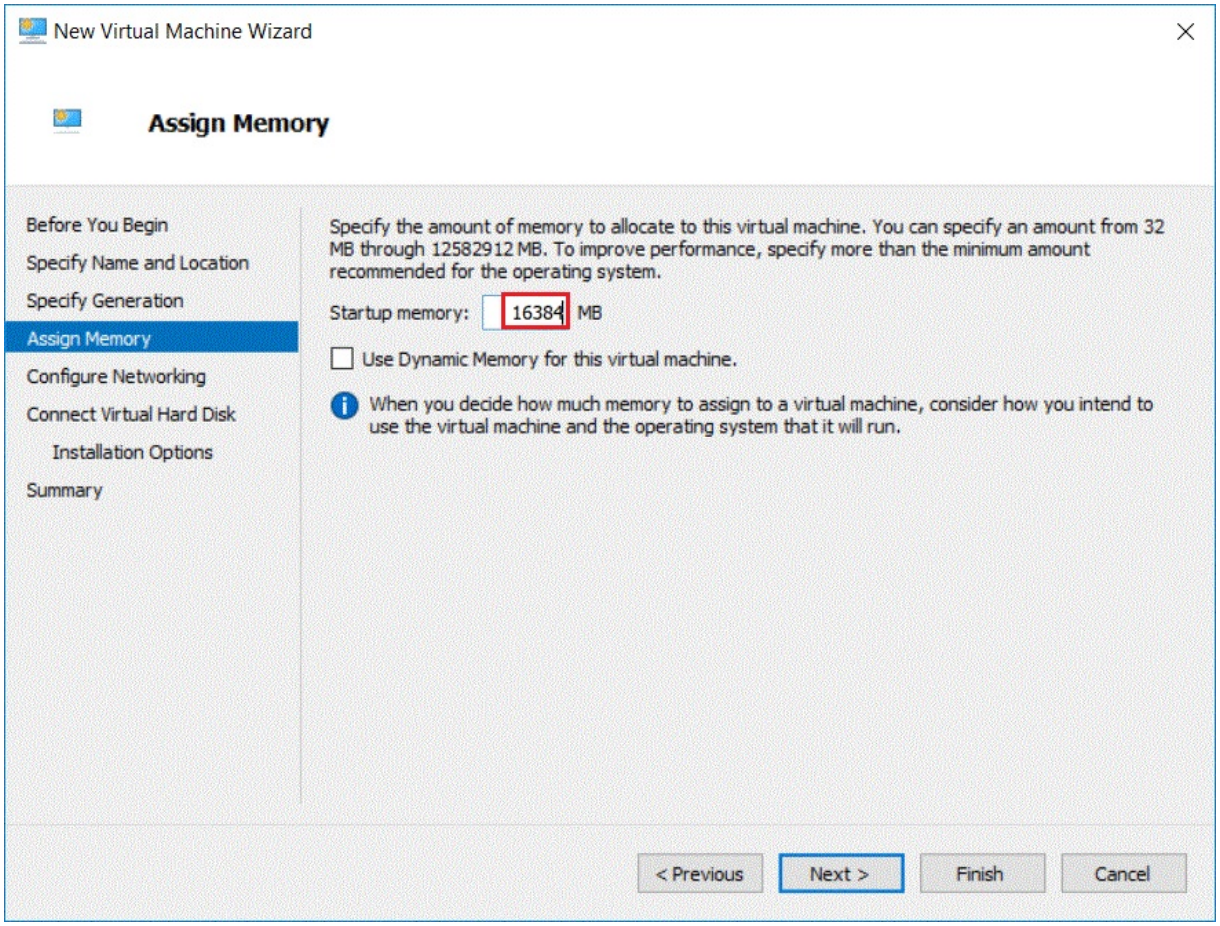

Figura 10. Memória da inicialização

8. Selecione um comutador virtual pré-configurado e clique em **Avançar**.

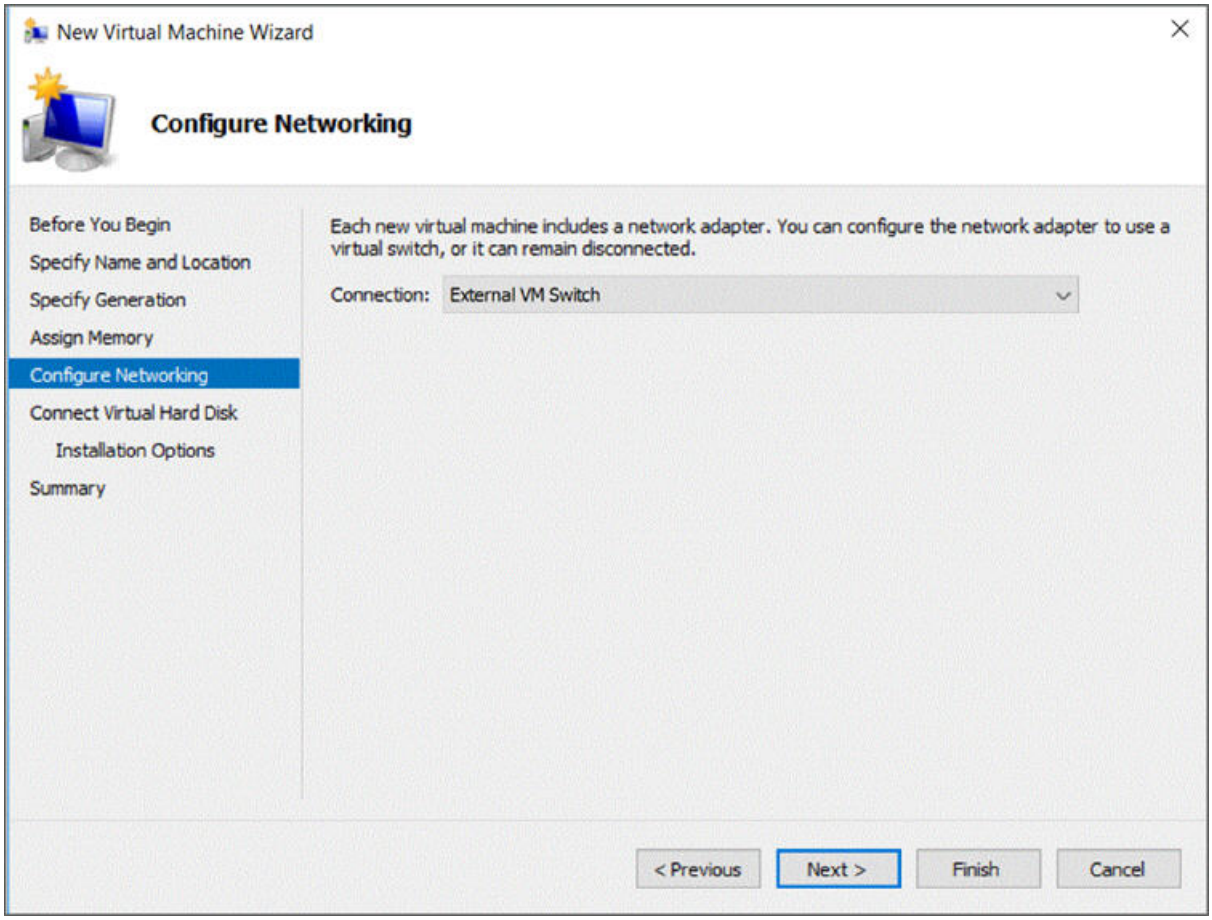

Figura 11. Configurar a rede

9. Selecione a opção **Usar um disco rígido virtual** e procure o arquivo *ibmtsa_2800.vhdx* copiado para o servidor Hyper-V na Etapa 2 e clique em **Avançar**.

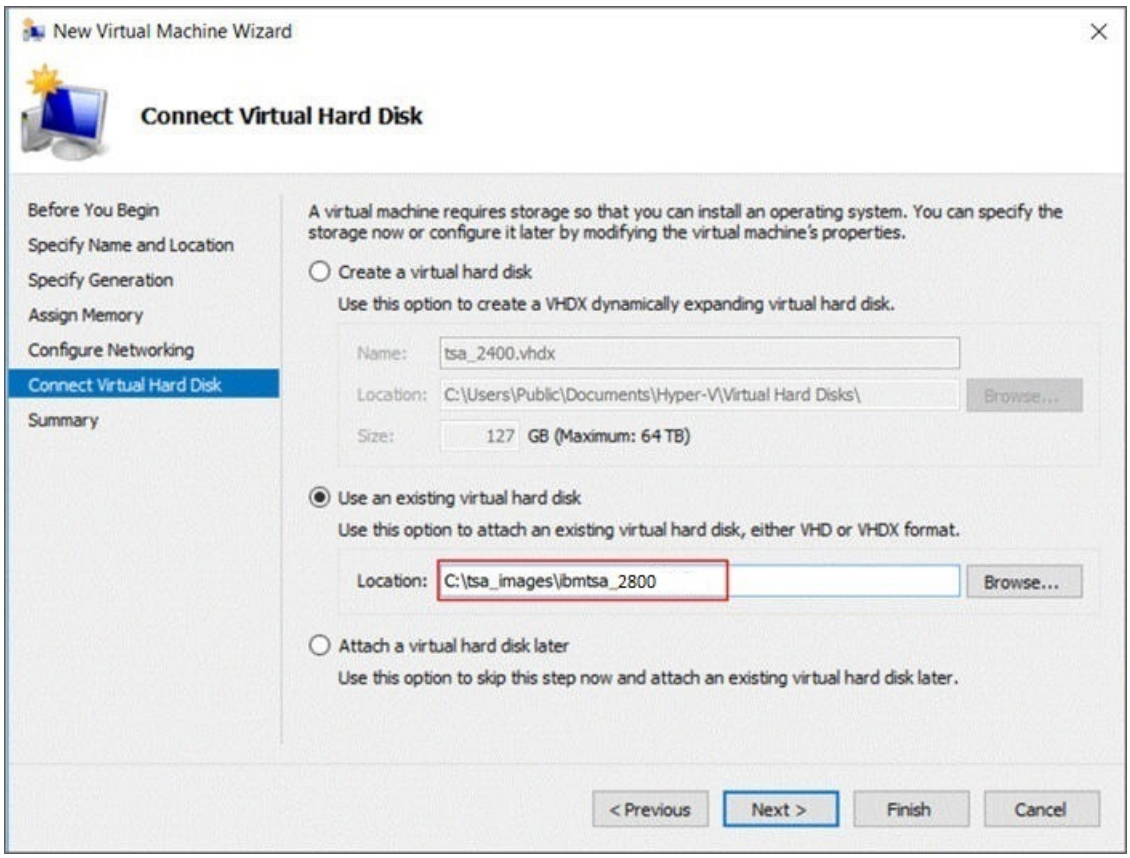

Figura 12. Conectar disco rígido virtual

10. Na página **Resumo**, revise as configurações e clique em **Concluir**.

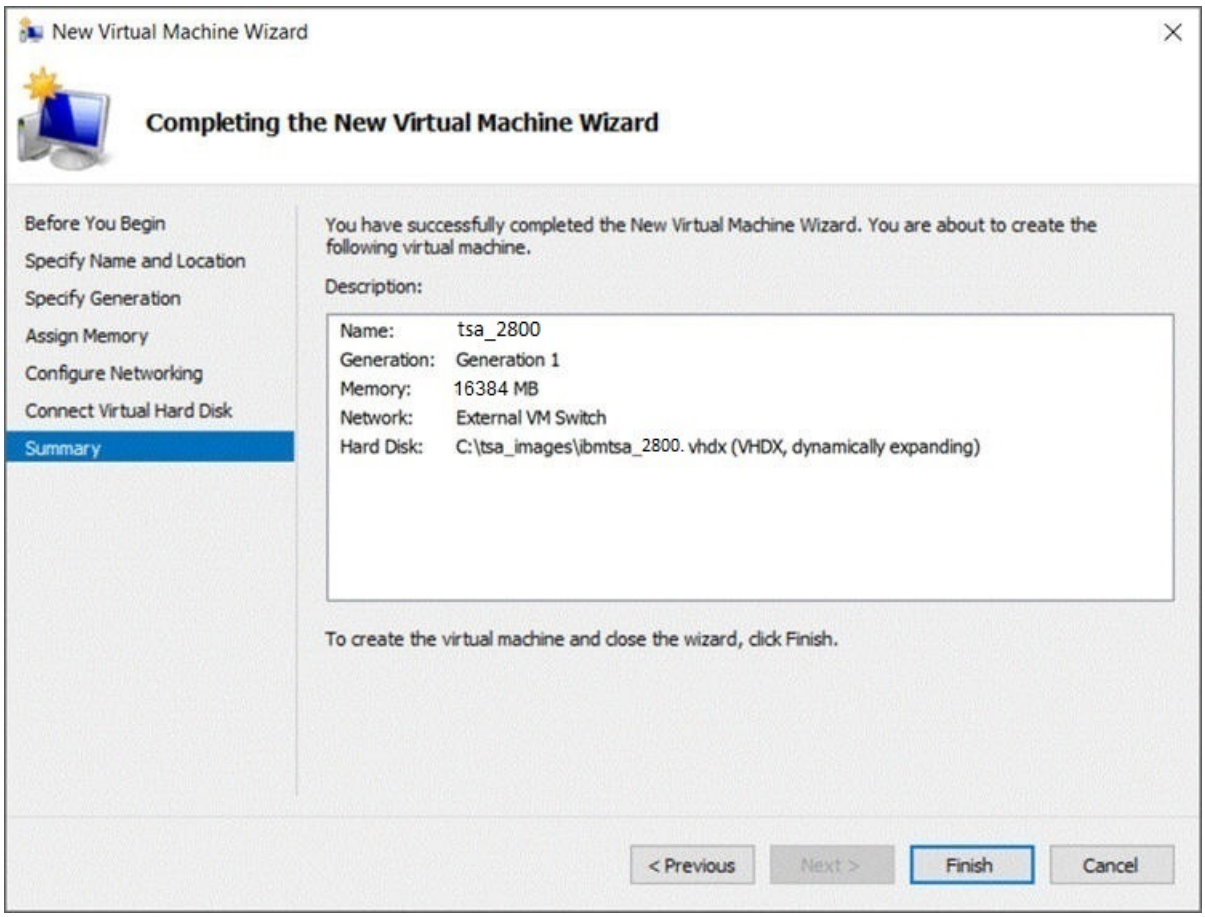

Figura 13. Resumo

11. A nova máquina virtual é incluída no Hyper-V Manager. Selecione a máquina virtual, vá para o menu **Ação** e clique em **Iniciar**.

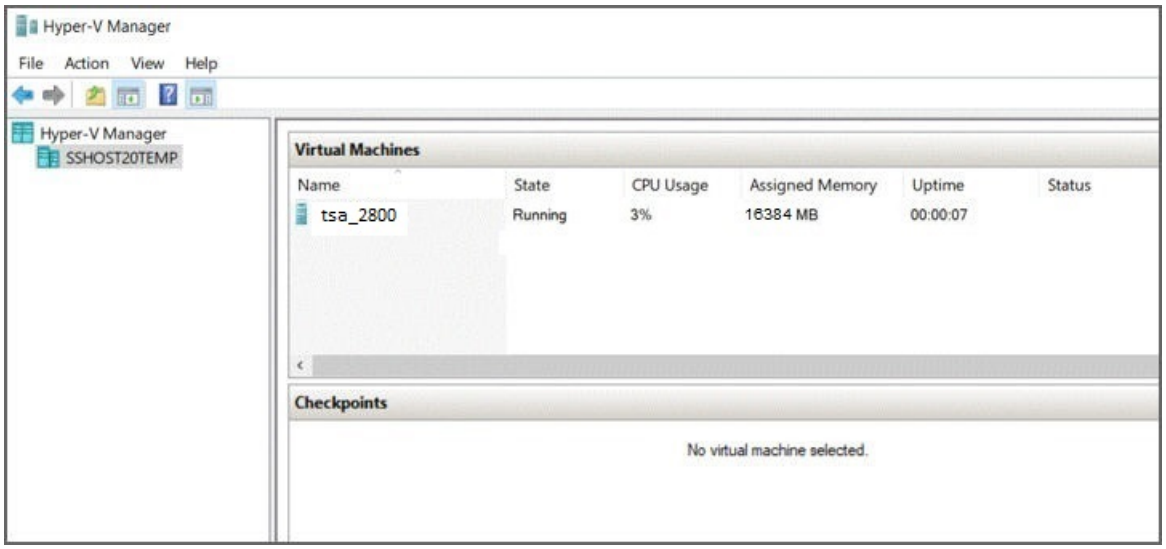

Figura 14. Hyper-V Manager

12. No menu **Ação**, selecione **Conectar** para iniciar uma sessão do console. No console do TSA, insira o **ibmtsa login** como **`tsausr`** e **Senha** como **`configTsa`**.
13. Necessário: Para mudar a senha de login, continue com as etapas listadas na seção "Mudando a senha tsausr (obrigatório)" na página 19.
14. Para concluir a instalação, continue com as etapas listadas na seção "Configurando os detalhes da rede" na página 19.

Mudando a senha *tsausr* (obrigatório)

Por motivos de segurança, é recomendável que a senha do *tsausr* seja mudada do seu valor inicial. Siga estas etapas para mudar a senha *tsausr*.

Procedimento

1. Selecione a opção **2) Mudar a senha tsausr** no **Menu de configuração do TSA**.

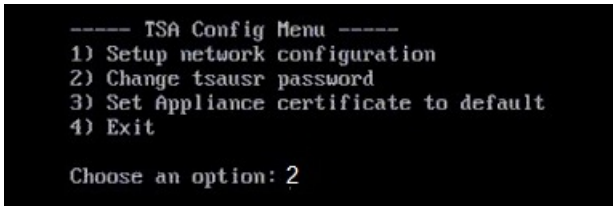

Figura 15. Mudar senha

2. Insira a nova senha no prompt **Nova senha**. Insira a mesma senha no prompt **Digitar novamente a nova senha**. A nova senha deve ter pelo menos sete caracteres.

Figura 16. Nova senha

Configurando os detalhes da rede

Procedimento

1. Selecione a opção **1) Definir a configuração da rede** no **Menu de configuração do TSA**.

Figura 17. Definir a configuração de rede

2. Insira os detalhes da configuração de rede seguinte.

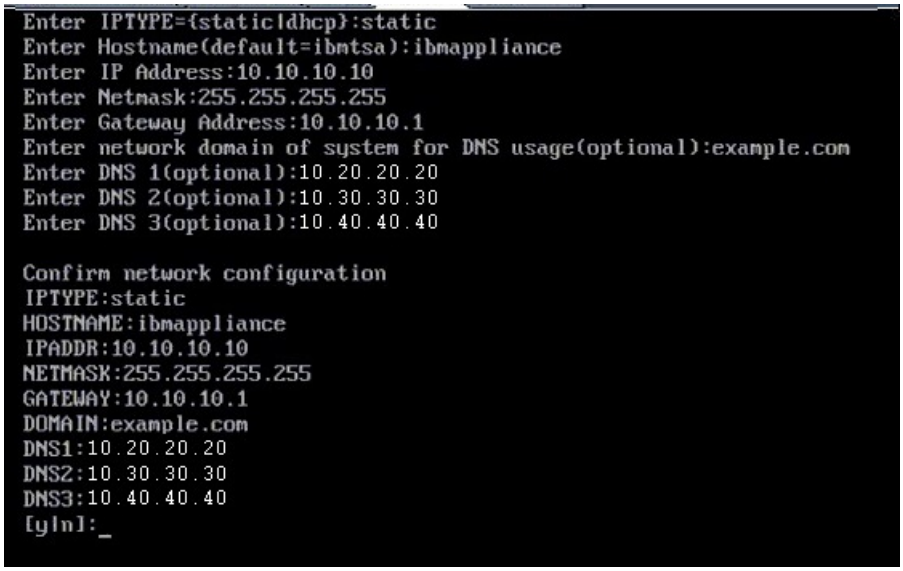

Figura 18. Configuração de rede

a) **Insira IPTYPE = {static|dhcp}**. Insira `static` ou `dhcp`. Se `static`, siga estas etapas; caso contrário, siga as etapas de configuração `dhcp` na seção Apêndice B, “Configurando os detalhes de rede do DHCP”, na página 129

IPTYPE: static

`Enter Hostname(default=ibmtsa)`. É possível mudar o nome do host padrão. Assegure-se de que o nome do host usado seja exclusivo.

`Enter IP Address`.

`Enter Netmask` e **`Enter Gateway`**.

`Enter network domain of system for DNS usage (optional)`.

`Enter DNS 1(optional)`, **`Enter DNS 2(optional)`** e **`Enter DNS 3(optional)`**.

Os detalhes de configuração de rede especificados são exibidos para confirmação.

b) Insira **[y|n]** para confirmar ou descartar a configuração de rede. Inserir **y** salva a configuração de rede e reinicia o sistema automaticamente.

Nota: Para qualquer configuração incorreta, é possível mudar os detalhes. Insira **n** para ignorar as configurações atuais e reiniciar a configuração na etapa “2.a” na página 20

c) O sistema reinicia em 15 segundos para que a nova configuração de rede entre em vigor.

d) Acesse o TSA no navegador usando HTTP seguro com o nome do host ou endereço IP que é inserido acima.
Por exemplo, `https://<hostname | IP address>.`

Nota: Na primeira conexão, seu navegador pode exibir uma exceção de segurança. Deve-se aceitar o certificado de segurança e continuar efetuando login no TSA.

Nota: Para modificar as configurações básicas de rede do TSA por meio da interface do usuário, siga as etapas em “Definindo configurações básicas de rede” na página 34. Para definir as configurações avançadas de rede, siga as etapas em “Definindo as configurações de rede avançada” na página 36.

3. Configure o Technical Support Appliance usando as etapas listadas em Capítulo 4, “Configurando o Technical Support Appliance”, na página 21

Resultados

Depois de configurar com sucesso o TSA, consulte Capítulo 5, “Configurando a descoberta a transmissão para a IBM”, na página 49

Capítulo 4. Configurando o Technical Support Appliance

Sobre Esta Tarefa

Siga estas etapas para começar a usar o TSA rapidamente. Se você ainda não fez isso, revise Capítulo 2, “Pré-requisitos”, na página 5.

Procedimento

1. “Efetuando login no Technical Support Appliance” na página 21
2. “Aceitando o Contrato de Licença” na página 23
3. “Usando o assistente de configuração para configuração inicial” na página 25
   a) “Configurando o IBM Connectivity” na página 25
   b) “Registrando o Technical Support Appliance” na página 27
   c) “Configurando o clock” na página 29
   d) “Configurando o planejamento de transmissão” na página 31
   e) “Atualizando o Technical Support Appliance” na página 32
4. “Definindo as configurações de rede” na página 33
5. “Configurando os certificados” na página 42.
6. Opcional: Apêndice C, “Contas do usuário e grupos de usuários”, na página 131

O que Fazer Depois

Quando terminar de configurar o TSA, consulte Capítulo 5, “Configurando a descoberta a transmissão para a IBM”, na página 49 para obter informações sobre como executar outras tarefas.

Efetuando login no Technical Support Appliance

Procedimento

1. Abra um navegador da Internet usando um sistema com acesso à rede para o TSA.
   Para obter mais informações, consulte “Navegadores da web obrigatórios” na página 5.
2. Insira a seguinte URL na barra de endereços do navegador:

   ```
   https://<hostname or IP address>
   ```

   Nota: Se o `<hostname>` não funcionar, tente o endereço IP atribuído do TSA.
3. Quando solicitado, insira as seguintes informações:

   ID do usuário:
   Insira `admin`

   Senha:
   Insira a senha do administrador do TSA.

   A senha inicial é `passw0rd`. Deve-se mudar essa senha inicial após efetuar logon no TSA.

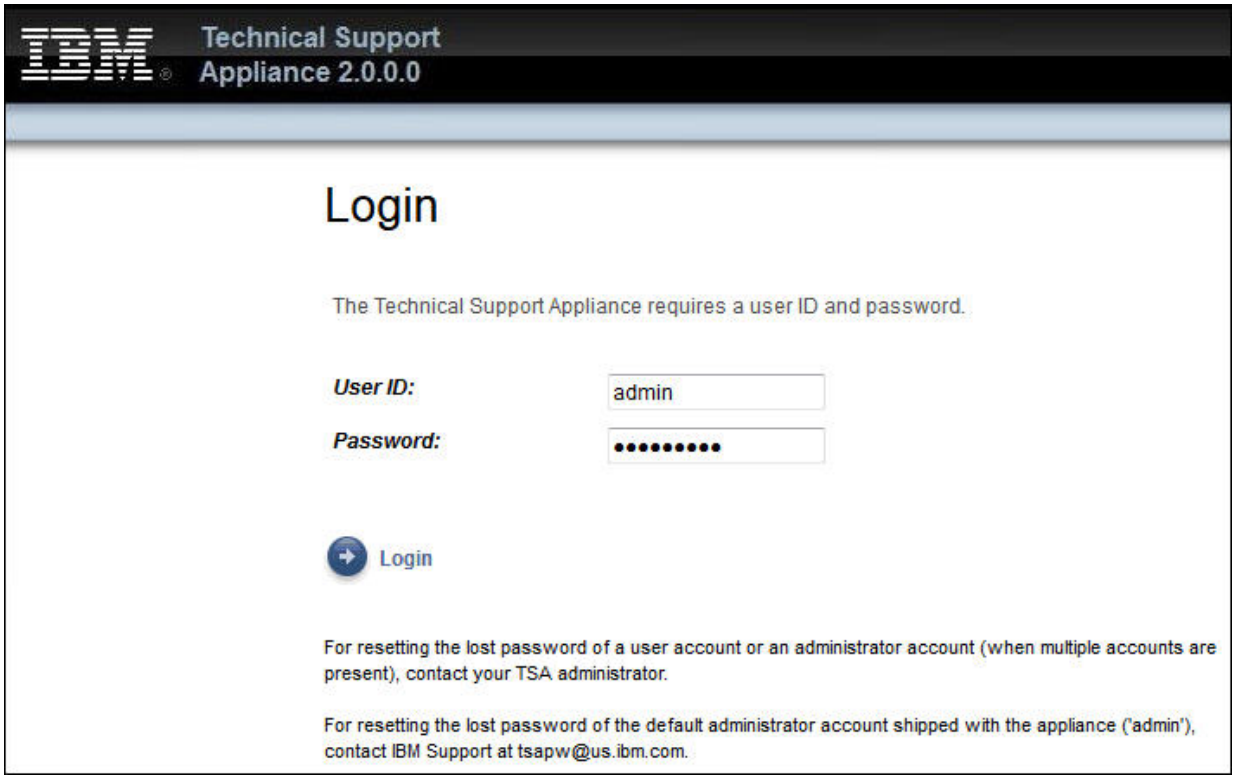

Figura 19. Efetuar login

A área de janela **Mudar senha** é exibida em seu primeiro login.

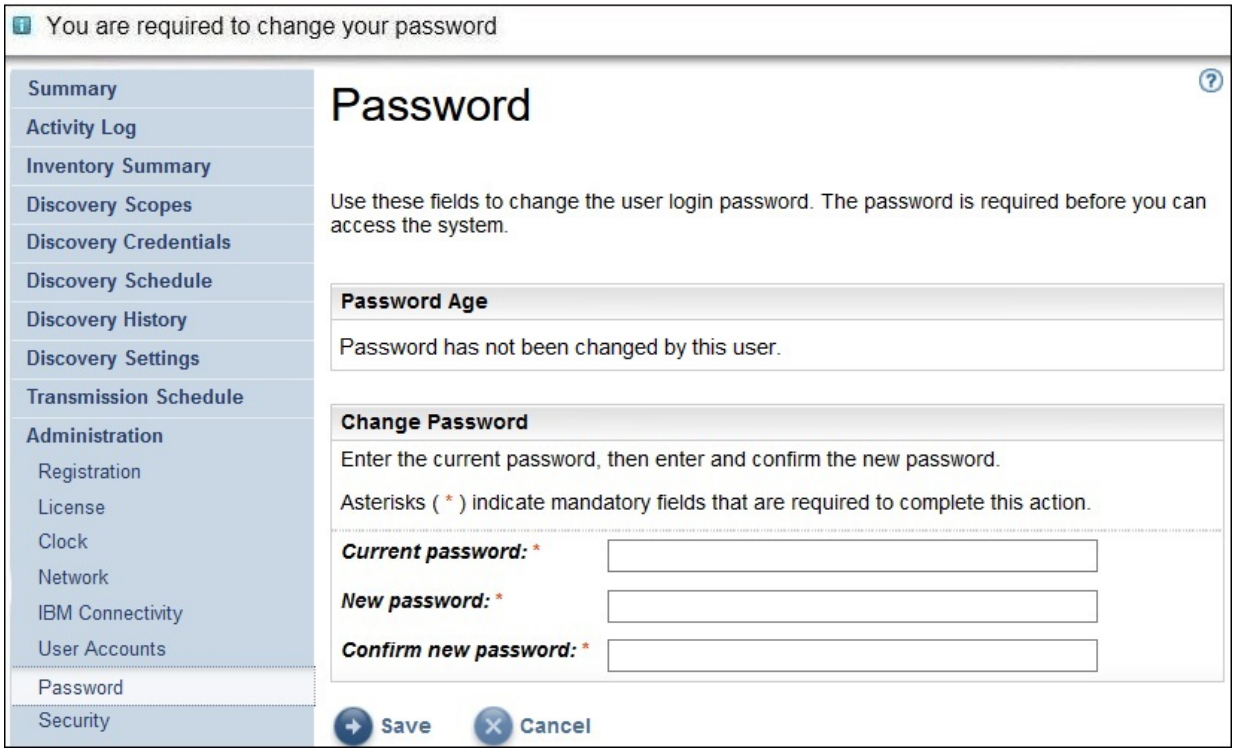

Figura 20. Mudar senha

Para mudar a senha inicial, siga estas etapas:

a) Insira uma nova senha.

A senha deve obedecer às seguintes regras:

- Deve ter pelo menos oito caracteres
- Deve conter pelo menos um caractere alfabético e um não alfabético
- Não deve conter o nome do usuário
- Não deve ser igual a nenhuma das oito últimas senhas
- Deve ser mudada pelo menos a cada 90 dias, mas não deve ser mudada mais de uma vez por dia.

b) Insira a nova senha novamente no campo **Confirmar nova senha**.

As duas senhas inseridas são comparadas para confirmar a correspondência antes que a senha seja salva.

c) Registre a nova senha para referência futura.

Importante: Não é possível recuperar uma senha, portanto, se a senha for perdida ou esquecida, não será possível efetuar logon no TSA para mudar as credenciais. Se você perder ou esquecer sua senha de uma conta de usuário ou de administrador (se você tiver várias contas), entre em contato com o administrador do TSA. Se você perder ou esquecer sua senha da conta de administrador padrão (fornecida com o TSA), entre em contato com o Suporte IBM.

d) Clique em **Salvar**. Para a primeira conexão, a página **Contrato de licença** é exibida.

Aceitando o Contrato de Licença

Leia e aceite o Contrato de licença para continuar.

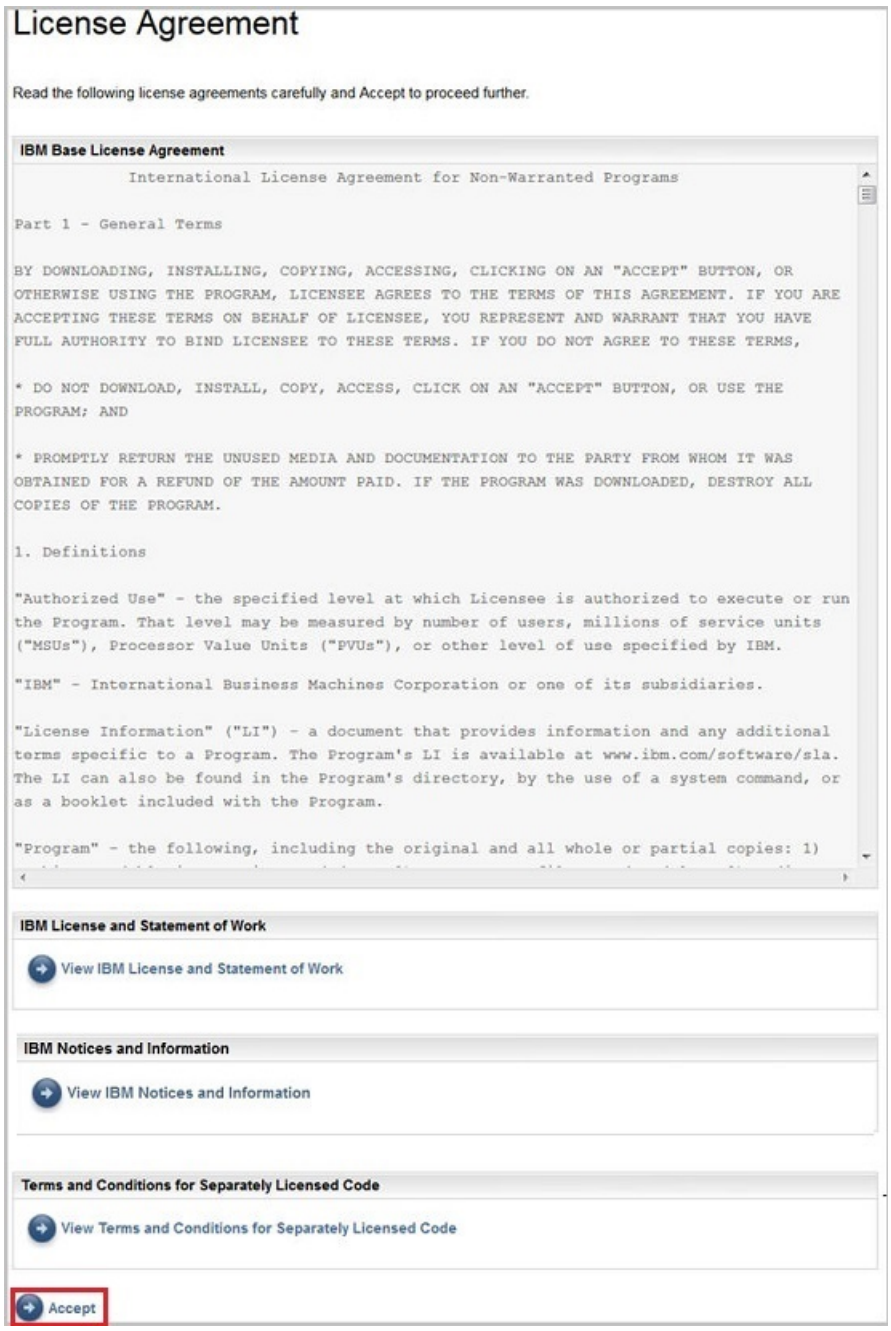

Figura 21. Contrato de Licença

O Contrato de Licença inclui os seguintes itens:

- **Contrato de licença base da IBM**: exibe o contrato de licença base da IBM.
- **Licença da IBM e descrição do trabalho**: clique em **Visualizar Licença da IBM e descrição do trabalho** para visualizar a Licença da IBM e a descrição do trabalho.

  Nota: O TSA está em conformidade com o GDPR [EU/2016/679]. É possível visualizar as informações de conformidade com o GDPR na seção **Licença e descrição do trabalho da IBM**.
- **Avisos e informações IBM**: clique em **Visualizar Avisos e informações IBM** para visualizar os avisos e informações IBM.
- **Termos e Condições para o código licenciado separadamente**: clique em **Visualizar Termos e Condições para o código licenciado separadamente** para visualizar os termos e condições para o código licenciado separadamente.

Clique em **Aceitar** para aceitar o contrato. Depois de aceitar a licença, o **Assistente de configuração** é exibido para configurar o TSA. É possível configurar o TSA por meio do **Assistente de configuração** ou sair do assistente e configurar as definições do TSA de acordo com os seus requisitos.

Nota: Para visualizar o Contrato de Licença novamente após aceitá-lo, clique em **Administração** > **Licença** na área de janela de navegação.

Conceitos relacionados

"Usando o assistente de configuração para configuração inicial" na página 25
Use o **assistente de configuração** para configurar o TSA para a configuração inicial.

"Configurando o Technical Support Appliance" na página 119
Se você sair ou ignorar a configuração de qualquer uma das definições no **Assistente de configuração**, será possível configurá-las manualmente no menu de navegação esquerdo do TSA.

Usando o assistente de configuração para configuração inicial

Use o **assistente de configuração** para configurar o TSA para a configuração inicial.

Depois de aceitar o contrato de licença, o **assistente de configuração** é exibido automaticamente.

Nota: Para iniciar o **Assistente de configuração** manualmente, na área de janela de navegação, clique em **Ferramentas** > **Assistente de configuração** > **Iniciar assistente de configuração**.

Figura 22. Assistente de configuração

O **Assistente de configuração** orienta através das seguintes etapas:

- "Configurando o IBM Connectivity" na página 25
- "Registrando o Technical Support Appliance" na página 27
- "Configurando o clock" na página 29
- "Configurando o planejamento de transmissão" na página 31
- "Atualizando o Technical Support Appliance" na página 32

Nota: Se você sair ou ignorar a configuração de qualquer uma das definições no **Assistente de configuração**, será possível configurá-las manualmente na área de janela de navegação esquerda do TSA. Para obter mais informações sobre como configurar essas definições, veja Apêndice A, "Configurando o Technical Support Appliance", na página 119.

Configurando o IBM Connectivity

Procedimento

É possível visualizar, mudar e testar a configuração que o TSA usa para se conectar à IBM.

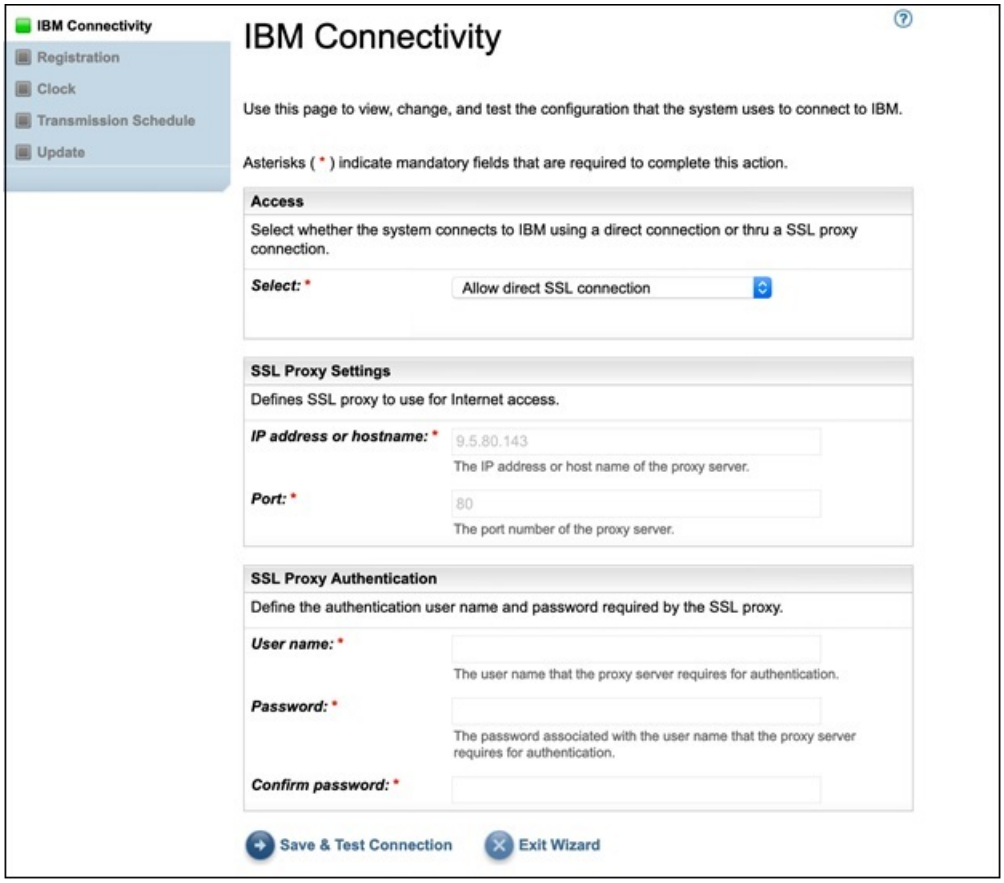

Figura 23. Conectividade IBM

1. Na área de janela **Acesso**, selecione um dos tipos de acesso à Internet a seguir:

   Permitir a conexão SSL direta
   O TSA se conecta à IBM usando uma conexão direta.

   Usar a conexão proxy SSL
   O TSA se conecta à IBM usando uma conexão proxy SSL.

   Usar a conexão proxy SSL de autenticação
   O TSA se conecta à IBM usando uma conexão proxy SSL de autenticação.

2. Se você selecionou **Usar conexão de proxy SSL** ou **Usar conexão de proxy SSL de autenticação**, especifique as seguintes informações para o servidor proxy.

   Endereço IP ou nome do host
   O endereço IP ou o nome do host do servidor proxy.

   Nota: O nome do host digitado não deve conter sublinhado ("_").

   Porta
   O número da porta do servidor proxy.

3. Se você selecionou **Usar conexão de proxy SSL de autenticação**, especifique as seguintes informações para o servidor proxy:

   Nome do usuário
   O nome do usuário que o servidor proxy requer para autenticação.

   Senha
   A senha associada ao nome de usuário que o servidor proxy requer para autenticação.

Confirmar senha
Insira a senha novamente. As duas senhas inseridas são comparadas para confirmar se são correspondentes antes que a senha seja salva.

O que Fazer Depois

- Clique em **Salvar e testar conexão** para salvar e testar a conexão especificada. Se a conexão for bem-sucedida, o botão **Continuar** será exibido.
- Clique em **Continuar** para ir para a página **Registro**.

  -ou-
- Clique em **Sair do assistente** para sair do **Assistente de configuração** e ir para a página **Resumo**.

Registrando o Technical Support Appliance

É possível visualizar e mudar o contato de serviço do sistema e o local físico.

Procedimento

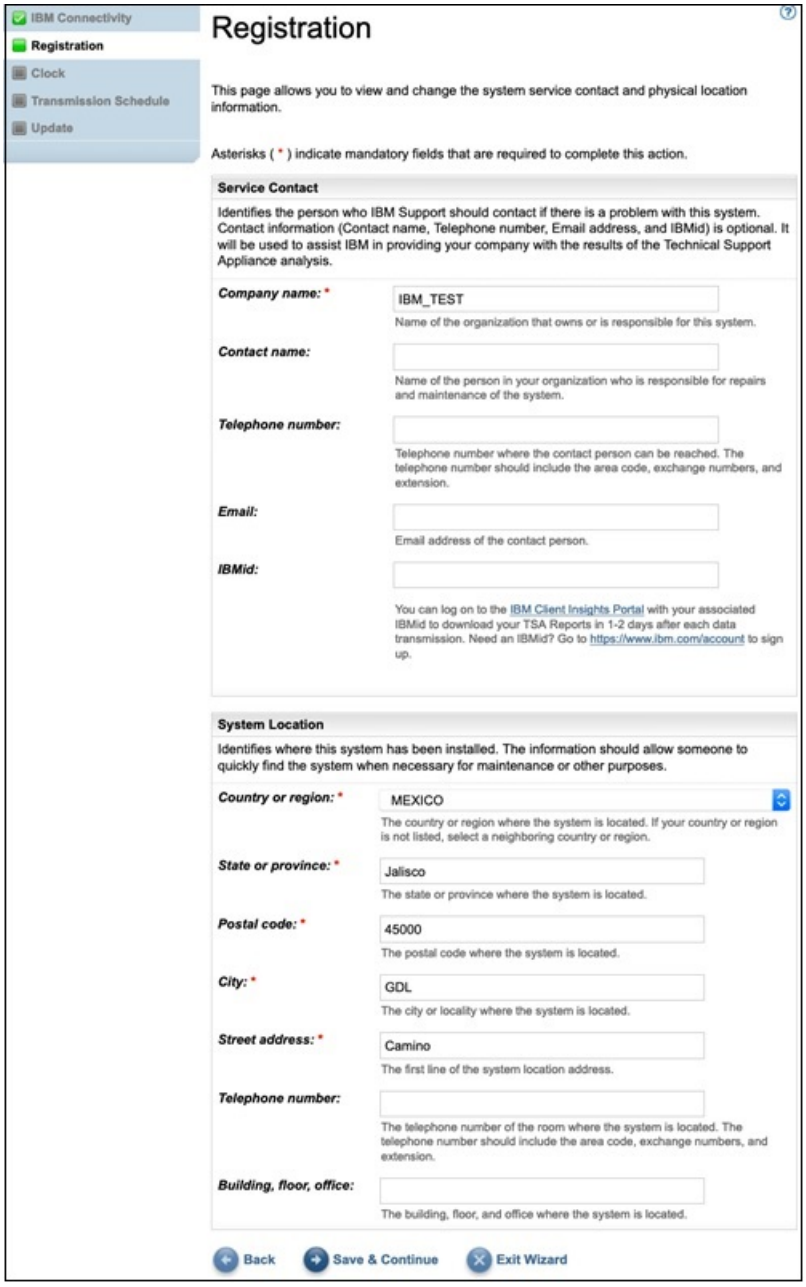

Figura 24. Registro

1. Especifique as informações de contato de serviço nos seguintes campos:

   Nome da empresa
   O nome da organização que usa o TSA.

   Nome do contato
   (Opcional) o nome da pessoa na organização que é responsável pelo TSA.

   Número de telefone
   (Opcional) O número de telefone da pessoa para contato. O número de telefone deve incluir o código de área, os números da central telefônica e o ramal. Não use parênteses no número de telefone.

   E-mail
   (Opcional) O endereço de e-mail da pessoa para contato.

IBMid
(Opcional) O IBMid da pessoa que você deseja autorizar para visualizar os relatórios no IBM Client Insights Portal.

Nota: É possível efetuar logon no https://clientinsightsportal.ibm.com/ com o IBMid associado para fazer o download dos seus TSA Reports em um a dois dias após cada transmissão de dados. Para se inscrever em um IBMid, acesse https://www.ibm.com/account.

Nota: O contato de serviço identifica a pessoa que o Suporte IBM deverá contatar caso haja algum problema com o sistema. As informações de contato são usadas para ajudar a IBM a fornecer à sua empresa os resultados da análise do Technical Support Appliance.

2. Especifique as informações de contato do TSA nos seguintes campos:

País ou região
O país ou a região em que o TSA está localizado.

Estado ou província
O estado ou o município em que o TSA está localizado. Se você não tiver certeza de qual estado é, digite *Unknown*

CEP
O código postal em que o TSA está localizado.

Cidade
A cidade ou localidade em que o TSA está localizado.

Endereço
Endereço da localização do TSA.

Número de telefone
(Opcional) O número de telefone da sala em que o TSA está localizado. O número de telefone deve incluir o código de área, os números da central telefônica e o ramal. Não use parênteses no número de telefone.

Prédio, piso, escritório
(Opcional) O prédio, andar e escritório em que o TSA está localizado.

O que Fazer Depois

- Clique em **Salvar e continuar** para salvar informações de registro e continuar para a página **Relógio**.
- Clique em **Voltar** para voltar para a página **IBM Connectivity**.

-ou-

- Clique em **Sair do assistente** para sair do **Assistente de configuração** e ir para a página **Resumo**.

Configurando o clock

É possível definir a hora, a data e o fuso horário local do sistema TSA durante a instalação.

Procedimento

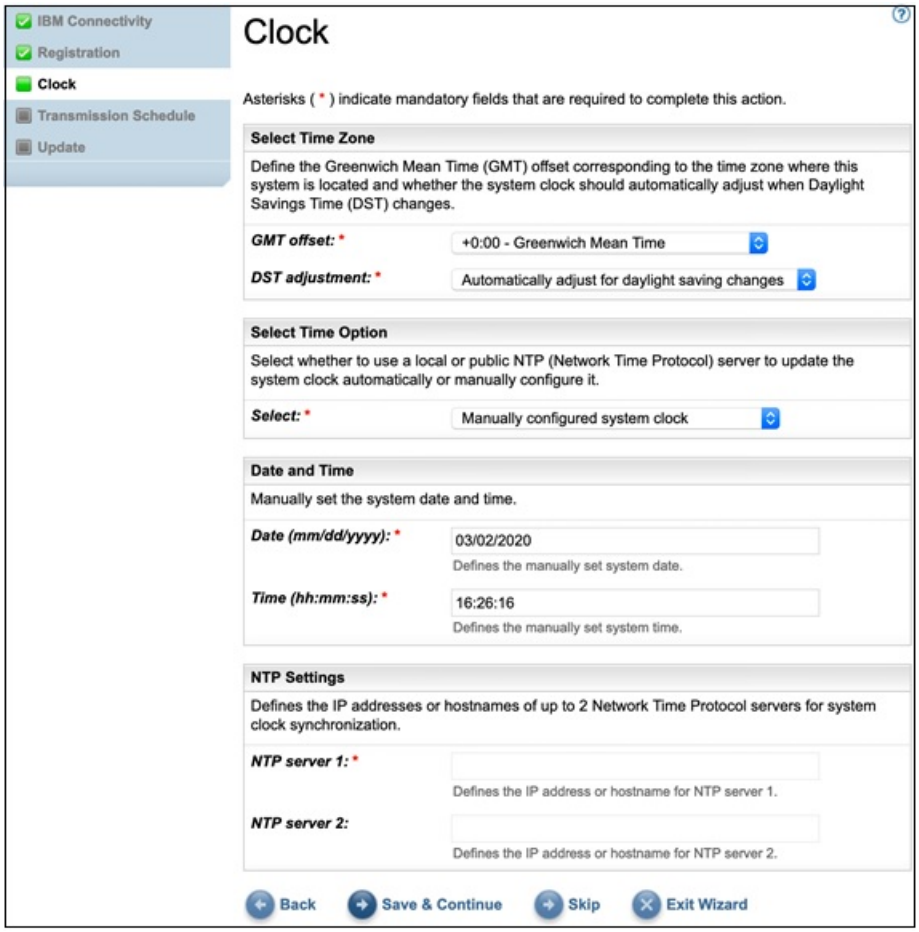

Figura 25. Relógio

1. Selecione seu fuso horário local na lista suspensa **Deslocamento do GMT**.
2. Selecione o ajuste de horário de verão na lista suspensa **Ajuste de horário de verão**.

   Nota: Nem todos os fusos horários permitem o DST. Se essa opção estiver selecionada para um fuso horário que não permitir horário de verão, uma mensagem de erro será exibida.
3. Selecione um método para atualizar o relógio do sistema na lista suspensa **Selecionar opção de horário**.

   As opções incluem a sincronização do relógio do sistema com um servidor Network Time Protocol (NTP) para atualizar o relógio do sistema automaticamente ou configurar manualmente.

   a) Se você selecionou configurar manualmente o relógio do sistema, deverá definir a data e a hora do sistema. Insira as informações de data e hora nos campos **Data** e **Hora**.

   b) Se a opção de sincronizar o clock do sistema com um servidor Network Time Protocol (NTP) para atualizar o clock do sistema automaticamente foi selecionada, os endereços IP e os nomes de host deverão ser especificados para os servidores NTP. Digite as informações de endereço IP ou do nome do host para até dois servidores nos campos **Servidor NTP**.

   Nota: Verifique se o servidor NTP está acessível através da rede para o TSA.

O que Fazer Depois

- Clique em **Salvar e continuar** para salvar informações do relógio e continuar para a página **Planejamento de transmissão**.

  -ou-

- Clique em **Ignorar** para ir para a página **Planejamento de transmissão**.

Para modificar as configurações na etapa anterior do assistente

- Clique em **Voltar** para voltar para a página de **Registro**.

Para sair do assistente

- Clique em **Sair do assistente** para sair do **Assistente de configuração** e ir para a página **Resumo**.

Configurando o planejamento de transmissão

O TSA fornece um planejamento padrão para o processo de transmissão ser executado em horários especificados. É possível modificar esse planejamento de acordo com suas necessidades.

Procedimento

1. Use as listas suspensas **Na hora** e **No minuto** para selecionar um novo horário.
2. Selecione o **Modo de seleção de dia**.

Semanalmente por dia(s) (de domingo a sábado)
Para planejar a transmissão em um determinado dia da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)**.

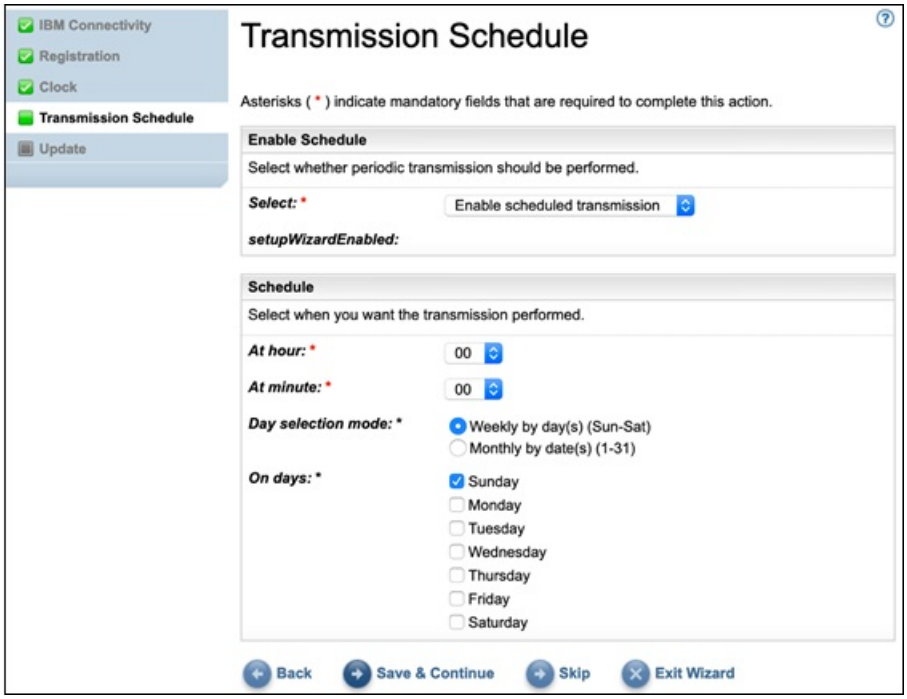

Figura 26. Semanalmente por dia(s) (de domingo a sábado)

Para o campo **Nos dias**, marque a caixa de seleção apropriada para selecionar um ou mais dias da semana.

Mensalmente por data(s) (de 1 a 31)
Para planejar a transmissão em determinados dias de um mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.

Para o campo **Nos dias**, marque a caixa de seleção apropriada para selecionar um ou mais dias do mês.

Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.

Nota: Certifique-se de que o horário de início da descoberta anteceda o horário de transmissão para evitar longos atrasos na transmissão dos dados recém-coletados.

O que Fazer Depois

- Clique em **Salvar e continuar** para salvar o planejamento da transmissão e continuar para a página **Atualizar**.

  -ou-

- Clique em **Ignorar** para ir para a página **Atualizar**.

Para modificar as configurações na etapa anterior do assistente

- Clique em **Voltar** para voltar para a página **Relógio**.

Para sair do assistente

- Clique em **Sair do assistente** para sair do **Assistente de configuração** e ir para a página **Resumo**.

Atualizando o Technical Support Appliance

É possível atualizar o TSA para a versão mais recente disponível.

Se uma atualização estiver disponível, a seguinte página **Atualizar** será exibida.

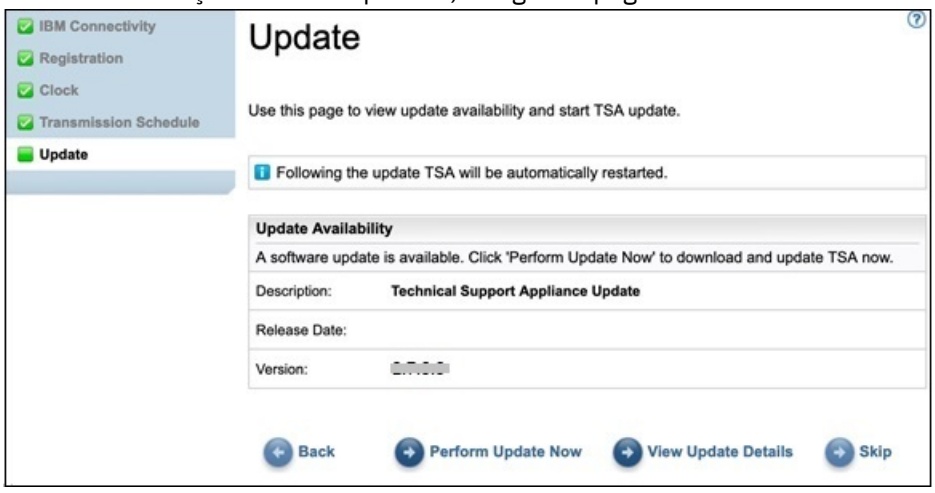

Figura 27. Atualizar disponibilidade

- Clique em **Executar atualização agora** para instalar a atualização e concluir o **Assistente de configuração**.

  -ou-

- Clique em **Visualizar detalhes da atualização** para visualizar informações sobre o conteúdo da atualização.

Para modificar as configurações na etapa anterior do assistente

- Clique em **Voltar** para voltar à página **Planejamento de transmissão**.

Para concluir o assistente

- Clique em **Ignorar** para concluir o **Assistente de configuração** sem aplicar a atualização.

Se uma atualização não estiver disponível, a seguinte página **Atualizar** será exibida.

Figura 28. Nenhuma atualização disponível

- Clique em **Concluir assistente** para concluir o **Assistente de configuração**. A página **Assistente de configuração concluído** é exibida.

  -ou-

- Clique em **Voltar** para voltar à página **Planejamento de transmissão**.

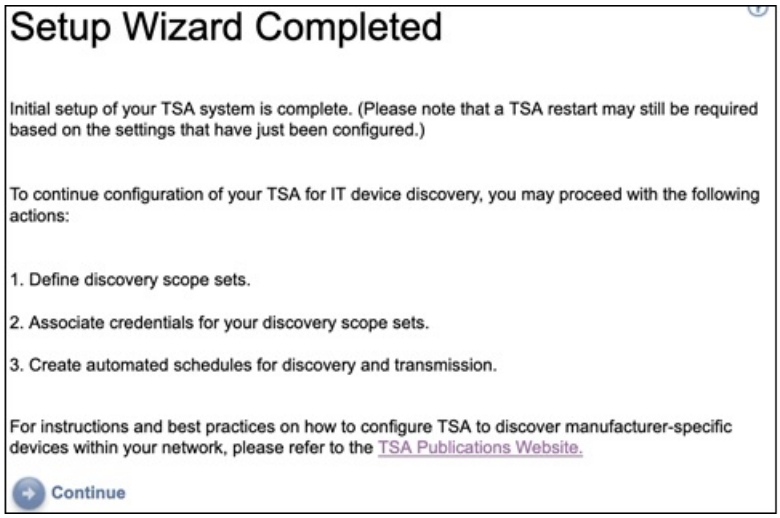

Figura 29. Assistente de configuração concluído

- Clique em **Continuar** para ir para a página **Resumo**.

  Nota: Algumas mudanças na página **Relógio** podem requerer uma reinicialização para que entrem em vigor. Por exemplo, se você definir a data ou a hora ou mudar da configuração manual para a configuração do servidor NTP, você será solicitado a reiniciar o sistema.

  – Clique em **OK** para concluir o **Assistente de configuração** e volte para a página **Resumo**. A página **Resumo** é exibida e o sistema é reinicializado.

Nota: Se você sair ou ignorar a configuração de qualquer uma das definições no **Assistente de configuração**, será possível configurá-las manualmente na área de janela de navegação esquerda do TSA. Para obter mais informações sobre como configurar essas definições, veja Apêndice A, “Configurando o Technical Support Appliance”, na página 119.

Definindo as configurações de rede

Instalar o TSA requer a configuração das definições básicas de rede. Se essas configurações forem adequadas para sua rede de TI, você poderá ignorar esta seção.

Antes de Iniciar

Use a página **Rede** para fazer qualquer um dos seguintes.

- Mude as definições básicas iniciais de rede

- Configure o TSA para acessar várias redes

Para definir as configurações básicas de rede no console, siga as etapas na seção “Configurando os detalhes da rede” na página 19.

Definindo configurações básicas de rede

Use a página **Rede** para alterar qualquer configuração de rede inicial.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Rede**.
   A página **Rede** é exibida.

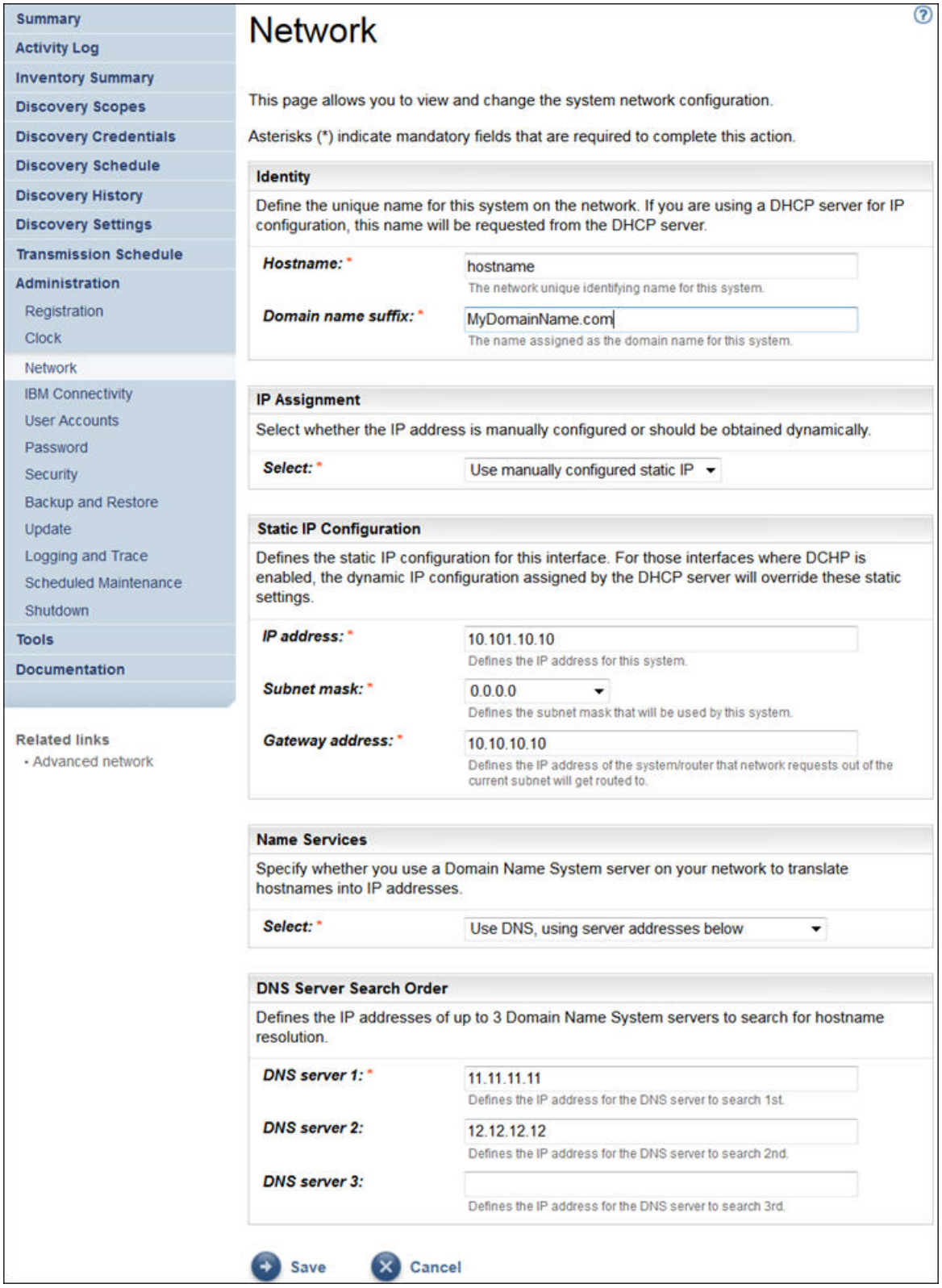

Figura 30. Rede

2. No campo **Nome do host**, especifique o nome exclusivo para esse sistema na rede local.
3. No campo **Sufixo de nome de domínio**, especifique o nome que é usado como o nome de domínio para esse sistema na rede local.

4. Selecione **Usar IP estático configurado manualmente** para *IP Assignment*. Para a designação de endereço DHCP, consulte a seção Apêndice B, “Configurando os detalhes de rede do DHCP”, na página 129.
5. Configurar o endereço IP estático:
   a) No campo **Endereço IP**, insira o endereço IP para esse sistema.
   b) Na lista suspensa **Máscara de sub-rede**, selecione a máscara de sub-rede a ser usada pelo sistema.
   c) No campo **Endereço do gateway**, insira o endereço IP do sistema ou do roteador que manipula solicitações fora da sub-rede atual.
6. Especifique os **Serviços de nomes** de acordo com a designação do IP.
   a) Para IP estático configurado manualmente, selecione a opção **Usar o DNS, usando endereços do servidor abaixo**.
   b) Para designação de endereço IP DHCP, selecione a opção **Usar DNS, mas obter endereços do servidor via DHCP**.
7. Insira até três endereços IP para os servidores de Sistema de Nomes de Domínio (DNS) a serem usados ao resolver nomes de host.

   O TSA pesquisa os servidores na ordem em que são exibidos.
8. Clique em **Salvar** para salvar as configurações de rede.

   Será solicitado que você reinicie o sistema.

   CUIDADO: Tenha cuidado ao mudar as configurações de rede. Se houver um erro com a configuração de rede, a interface com o usuário do TSA poderá não estar acessível. Nesse caso, o console do TSA deve ser usado para reparar a configuração de rede:
   - Para o VMware, use a interface da web d VMware ESXi ou o VMware vSphere Client
   - Para o Microsoft Hyper-V, use o Hyper-V Manager
9. Clique em **Cancelar** para sair da página **Rede** sem salvar as configurações.

Definindo as configurações de rede avançada

Se você deseja configurar o TSA para acessar várias redes, use a página **Rede (avançada)** para especificar essas configurações de rede.

Para definir as configurações de rede avançada, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Rede**.
2. Na área de janela de navegação inferior, em **Links relacionados**, clique em **Rede avançada**.

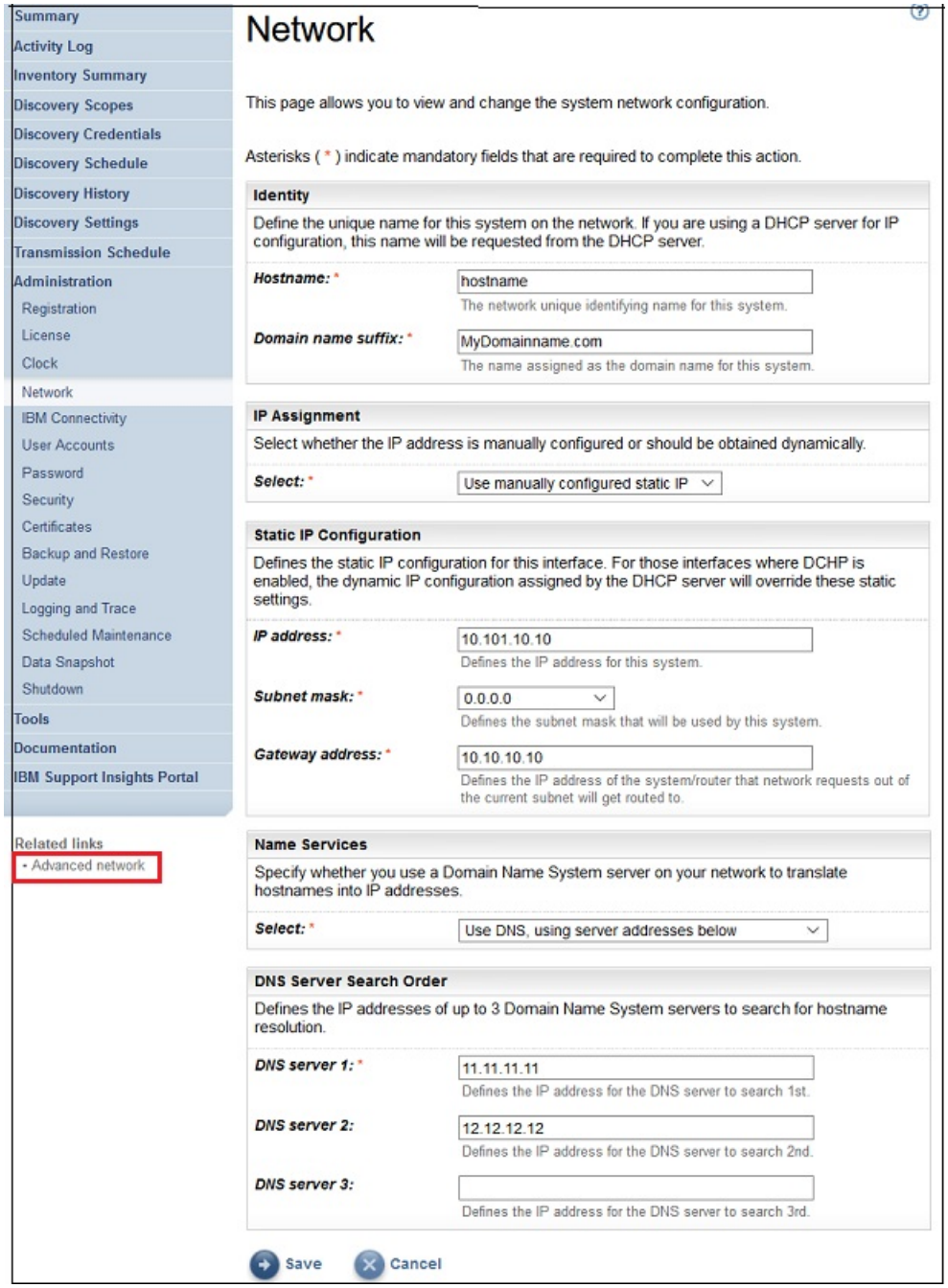

Figura 31. Acessar a página de Rede (avançada)

A página **Rede (avançada)** é exibida

A página **Rede (avançada)** é dividida nas seguintes páginas separadas:

- Global
- Interfaces de rede
- Configurações de DNS
- Rotas de rede

Para acessar essas páginas individuais, clique na guia da página que você deseja exibir.

Importante: Deve-se clicar em **Salvar** antes de sair de uma página para salvar as mudanças feitas nos campos dessa página. Será solicitado que você reinicie o sistema para que as mudanças entrem em vigor.

Global

Use essa página para visualizar e mudar as configurações de rede global:

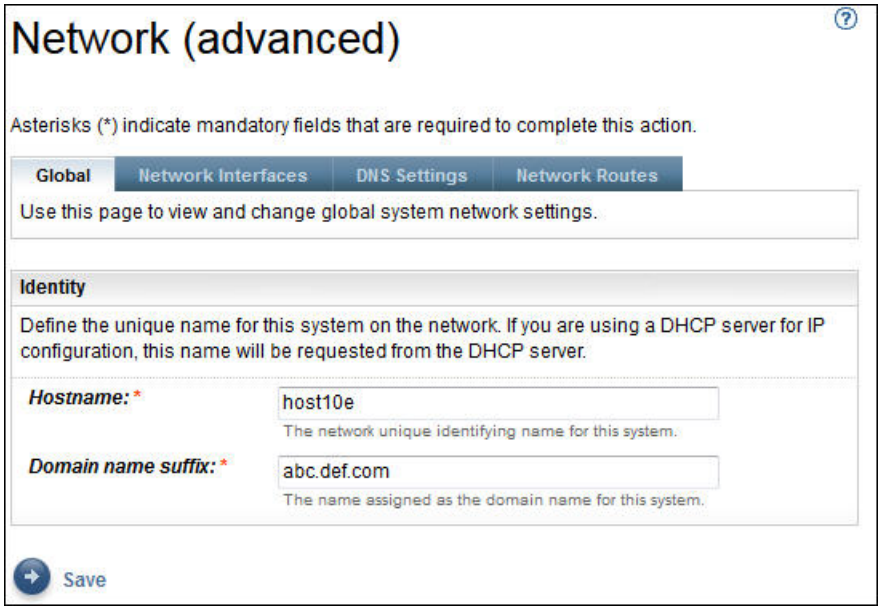

Figura 32. Rede (avançada) - Global

Identidade

Defina a identidade deste sistema na rede.

1. No campo **Nome do host**, especifique o nome específico para esse sistema.
2. No campo **Sufixo do nome de domínio**, especifique o nome usado como o nome de domínio para esse sistema.

Interfaces de rede

O TSA é configurado para ter dois Network Interface Controllers (NICs) - eth0 e eth1. Use esta página para visualizar as configurações atuais da interface de rede selecionada.

1. Clique em **eth0** para selecionar a interface de rede eth0.
2. Clique em **eth1** para selecionar a interface de rede eth1.

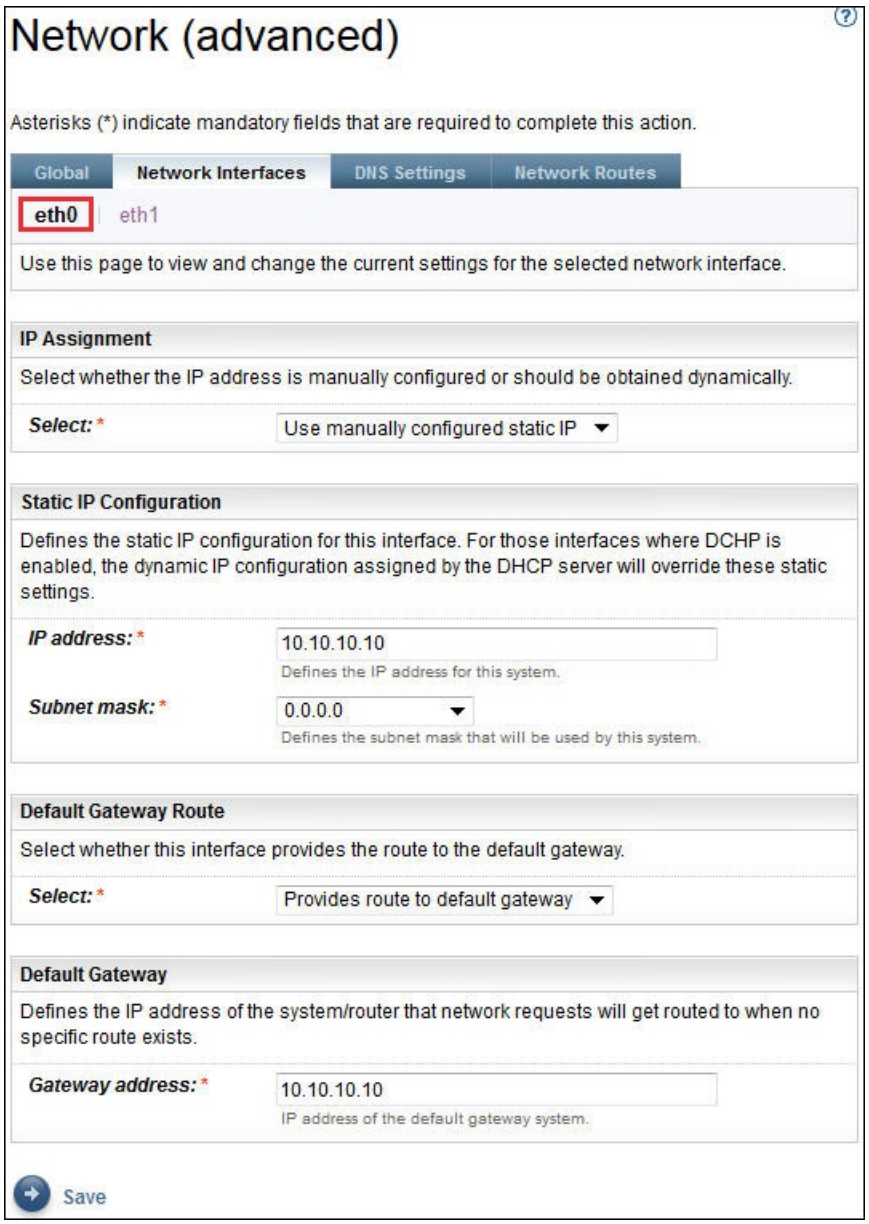

Figura 33. Rede (avançada) - Interfaces de rede

Designação de IP

Selecione um método para atribuir o endereço IP para este sistema. As opções incluem obter dinamicamente o endereço IP de um servidor DHCP ou usar um endereço IP estático configurado manualmente. Se você optar por usar um endereço IP estático configurado manualmente, deverá configurar o endereço IP do sistema nesta página.

Configuração de IO estático

Se você optou por configurar manualmente um endereço IP estático, especifique as informações de IP para esta interface de rede da seguinte maneira:

1. No campo **endereço IP**, especifique o endereço IP para esse sistema.
2. Na lista suspensa **Máscara de sub-rede**, selecione a máscara de sub-rede a ser usada pelo sistema.

Rota de gateway padrão

Especifique se essa interface de rede fornece uma rota para o gateway padrão.

Gateway padrão

No campo **endereço de gateway**, especifique o endereço IP do gateway padrão para esse sistema.

Configurações de DNS

Use essa página para visualizar e mudar as configurações de DNS.

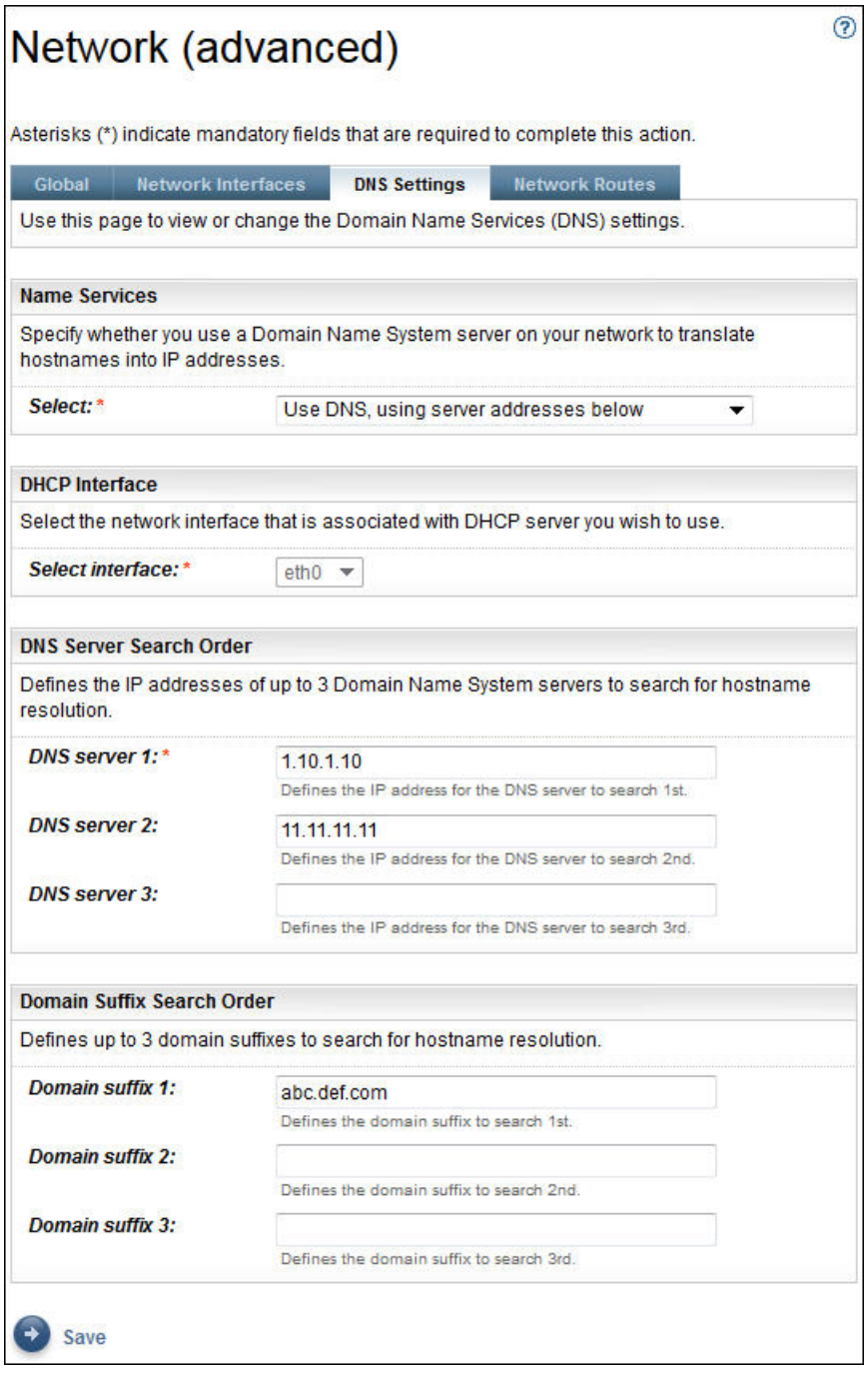

Figura 34. Rede (avançada) - configurações de DNS

Serviços de nome

Especifique um Sistema de Nomes de Domínio (DNS) na sua rede para converter nomes de host em endereços IP. É possível escolher entre as seguintes opções:

- Use DNS, mas obtenha endereços de servidor de um servidor DHCP.

Se você escolher esta opção, deverá selecionar a interface de rede associada ao servidor DHCP que deseja usar.

- Use DNS com endereços de servidor que você especificar.

  Se você escolher esta opção, deverá especificar pelo menos um servidor DNS nesta página.

Interface DHCP
Selecione a interface de rede associada ao servidor DHCP que você deseja usar.

Ordem de procura de servidor DNS
Se você optar por usar o DNS com endereços de servidor especificados, insira até três endereços IP para os servidores Domain Name System (DNS) a serem usados ao resolver nomes de host. O TSA pesquisa os servidores na ordem em que são exibidos.

Ordem de procura de sufixo do domínio
Se você optar por usar o DNS com endereços de servidor especificados, insira até três sufixos de nome de domínio a serem usados na resolução de nomes de host. O TSA pesquisa esses sufixos de nome de domínio na ordem em que são exibidos.

Rotas de rede

Use esta página para visualizar, incluir, mudar ou excluir entradas de roteamento estático.

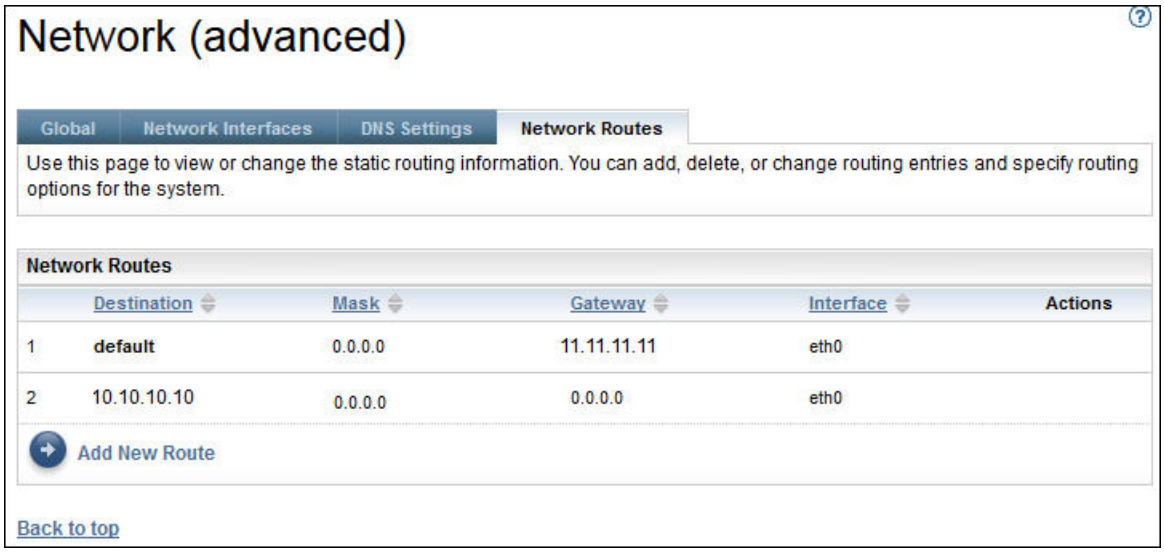

Figura 35. Rede (avançada) - Rotas de rede

As seguintes informações são exibidas para cada rota de rede:

Destino

Especifica o endereço do host ou da sub-rede da rede de destino TCP/IP.

Máscara
Especifica a máscara de sub-rede a ser usada como máscara de rede ao incluir uma rota. Esse é o endereço de sub-rede para a parte do host do endereço IP. As interfaces de rede podem usar máscaras de sub-rede diferentes, oferecendo a capacidade de incluir rotas selecionando uma máscara de sub-rede (rotas de sub-rede variáveis). Deve-se selecionar uma máscara de sub-rede ao incluir uma rota, em notação decimal pontilhada de 32 bits.

Gateway
Especifica o endereço do gateway TCP/IP dos pacotes de IP de roteamento.

Interface
Selecione o adaptador no menu. Esse é o nome do adaptador de rede associado à entrada da tabela.

Ações
Clique no ícone **Excluir** ( ) para excluir a rota.

Nota: Nenhuma das duas rotas mostradas na figura pode ser modificada ou excluída.

Clique em **Incluir nova rota** para definir uma nova rota de rede estática. A página **Rota de rede** é exibida.

Incluindo rotas de rede

É possível incluir rotas de rede estática.

Procedimento

Para incluir uma rota de rede, siga estas etapas:

1. Na página **Rede (avançado) - Rotas de rede**, clique em **Incluir nova rota**. A página **Rota de rede** é exibida.

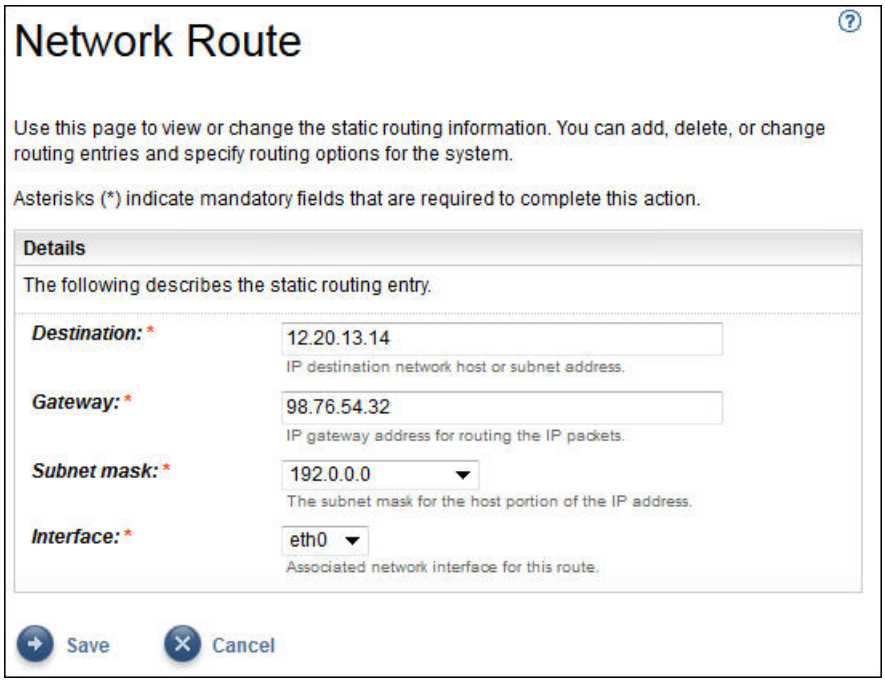

Figura 36. Nova rota de rede

2. No campo **Destino**, insira o endereço IP para o host de rede ou a sub-rede TCP/IP de destino.
3. No campo **Gateway**, insira o endereço de gateway TCP/IP para roteamento das informações. O endereço deve estar em notação decimal pontilhada de 32 bits. Por exemplo: `xxx.xxx.xxx.xxx`.
4. Na lista suspensa **Máscara de sub-rede**, selecione a máscara de sub-rede a ser usada como máscara de rede para esta rota.
5. Na lista suspensa **Interface**, selecione o adaptador de rede a ser associado a esta rota.
6. Clique em **Salvar** para salvar esta rota de rede.

Configurando os certificados

A página **Certificados** permite visualizar informações de assinatura de certificado, gerar e instalar certificados ou importar certificados. Esses são os certificados de servidor que o TSA apresenta a um servidor da web quando a interface com o usuário é acessada.

A configuração padrão do TSA implementa um certificado de servidor SSL autoassinado genérico para facilitar a instalação. Para maior segurança, é recomendável substituir o certificado padrão após a conclusão das etapas iniciais de implementação e configuração. É possível usar o TSA para gerar e instalar um certificado autoassinado do servidor SSL que seja exclusivo desse TSA, gerar e instalar um certificado customizado assinado pela autoridade de certificação de sua escolha ou fazer upload do seu próprio arquivo Java keystore com um certificado customizado do servidor SSL.

É possível instalar um certificado customizado usando um dos métodos a seguir:

- “Instalando um certificado customizado (usando assinantes)” na página 44
- “Instalando um certificado customizado (método alternativo) ” na página 45

Visualizando o status do certificado do servidor SSL

A configuração do TSA instala o certificado do TSA padrão que é entregue com o Technical Support Appliance.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Certificados**.
   A página **Certificados** é exibida.

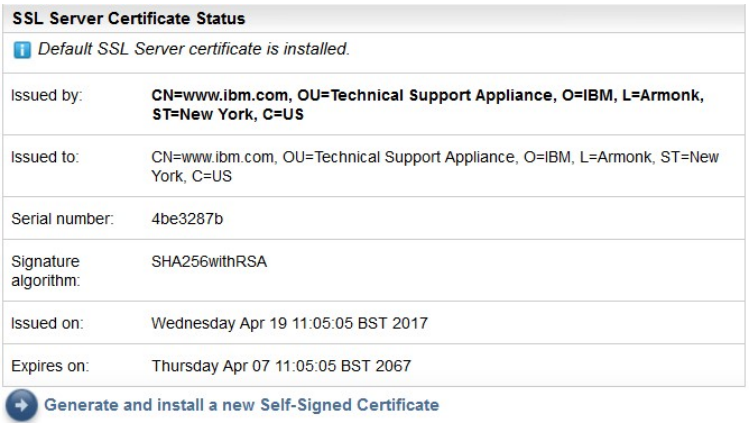

   Figura 37. Status do certificado do servidor SSL

   A seção **Status do certificado do servidor SSL** exibe as informações sobre o certificado do servidor SSL que está instalado no TSA. As informações do certificado incluem *Issued by*, *Issued to*, *Issued on*, *Expires on*, *Serial number* e *Signature algorithm*.
2. Clique em **Gerar e instalar um novo certificado autoassinado** para instalar um certificado autoassinado exclusivo desse TSA. Uma mensagem de aviso é exibida informando que o dispositivo será reiniciado automaticamente depois que você gerar e instalar um certificado autoassinado.

   Nota: O botão **Gerar e instalar um novo certificado autoassinado** fica visível somente quando o certificado padrão está instalado no TSA.

Gerando e fazendo download do CSR

Para solicitar um certificado SSL que é certificado por uma Autoridade de Certificação, é necessário fornecer as seguintes informações para gerar e fazer download do arquivo Certificate Signing Request (CSR).

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Certificados**.
   A página **Certificados** é exibida.

Figura 38. Solicitação de assinatura de certificado

2. Insira o nome qualificado do host (FQDN) do TSA no campo **Nome comum**. O limite mínimo de caracteres é um, e o máximo é 64.
3. Especifique o nome da organização, que diferencia as divisões de uma organização no campo **Unidade da organização**.
4. Especifique o nome da corporação, parceria limitada, universidade ou agência governamental no campo **Organização**.
5. Especifique a cidade ou o nome da localidade em que o TSA é operado no campo **Cidade**.
6. Especifique o nome do estado ou do município em que o TSA é operado no campo **Estado**. Se você não tiver certeza do seu estado ou se o estado não se aplicar ao seu país, digite *Unknown*.
7. Selecione o nome do país em que o TSA é operado no menu suspenso **País**.
8. Especifique o número de dias em que o certificado é válido a partir do momento em que o certificado é criado, no campo **Número de dias até a expiração**.
9. Clique em **Gerar e fazer o download do arquivo Certificate Signing Request (CSR)** para criar e fazer o download do arquivo CSR com as informações especificadas.

   Nota: Para restaurar o certificado padrão que acompanha o TSA, veja a seção "Restaurando o certificado padrão" na página 46.

Instalando um certificado customizado (usando assinantes)

Use esse recurso para instalar um certificado customizado. São necessários o certificado do servidor gerado por uma autoridade de certificação, o certificado raiz da autoridade de certificação e quaisquer certificados intermediários da autoridade de certificação.

Antes de Iniciar

Assegure-se de que os arquivos de certificado (os certificados raiz, intermediário e do servidor) estejam nos seguintes formatos:

- *.crt*
- *.der*
- *.pem*

Procedimento

Siga as etapas a seguir para fazer upload e instalar os certificados no TSA:

1. Na área de janela de navegação, clique em **Administração** > **Certificados**.

   A página **Certificados** é exibida.

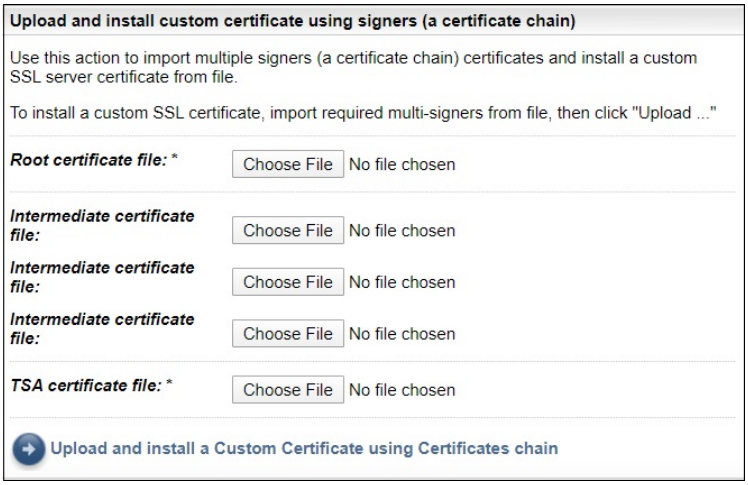

Figura 39. Instalar certificado customizado

2. No campo **Arquivo de certificado raiz**, especifique o local do arquivo de certificado raiz que você deseja instalar no TSA.
3. No campo **Arquivo de certificado intermediário**, especifique o local do arquivo de certificado intermediário que você deseja instalar no TSA.

   Nota: Pode haver vários arquivos de certificado intermediários (no máximo 3) com base nos vários assinantes importados.
4. No campo **Arquivo de certificado do TSA**, especifique o local do arquivo de certificado do servidor TSA que você deseja instalar no TSA.
5. Clique em **Fazer upload e instalar um certificado customizado usando uma cadeia de certificados** para fazer upload de todos os arquivos (*Root Certificate file*, *Intermediate certificate files*, *TSA certificate file*) especificados e instalar um certificado customizado usando a cadeia de certificados.

   Nota: Para restaurar o certificado padrão que acompanha o TSA, veja a seção "Restaurando o certificado padrão" na página 46.

Instalando um certificado customizado (método alternativo)

Use esse recurso para instalar um certificado customizado. É possível usar esta função para implementar um arquivo Java keystore completo já construído.

Antes de Iniciar

Recomenda-se usar as funções **Solicitação de assinatura da autoridade de certificação** e **Fazer upload e instalar o certificado customizado usando assinantes (uma cadeia de certificados)** na página **Certificados** para implementar um certificado customizado. No entanto, se você já construiu um arquivo Java keystore completo de forma independente (contendo as chaves, o certificado customizado e os certificados de certificação relevantes), será possível usar esta função para implementar o arquivo keystore. Deve-se fornecer o local do arquivo keystore e a senha para o arquivo.

Nota: Ao criar o arquivo keystore, certifique-se de que a senha de entrada de chave e a senha do keystore são idênticas.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Certificados**.

   A página **Certificados** é exibida.

Figura 40. Instalação do certificado customizado

2. Para instalar um certificado de servidor customizado, siga estas etapas.
   a) Insira a senha para o certificado no campo **Senha do certificado**.
   b) Insira a senha novamente no campo **Confirmar senha**.

      As duas senhas inseridas são comparadas para confirmar a correspondência antes que a senha seja salva.
   c) Especifique o local do arquivo Java keystore que contém o certificado customizado no campo **Arquivo de certificado customizado**.
   d) Clique em **Fazer upload e instalar o arquivo JKS completo** para fazer upload do arquivo Java keystore especificado e instalar um certificado customizado. O arquivo Java keystore deve incluir o certificado customizado e qualquer raiz de autoridade de certificado e certificados intermediários relevantes. O dispositivo será reiniciado para ativar o uso do novo certificado.

Nota: Para restaurar o certificado padrão que acompanha o TSA, veja a seção "Restaurando o certificado padrão" na página 46.

Resultados

Depois que o novo certificado é instalado, o TSA reinicia automaticamente. Quando a reinicialização for concluída, seu navegador poderá exibir um prompt de segurança sobre a confiança no novo certificado.

Restaurando o certificado padrão

Para restaurar o certificado padrão que acompanha o TSA, use o console do TSA e selecione a opção **Definir certificado do dispositivo como padrão**.

Procedimento

1. Ative o console do TSA.
2. Selecione a opção **3) Configurar o certificado do dispositivo como o padrão** no **Menu de configuração do TSA**.

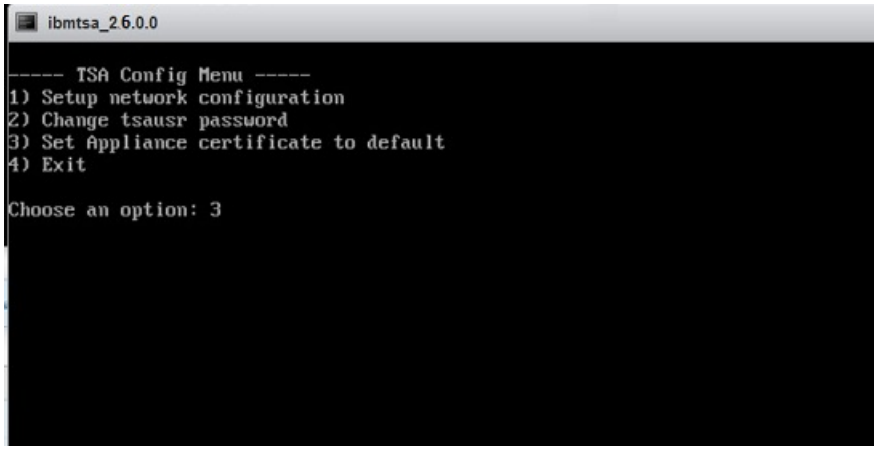

Figura 41. Configurar certificado de dispositivo como padrão

3. **Confirme a configuração do certificado do dispositivo como o certificado padrão [s|n]:** Insira **y** para confirmar a configuração do certificado do TSA como o certificado padrão.

Resultados

Após a instalação do certificado padrão, o TSA será reiniciado automaticamente em cinco segundos. Quando a reinicialização for concluída, o navegador poderá exibir um prompt de segurança perguntando se o certificado padrão é confiável.

Planejando a limpeza de dados do inventário

É possível planejar ou executar manualmente uma rotina de limpeza para todos os dados de inventário coletados nos recursos a partir do momento em que eles são descobertos.

Sobre Esta Tarefa

Atenção: É recomendado que você execute a rotina de limpeza uma vez por semana para a maioria das instalações.

Para visualizar o planejamento atual da rotina de limpeza de inventário, selecione **Resumo de inventário** > **Planejamento de limpeza de inventário**.

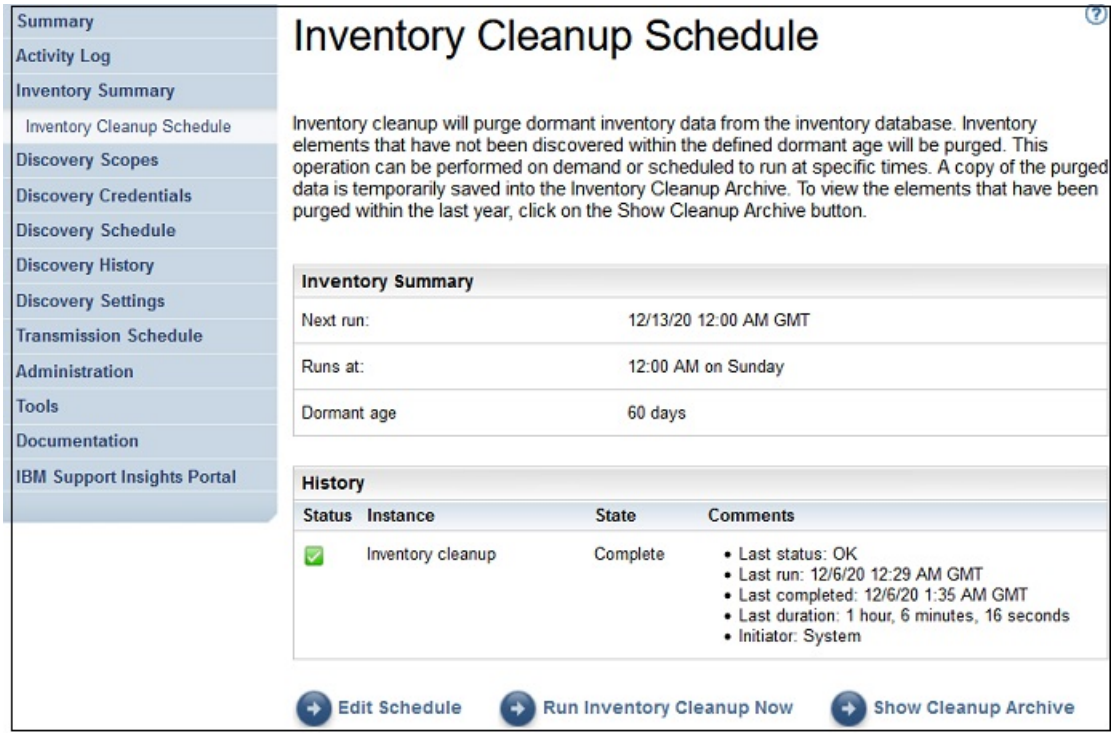

Figura 42. Planejamento de limpeza de inventário

Para executar a limpeza de inventário manualmente, clique em **Executar limpeza de inventário agora**.

Para editar, ativar ou desativar o planejamento atual de limpeza de inventário, siga estas etapas:

Procedimento

1. Na página **Planejamento de limpeza de inventário**, clique em **Editar planejamento**.
2. Na página **Configurações do inventário**, selecione **Ativar limpeza de inventário planejado** para ativar a rotina de limpeza de inventário ou **Desativar a limpeza de inventário planejado** para desativar a rotina de limpeza de inventário.
3. Se você optar por ativar a rotina de limpeza de inventário, execute as seguintes etapas:
   a) Selecione as listas suspensas **Na hora** e **No minuto** para selecionar um novo horário.

b) Selecione o **Modo de seleção de dia**. Para planejar a limpeza de inventário em um determinado dia da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)** ou para planejar a limpeza de inventário em determinados dias do mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.

c) No campo **Nos dias**, marque a caixa de seleção apropriada para selecionar dias diferentes ou adicionais da semana ou mês.

Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.

4. Selecione o período para o qual você deseja manter os dados do inventário na lista **Prazo de inatividade**.
5. Clique em **Salvar**.

Capítulo 5. Configurando a descoberta a transmissão para a IBM

Após a conclusão da configuração do TSA, será possível usar vários recursos de administração para gerenciar a descoberta, a transmissão e as tarefas.

Escopos de descoberta

Um escopo de descoberta especifica o endereço IP ou nome do host, intervalo de endereços IP ou rede a ser usado para descobrir elementos de TI. Os escopos de descoberta são agrupados em conjuntos de escopos de descoberta.

O TSA fornece diversos tipos de escopos de descoberta:

- Conjuntos de escopos dinâmicos de HMC - podem ser usados para descobrir HMCs com todas as partições gerenciadas por eles.
- Conjuntos de escopos dinâmicos do VMware - podem ser usados para descobrir hosts do VMware vCenter ou do ESXi com todas as máquinas virtuais nos hosts ESXi.
- Escopos de descoberta geral - usados para descobrir todos os outros recursos que não são descobertos usando um conjunto de escopos dinâmicos. É possível inserir os endereços IP, intervalo de endereços IP ou redes manualmente ou importar uma lista de endereços IP e nomes de host de um arquivo para o TSA.

Escopos dinâmicos de HMC

É possível definir escopos dinâmicos do HMC para coletar inventário detalhado dos HMCs, dos IBM Power Systems que eles gerenciam e também das LPARs do VIOS, AIX e Linux nesses sistemas.

Sobre Esta Tarefa

Além de recuperar informações de inventário dos HMCs definidos, o TSA também consulta dinamicamente as LPARs gerenciadas por esses HMC, sem requerer a criação e a manutenção de várias definições de escopo. Deve-se definir um escopo para os HMCs e selecionar quais tipos de LPARs (AIX, VIOS e Linux) você gostaria de varrer automaticamente quando esses HMCs forem descobertos. A vantagem é que, mesmo que as LPARs mudem, não será necessário reconfigurar o TSA.

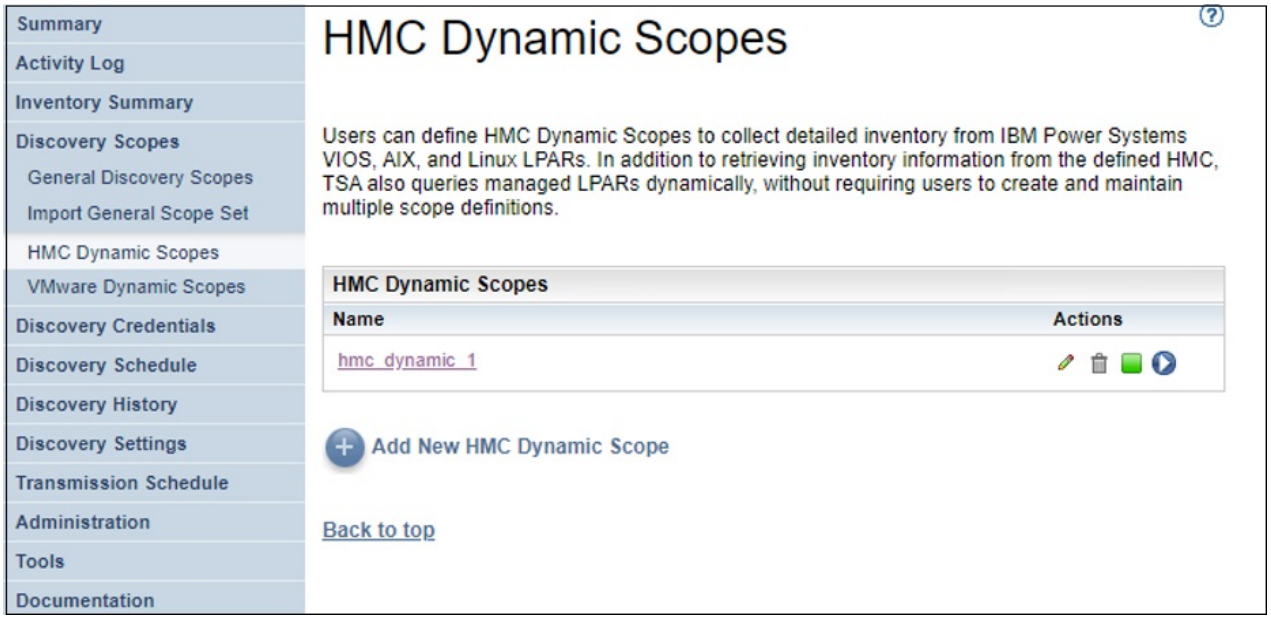

Figura 43. Escopos dinâmicos de HMC

Exibindo escopos dinâmicos do HMC

É possível exibir os escopos dinâmicos existentes do HMC.

Sobre Esta Tarefa

Para exibir os conjuntos de escopos dinâmicos existentes do HMC, clique em **Escopos de descoberta** > **Escopos dinâmicos do HMC** na área de janela de navegação. A página **Escopos dinâmicos de HMC** é exibida. A área de janela **Escopos dinâmicos do HMC** contém uma lista dos escopos dinâmicos do HMC.

Para exibir os escopos e credenciais associados a um conjunto de escopos dinâmicos específico, clique no nome do conjunto de escopos na coluna **Nome**. A página **Conjunto de escopos dinâmicos de HMC** é exibida.

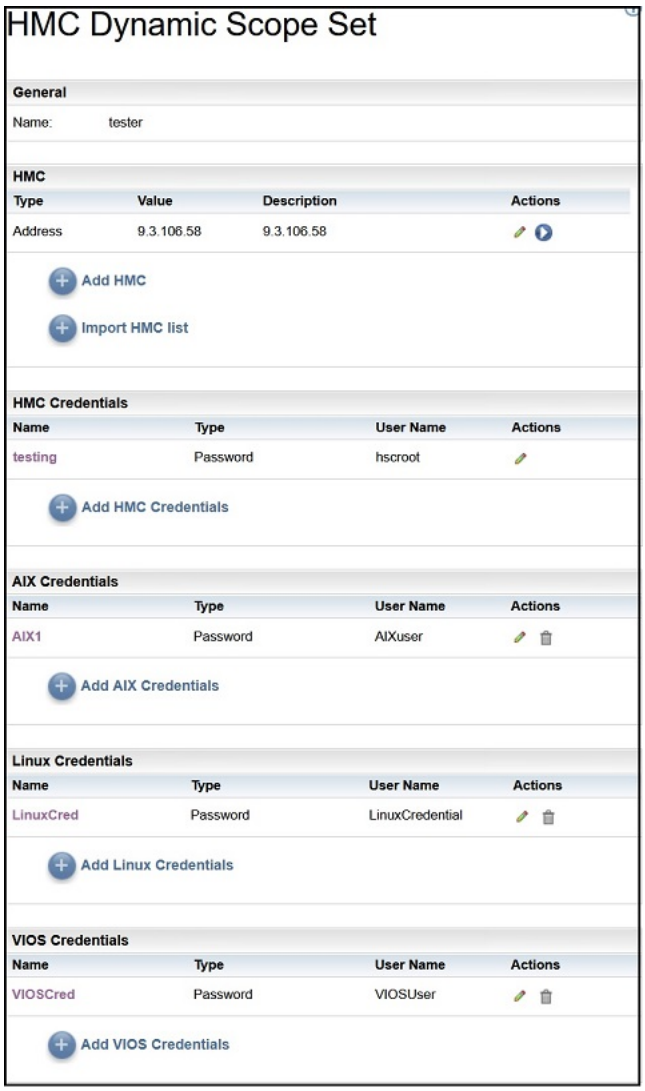

Figura 44. Visualizar o conjunto de escopos dinâmicos de HMC

A área de janela **HMC** exibe a lista de endereços IP dos HMCs que o conjunto de escopos dinâmicos descobre. Se o HMC foi definido usando um nome de host, esse valor é mostrado na coluna **Descrição** da lista do HMC. As várias áreas de janela de credenciais, tais como **Credenciais do AIX**, listam as credenciais que são configuradas no conjunto de escopos.

Incluindo escopos dinâmicos de HMC

Para incluir um Conjunto de escopos dinâmicos do HMC, especifique o endereço IP ou nome de host de um único HMC junto com uma única credencial para acessar o HMC. Opcionalmente, é possível especificar as credenciais para AIX, Linux e VIOS para permitir a descoberta das LPARs do IBM Power Systems que o HMC gerencia. Após a criação do Conjunto de escopos dinâmicos do HMC, é possível editá-lo para definir endereços IP ou nomes do host adicionais do HMC. Também é possível editar os conjuntos de escopos dinâmicos do HMC para oferecer suporte a várias credenciais para acessar os HMCs e várias credenciais para acessar as LPARs.

Sobre Esta Tarefa

Para incluir um conjunto de escopos, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.

A página **Escopos dinâmicos de HMC** é exibida.

2. Para definir um novo conjunto de escopos dinâmicos de HMC, clique em **Incluir um novo escopo dinâmico de HMC**.

   A página **Conjunto de escopos dinâmicos de HMC** é exibida.

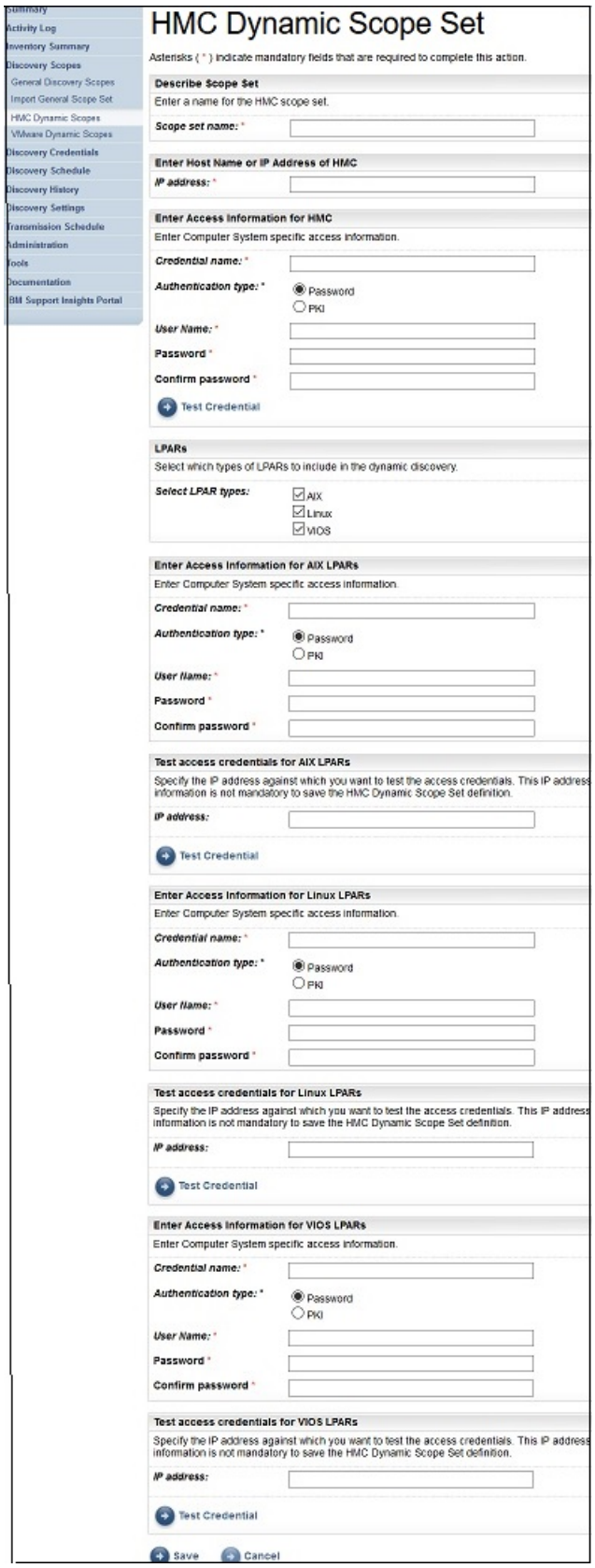

Figura 45. Incluir um conjunto de escopos dinâmicos de HMC

3. Na área de janela **Descrever conjunto de escopos**, insira um nome exclusivo no campo **Nome do conjunto de escopos**.

4. Na área de janela **Inserir nome do host ou endereço IP do HMC**, insira o endereço IP ou o nome do host de HMC.
5. Na área de janela **Inserir informações de acesso para o HMC**, insira os seguintes detalhes:
   a) Insira o **Nome da credencial**
   b) Selecione o **Tipo de autenticação**
      - **Senha** - Usa a senha fornecida.
      - **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.
   c) Insira o **Nome do usuário** usado para a autenticação com o HMC.
   d) Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.
   e) Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.
   f) Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do HMC.
   g) Opcional: Clique em **Testar credencial** para testar as credenciais de HMC de destino.
6. Na área de janela **LPARs**, selecione quais tipos de LPAR (AIX, Linux, VIOS) incluir na descoberta dinâmica.
7. Se você selecionar qualquer um dos tipos de LPAR (AIX, Linux, VIOS), insira as respectivas informações de acesso.

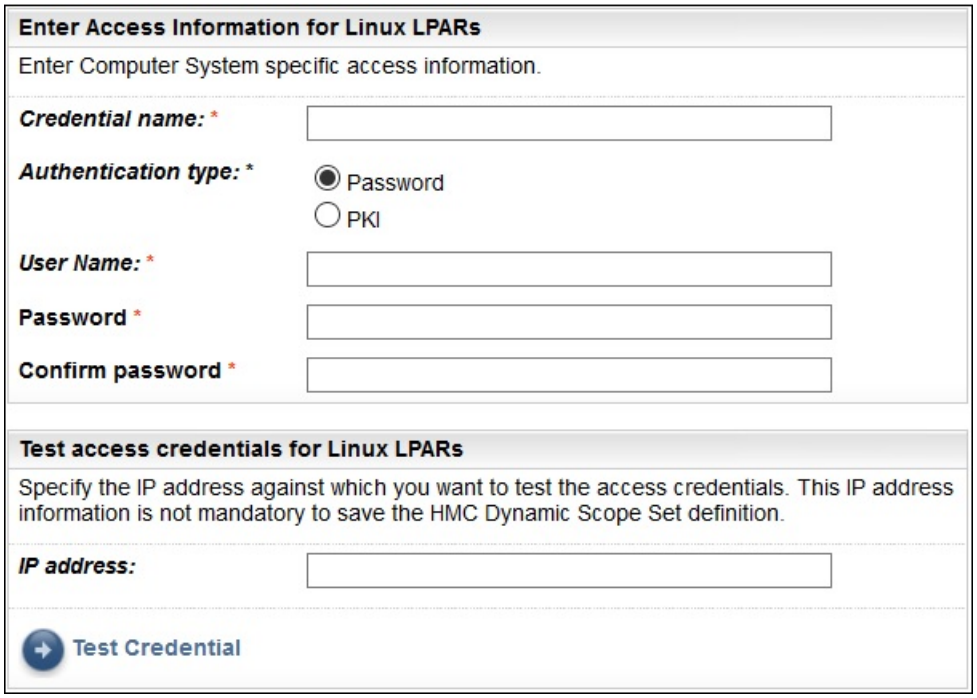

Figura 46. Exemplo: inserir informações de acesso para LPARs Linux

   a) Insira o **Nome da credencial**.
   b) Selecione o **Tipo de autenticação**
      - **Senha** - Usa a senha fornecida.
      - **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.
   c) Insira o **Nome do usuário** que é usado para autenticar a respectiva LPAR.
   d) Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.

e) Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.

f) Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública em cada LPAR.

g) Opcional: Insira o **Endereço IP** de uma LPAR gerenciada por este HMC e clique em **Testar credencial** para testar as credenciais.

8. Clique em **Salvar** para salvar o conjunto de escopos dinâmicos de HMC.

Modificando Escopos dinâmicos do HMC - endereços IP do HMC

É possível modificar a lista de endereços IP do HMC associados a um conjunto de escopos dinâmicos do HMC existente.

Sobre Esta Tarefa

Para modificar a lista de endereços IP do HMC, siga estas etapas.

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida.
2. Para editar o conjunto de escopos, clique no ícone **Editar** ( ).
   A página **Conjunto de escopos dinâmicos de HMC** é exibida.
   - Para incluir um endereço IP ou nome do host no conjunto de escopos, siga estas etapas:
     a. Na área de janela **HMC**, clique em **Incluir HMC**. A página **Escopos dinâmicos de HMC** é exibida.
     b. Insira o endereço IP ou nome do host do HMC no campo **Endereço IP**.
     c. Clique em **Salvar** para incluir o HMC.
   - Para editar um endereço IP do HMC existente no conjunto de escopos, siga estas etapas:
     a. Na área de janela **HMC**, clique no ícone **Editar** ( ). A página **Escopos dinâmicos de HMC** é exibida.
     b. Modifique o campo **Endereço IP** com o endereço IP ou nome do host do HMC na área de janela **Descrever endereço ou host**.
     c. Clique em **Salvar** para modificar o HMC.
   - Para excluir um endereço IP do HMC existente no conjunto de escopos, siga estas etapas:
     a. Na área de janela **HMC**, clique no ícone **Excluir** ( ).
     b. Na caixa de diálogo, clique em **OK** para confirmar a exclusão.

     Nota: Um conjunto de escopos dinâmicos do HMC deve sempre ter pelo menos um endereço IP do HMC definido. O TSA não permite que todos os endereços IP do HMC sejam excluídos.

Importando o Conjunto de escopos dinâmicos do HMC

É possível importar uma lista de endereços IP e nomes de host para um conjunto de escopos dinâmicos do HMC.

Sobre Esta Tarefa

É possível importar uma lista de endereços IP e nomes de host de um arquivo de entrada para um conjunto de escopos dinâmicos do HMC existente. O TSA executa as seguintes validações quando você importa um conjunto de escopos:

- Valida cada linha do arquivo para verificar se é ou não um endereço IP ou nome de host válido.

- Ignora os espaços em branco à direita e à esquerda ao validar o endereço IP ou nome do host.
- Ignora os endereços IP ou nomes de host duplicados.
- Ignora qualquer entrada que tenha o mesmo endereço IP ou nome do host que um endereço IP HMC existente.

Procedimento

Para importar os endereços IP, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida.
2. Clique em um escopo existente na lista. A página **Conjunto de escopos dinâmicos de HMC** é exibida.
3. Na área de janela do HMC, clique em **Importar lista do HMC**. A página **Importar conjunto de escopos dinâmicos de HMC** é exibida.
4. Clique em **Escolher arquivo** para selecionar o arquivo de texto.

   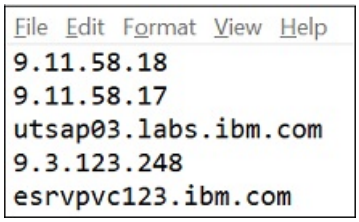

   Figura 47. Importar Conjunto de escopos dinâmicos do HMC

   Nota: O arquivo de texto deve ser formatado como uma única coluna, em que cada linha contém um único endereço IP ou nome de host e nenhum outro dado.
5. Clique em **Importar arquivo** para importar os endereços IP e nomes de host.
6. Clique em **OK** na caixa de diálogo perguntando se deseja importar a lista selecionada. Uma mensagem de status é exibida quando a importação é concluída com sucesso: **`Successfully imported Scope "[n]" IP addresses / hostnames Set`**.

   Nota: Se o arquivo de conjunto de escopos fizer com que o conjunto de escopos dinâmicos do HMC tenha mais de 400 endereços IP, uma mensagem de aviso será exibida - **`This Scope Set resolves to over 400 IP addresses. Para evitar possíveis problemas de desempenho, mantenha o número cumulativo de endereços IP em um Conjunto de escopos abaixo desse limite.`**
7. Depois de importar os endereços IP e nomes de host, é possível editar o escopo dinâmico do HMC definido na página **Escopos de descoberta do HMC** da interface com o usuário.

Modificando escopos dinâmicos do HMC - Credenciais

É possível modificar a lista de credenciais associadas a um conjunto de escopos dinâmicos existente do HMC.

Sobre Esta Tarefa

Um conjunto de escopos dinâmicos do HMC deve sempre ter pelo menos uma credencial do HMC definida. O TSA não permite que todas as credenciais do HMC sejam excluídas. Se não houver credenciais para o AIX, o Linux ou o VIOS, o TSA não coletará informações detalhadas sobre esse tipo de LPAR.

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida.
2. Para editar o conjunto de escopos, clique no ícone **Editar** ( ).
   A página **Conjunto de escopos dinâmicos de HMC** é exibida.

- Para incluir uma credencial para HMC, AIX, Linux ou VIOS, siga estas etapas:
  a. Na área de janela **Credenciais** apropriada, clique em **Incluir credenciais**. Por exemplo, para incluir uma credencial do HMC, clique em **Incluir credenciais do HMC** na área de janela **Credenciais do HMC**. A página **Novas credenciais de descoberta do HMC** é exibida.
  b. Insira o **Nome da credencial**
  c. Selecione o **Tipo de autenticação**
     – **Senha** - Usa a senha fornecida.
     – **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.
  d. Insira o **Nome do usuário** que é usado para autenticação no respectivo HMC ou LPAR.
  e. Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.
  f. Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.
  g. Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do HMCs.
  h. **Opcional:** insira o endereço IP ou nome do host do HMC ou LPAR no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.
  i. Clique em **Salvar** para salvar a credencial do conjunto de escopos dinâmicos do HMC.
- Para editar uma credencial para HMC, AIX, Linux ou VIOS, siga estas etapas:
  a. Na área de janela **Credenciais** apropriada, clique no ícone **Editar** ( ) para a credencial que você deseja modificar. Por exemplo, para editar uma credencial do HMC, clique no ícone **Editar** ( ) na área de janela **Credenciais do HMC** para a credencial a ser modificada. A página **Editar credenciais de descoberta do HMC** é exibida.
  b. Na área de janela **Inserir informações de acesso**, é possível modificar os seguintes detalhes:
     1) Insira o **Nome do usuário** que é usado para autenticação no respectivo HMC ou LPAR.
     2) Selecione o **Tipo de autenticação**
        – **Senha** - Usa a senha fornecida.
        – **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.
     3) Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.
     4) Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.
     5) Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do HMC.
  c. **Opcional:** insira o endereço IP ou nome do host do HMC ou LPAR no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.
  d. Clique em **Salvar** para atualizar a credencial.
- Para excluir uma credencial para HMC, AIX, Linux ou VIOS, siga estas etapas:
  a. Na área de janela **Credenciais** apropriada, clique no ícone **Excluir** ( ) para a respectiva credencial. Por exemplo, para excluir uma credencial do HMC, clique no ícone **Excluir** ( ) na área de janela **Credenciais do HMC** para a credencial a ser excluída. Uma mensagem de confirmação é exibida.
  b. Clique em **OK** para excluir a credencial.
- Para modificar a ordem de uma credencial para HMC, AIX, Linux ou VIOS, siga estas etapas:

a. Se existir mais de uma credencial para o HMC, o AIX, o Linux ou o VIOS, a ordem das credenciais dos HMCs e da LPAR poderá ser modificada. Quando existe uma única credencial, as setas para cima e para baixo não aparecem na coluna **Ações** do painel de credenciais.

b. Na área de janela **Credenciais** apropriada, clique nos ícones **Para cima** ( ) ou **Para baixo** ( ) para reorganizar a credencial.

Ativando ou desativando Conjuntos de escopos dinâmicos

É possível ativar ou desativar um Conjuntos de escopos dinâmicos do HMC.

Sobre Esta Tarefa

Um Conjuntos de escopos desativado é ignorado durante uma descoberta planejada.

Nota: Uma descoberta manual pode sempre ser executada, independentemente do estado do conjunto de escopos.

Desativando Conjuntos de escopos dinâmicos

Procedimento

Para desativar um conjunto de escopos dinâmicos do HMC, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**. A página **Escopos dinâmicos de HMC** é exibida.
2. Clique no ícone **Ativar** ( ) ao lado do conjunto de escopos que você deseja desativar.

Ativando os Conjuntos de escopos dinâmicos

Procedimento

Para ativar um conjunto de escopos dinâmicos do HMC, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**. A página **Escopos dinâmicos de HMC** é exibida.
2. Clique no ícone **Desativar** ( ) ao lado do conjunto de escopos que você deseja ativar.

Descobrindo um HMC

É possível iniciar manualmente uma descoberta de um único HMC dentro de um Conjunto de escopos dinâmicos do HMC. A descoberta coleta informações sobre o HMC junto com suas LPARs associadas.

Procedimento

Para iniciar manualmente uma descoberta de um HMC, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**. A página **Escopos dinâmicos de HMC** é exibida.
2. Clique no ícone **Editar** ( ) para o Conjunto de escopos dinâmicos do HMC necessário. A página **Conjunto de escopos dinâmicos de HMC** é exibida.
3. Clique no ícone **Executar** ( ) ao lado do endereço IP do HMC que você deseja descobrir.

Descobrindo conjuntos de escopos dinâmicos

É possível iniciar manualmente uma descoberta para um Conjunto de escopos dinâmicos do HMC. A descoberta coleta informações sobre todos os HMCs definidos para o conjunto de escopos junto com suas LPARs associadas.

Procedimento

Para iniciar manualmente uma descoberta para um Conjunto de escopos dinâmicos do HMC, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida.
2. Clique no ícone **Executar** ( ) ao lado do conjunto de escopo que você deseja descobrir.

Excluindo escopos dinâmicos de HMC

É possível excluir um conjunto de escopos dinâmicos de HMC existente.

Procedimento

Para excluir um conjunto de escopos dinâmicos de HMC, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida.
2. Clique no ícone **Excluir** ( ) ao lado do conjunto de escopos que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir o conjunto de escopos dinâmicos de HMC.

   Nota: Quando você confirma a exclusão do conjunto de escopos dinâmicos do HMC, as informações de acesso associadas para APARs do AIX, Linux ou VIOS também são excluídas.

Escopos dinâmicos de VMware

É possível definir escopos dinâmicos do VMware para coletar um inventário detalhado das instâncias do VMware vCenter Servers e ESXi. Escopos dinâmicos do VMware também coletam informações sobre os servidores x86 gerenciados pela instância do VMware vCenter Server ou ESXi e as máquinas virtuais Linux e Windows nesses sistemas.

O TSA recupera informações sobre o inventário das instâncias do VMware vCenter Server e ESXi definidas. O TSA também consulta máquinas virtuais que são gerenciadas dinamicamente pelas instâncias do VMware, sem a necessidade de criar e manter várias definições de escopo. Deve-se definir um escopo para as instâncias do VMware e selecionar quais tipos de máquinas virtuais (Linux e Windows) você gostaria de varrer automaticamente quando essas instâncias do VMware forem descobertas. A vantagem é que, mesmo que as máquinas virtuais mudem, não será necessário reconfigurar o TSA.

A descoberta do VMware vCenter Server localiza todas as instâncias do VMware ESXi que ele gerencia, eliminando, assim, a necessidade de descobrir instâncias do VMware ESXi diretamente. Qualquer instância do VMware ESXi não gerenciada por um VMware vCenter Server pode ser descoberta diretamente pelo TSA definindo o VMware ESXi no escopo dinâmico do VMware.

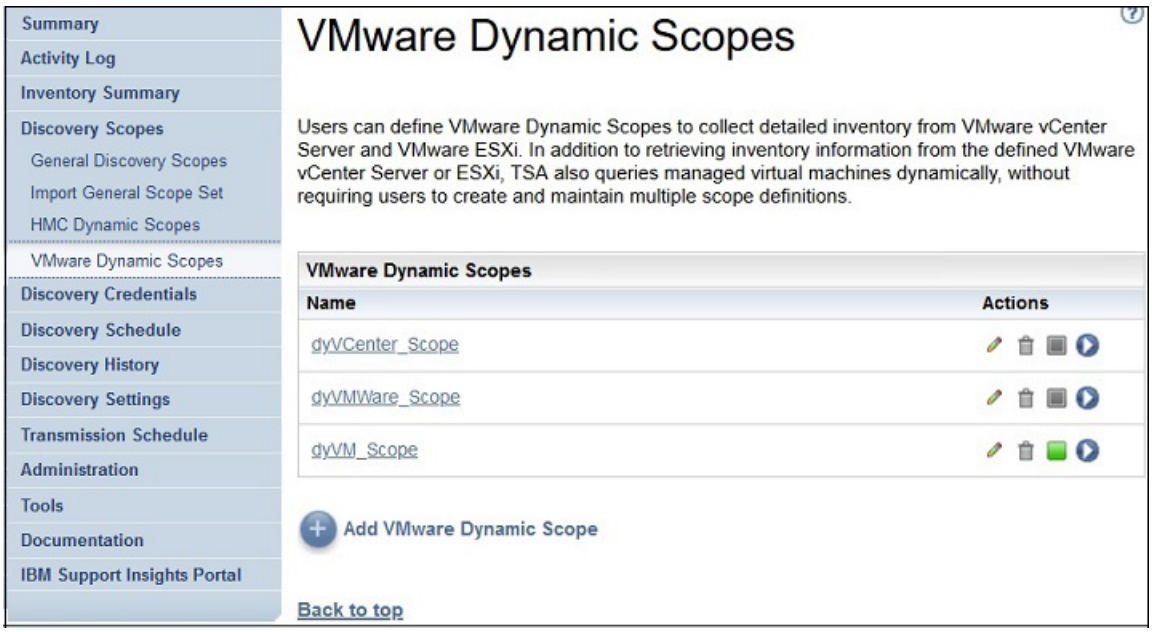

Figura 48. Escopos dinâmicos de VMware

Exibindo Escopos dinâmicos do VMware, conjuntos de escopos e credenciais

É possível exibir os escopos dinâmicos do VMware e conjuntos de escopos existentes.

Sobre Esta Tarefa

Para exibir os conjuntos de escopos dinâmicos do VMware existentes, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware** na área de janela de navegação. A página **Escopos dinâmicos do VMware** é exibida. A área de janela **Escopos dinâmicos do VMware** contém uma lista de escopos dinâmicos do VMware.

Para exibir os escopos e credenciais associados a um conjunto de escopos dinâmicos específico, clique no nome do conjunto de escopos na coluna **Nome**. A página **Conjunto de escopos dinâmicos do VMware** é exibida.

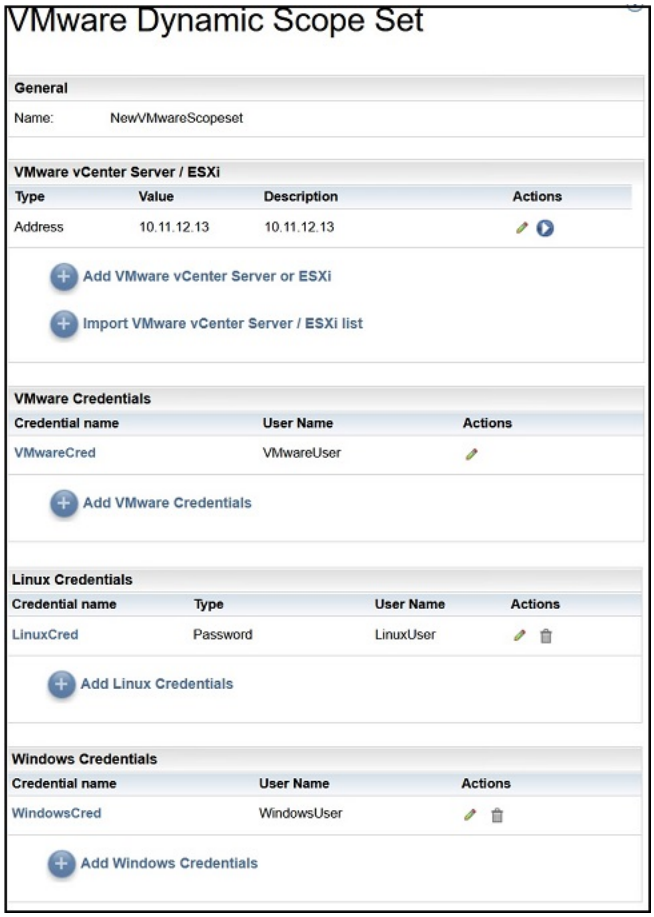

Figura 49. Visualizar Conjunto de escopos dinâmicos do VMware

A área de janela **VMware vCenter Server / ESXi** exibe a lista de endereços IP das instâncias do VMware vCenter Server e ESXi que o conjunto de escopos dinâmicos descobre. Se a instância do VMware vCenter Server ou ESXi foi definida usando um nome de host, esse valor é mostrado na coluna **Descrição** da lista do VMware vCenter Server/ESXi. As várias áreas de janela de credenciais, tais como **Credenciais do Linux**, listam as credenciais que são configuradas no conjunto de escopos.

Incluindo escopos dinâmicos do VMware

Para incluir um Conjunto de escopos dinâmicos do VMware, especifique o endereço IP ou nome de host de uma única instância do VMware vCenter Server ou ESXi junto com uma única credencial para acessar a instância do VMware. Opcionalmente, é possível especificar as credenciais para Linux e Windows para permitir a descoberta das máquinas virtuais dos servidores x86 que a instância do VMware gerencia. Após a criação do Conjunto de escopos dinâmicos do VMware, é possível editá-lo para definir endereços IP ou nomes de host adicionais do VMware vCenter Server ou ESXi. Os conjuntos de escopos dinâmicos do VMware também podem ser editados para oferecer suporte a várias credenciais para acessar a instância do VMware e várias credenciais para acessar as máquinas virtuais.

Sobre Esta Tarefa

Para incluir um conjunto de escopos dinâmicos do VMware, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**. A página **Escopos dinâmicos do VMware** é exibida.

2. Para definir um novo conjunto de escopos dinâmicos do VMware, clique em **Incluir escopo dinâmico do VMware**.

   A página **Conjunto de escopos dinâmicos do VMware** é exibida.

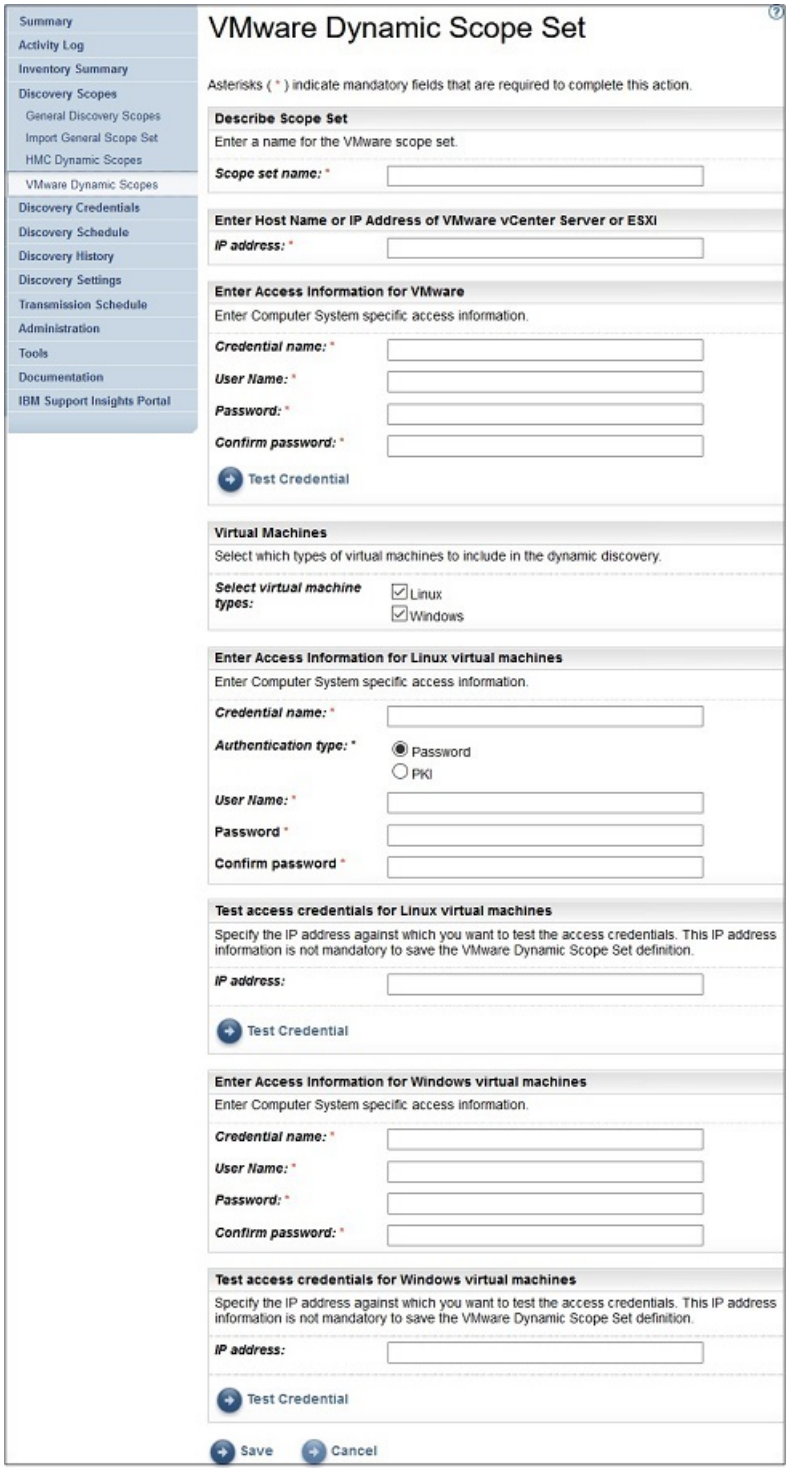

Figura 50. Incluir conjunto de escopos dinâmicos do VMware

3. Na área de janela **Descrever conjunto de escopos**, insira um nome exclusivo no campo **Nome do conjunto de escopos**.
4. Na área de janela **Inserir nome do host ou endereço IP do VMware vCenter Server ou ESXi**, insira o endereço IP ou o nome do host da instância do VMware vCenter Server ou ESXi.
5. Na área de janela **Inserir informações de acesso para o VMware**, insira os seguintes detalhes:
   a) Insira o **Nome da credencial**

b) Insira o **Nome de usuário** usado para autenticação na instância do VMware vCenter Server ou ESXi

c) Insira a **Senha** e **Confirme a senha**

d) Opcional: Clique em **Testar credencial** para testar as credenciais da instância de destino do VMware vCenter Server ou ESXi.

6. Na área de janela **Máquinas virtuais**, selecione quais máquinas virtuais (Linux, Windows) incluir na descoberta dinâmica.
7. Ao selecionar a máquina virtual Linux, insira as informações de acesso respectivas.

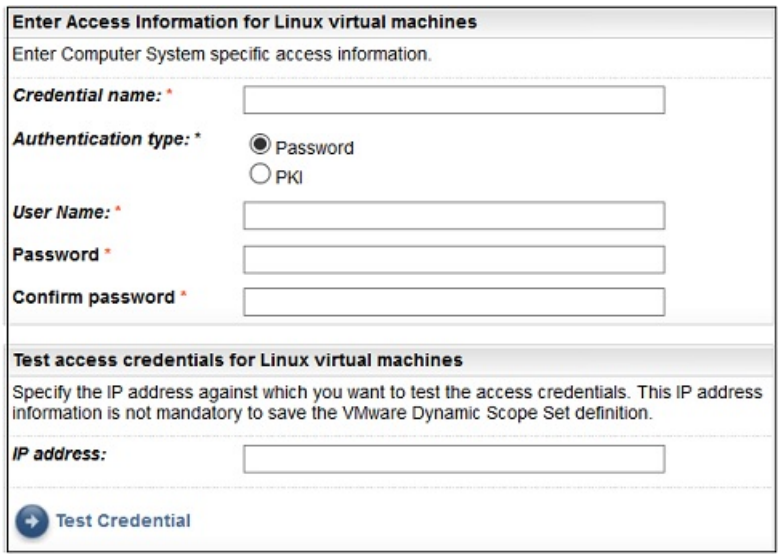

Figura 51. Insira as informações de acesso para máquinas virtuais Linux

a) Insira o **Nome da credencial**.

b) Selecione o **Tipo de autenticação**

- **Senha** - Usa a senha fornecida.
- **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.

c) Insira o **Nome do usuário** que é usado para autenticação da respectiva máquina virtual.

d) Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.

e) Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.

f) Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do Linux.

g) Opcional: Insira o endereço IP ou nome do host de uma máquina virtual Linux no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.

8. Ao selecionar a máquina virtual Windows, insira as informações de acesso respectivas.

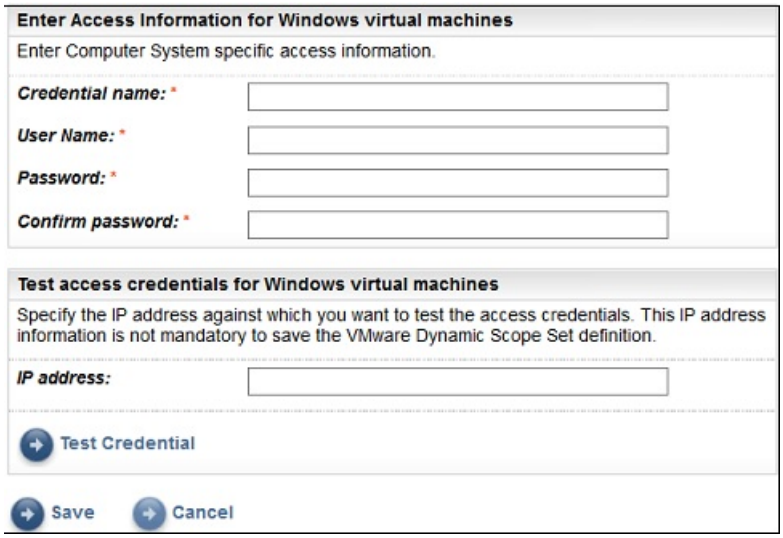

Figura 52. Insira as informações de acesso para máquinas virtuais Windows

a) Insira o **Nome da credencial**.

b) Insira o **Nome do usuário** que é usado para autenticação da respectiva máquina virtual.

c) Insira a **Senha** e **Confirme a senha**.

d) Opcional: Insira o endereço IP ou nome do host de uma máquina virtual Windows no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.

9. Clique em **Salvar** para salvar o conjunto de escopos dinâmicos do VMware.

Modificando endereços IP de Escopos dinâmicos do VMware - VMware vCenter Server ou ESXi

É possível modificar a lista de endereços IP ou nomes de host do VMware vCenter Server ou do ESXi associados a um conjunto de escopos dinâmicos do VMware existente.

Sobre Esta Tarefa

Para modificar a lista de endereços IP ou nomes de host do VMware vCenter Server ou do ESXi, siga estas etapas.

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**.
   A página **Escopos dinâmicos do VMware** é exibida.
2. Para editar o conjunto de escopos, clique no ícone **Editar** ( ).
   A página **Conjunto de escopos dinâmicos do VMware** é exibida.
   - Para incluir um endereço IP ou nome do host do VMware vCenter Server ou do ESXi no conjunto de escopos, siga estas etapas:
     a. Na área de janela **VMware vCenter Server / ESXi**, clique em **Incluir VMware vCenter Server ou ESXi**. A página **Escopos dinâmicos do VMware** é exibida.
     b. Na página **Descrever endereço ou host**, insira o endereço IP ou nome do host do VMware vCenter Server ou do ESXi no campo **Endereço IP**.
     c. Clique em **Salvar** para incluir a instância do VMware vCenter Server ou ESXi.
   - Para editar um endereço IP existente do VMware vCenter Server ou ESXi no conjunto de escopos, siga estas etapas:

a. Na área de janela **VMware vCenter Server/ESXi**, clique no ícone **Editar** ( ). A página **Escopos dinâmicos do VMware** é exibida.

b. Na área de janela **Descrever endereço ou host**, modifique o endereço IP ou nome do host da instância do VMware vCenter Server ou do ESXi no campo **Endereço IP**.

c. Clique em **Salvar**.

- Para excluir um endereço IP existente do VMware vCenter Server ou ESXi no conjunto de escopos, siga estas etapas:

a. Na área de janela **VMware vCenter Server/ESXi**, clique no ícone **Excluir** ( ).

b. Na caixa de diálogo, clique em **OK** para confirmar a exclusão.

Nota: Um conjunto de escopos dinâmicos do VMware deve ter sempre pelo menos um endereço IP do VMware vCenter Server ou ESXi definido. O TSA não permite que todos os endereços IP do VMware sejam excluídos.

Importando o Conjunto de escopos dinâmicos do VMware

É possível importar uma lista de endereços IP e nomes de host para um Conjunto de escopos dinâmicos do VMware.

Sobre Esta Tarefa

É possível importar uma lista de endereços IP ou nomes de host de um arquivo de entrada para um conjunto de escopos dinâmicos do VMware existente. O TSA executa as seguintes validações quando você importa um conjunto de escopos:

- Valida cada linha do arquivo para verificar se é ou não um endereço IP ou nome de host válido.
- Ignora os espaços em branco à direita e à esquerda ao validar o endereço IP ou nome do host.
- Ignora os endereços IP ou nomes de host duplicados.
- Ignora qualquer entrada que tenha o mesmo endereço IP ou nome do host que um endereço VMware vCenter Server ou ESXi existente.

Procedimento

Para importar os endereços IP, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**.
   A página **Escopos dinâmicos do VMware** é exibida.
2. Clique em um escopo existente na lista. A página **Conjunto de escopos dinâmicos do VMware** é exibida.
3. Na área de janela **VMware vCenter Server / ESXi**, clique em **Importar lista de VMware vCenter Server / ESXi**. A página **Importar conjunto de escopos dinâmicos do VMware** é exibida.
4. Clique em **Escolher arquivo** para selecionar o arquivo de texto.

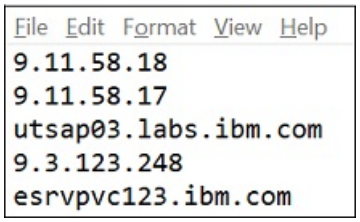

Figura 53. Importar conjunto de escopos dinâmicos do VMware

Nota: O arquivo de texto deve ser formatado como uma única coluna, em que cada linha contém um único endereço IP ou nome de host e nenhum outro dado.

5. Clique em **Importar arquivo** para importar os endereços IP e nomes de host.

6. Clique em **OK** na caixa de diálogo perguntando se deseja importar a lista selecionada. Uma mensagem de status é exibida quando a importação é concluída com sucesso: **Successfully imported Scope "[n]" IP addresses / hostnames Set**.

   Nota: Se o arquivo de conjunto de escopos fizer com que o conjunto de escopos dinâmicos do VMware tenha mais de 400 endereços IP, uma mensagem de aviso será exibida - **This Scope Set resolves to over 400 IP addresses. To avoid potential performance issues keep the cumulative number of IP addresses in a Scope Set below this threshold.**
7. Depois de importar os endereços IP e nomes de host, é possível editar o escopo dinâmico do VMware definido na página **VMware Discovery Scopes** da interface com o usuário.

Modificando Conjuntos de escopos dinâmicos do VMware - Credenciais

É possível modificar a lista de credenciais associadas a um Conjunto de escopos dinâmicos do VMware existente.

Sobre Esta Tarefa

Um conjunto de escopos dinâmicos do VMware sempre deve ter pelo menos uma credencial do VMware definida. O TSA não permite que todas as credenciais do VMware sejam excluídas. Se não houver credenciais para Linux ou Windows, o TSA não coletará informações detalhadas sobre esse tipo de máquina virtual.

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**.
   A página **Escopos dinâmicos do VMware** é exibida.
2. Para editar o conjunto de escopos, clique no ícone **Editar** .
   A página **Conjunto de escopos dinâmicos do VMware** é exibida.
   - Para incluir uma credencial para o VMware ou o Windows, siga as etapas a seguir:
     a. Na área de janela **Credenciais** apropriada, clique em **Incluir credenciais**. Por exemplo, para incluir uma credencial do VMware, clique em **Incluir credenciais do VMWare** na área de janela **Credenciais do VMWare**. A página **Novas credenciais de descoberta do VMware** é exibida.
     b. Insira o **Nome da credencial**
     c. Insira o **Nome de usuário** usado para a autenticação nas instâncias do VMware vCenter Server ou do ESXi ou nas respectivas máquinas virtuais.
     d. Insira a **Senha** e **Confirme a senha**.
     e. **Opcional:** insira o endereço IP ou nome do host da instância do VMware vCenter Server ou ESXi ou máquina virtual Windows, no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.
     f. Clique em **Salvar** para salvar a credencial.
   - Para incluir uma credencial no Linux, siga estas etapas:
     a. Na área de janela **Credenciais do Linux**, clique em **Incluir credenciais do Linux**. A página **Novas credenciais de descoberta do VMware** é exibida.
     b. Insira o **Nome da credencial**
     c. Selecione o **Tipo de autenticação**
        – **Senha** - Usa a senha fornecida.
        – **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.
     d. Insira o **Nome de usuário** usado para a autenticação nas máquinas virtuais do Linux.
     e. Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.

f. Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.

g. Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do Linux.

h. **Opcional:** insira o endereço IP ou nome do host da máquina virtual Linux, no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.

i. Clique em **Salvar** para salvar a credencial do Linux.

- Para editar uma credencial para o VMware ou o Windows, siga as etapas a seguir:

  a. Na área de janela **Credenciais** apropriada, clique no ícone **Editar** ( ) para a credencial que você deseja modificar. Por exemplo, para editar uma credencial do VMware, clique no ícone **Editar** ( ) na área de janela **Credenciais do VMware** para a credencial a ser modificada. A página **Editar credenciais de descoberta do VMware** é exibida.

  b. Na área de janela **Inserir informações de acesso**, é possível modificar os seguintes detalhes:

     1) Insira o **Nome do usuário** usado para autenticação ao se conectar às instâncias do VMware vCenter Server ou ESXi ou máquinas virtuais do Windows.

     2) Insira a **Senha** e **Confirme a senha**.

  c. **Opcional:** insira o endereço IP ou nome do host da instância do VMware vCenter Server ou ESXi ou máquina virtual Windows, no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.

  d. Clique em **Salvar** para atualizar a credencial.

- Para editar uma credencial para o Linux, siga as etapas a seguir:

  a. Na área de janela **Credenciais do Linux**, clique no ícone **Editar** ( ) para a credencial que você deseja modificar. A página **Editar credenciais de descoberta do VMware** é exibida.

  b. Na área de janela **Inserir informações de acesso**, é possível modificar os seguintes detalhes:

     1) Selecione o **Tipo de autenticação**

        – **Senha** - Usa a senha fornecida.

        – **PKI** - Usa a chave SSH que está associada ao conjunto de escopos específico.

     2) Insira o **Nome de usuário** usado para a autenticação nas máquinas virtuais Linux.

     3) Quando **Tipo de autenticação** for **Senha**, insira a **Senha** e **Confirme a senha**.

     4) Quando **Tipo de autenticação** for **PKI**, insira a **Passphrase** e **Confirme a passphrase** se a chave SSH estiver criptografada. Se a chave SSH não estiver criptografada, deixe esses dois campos em branco.

     5) Se **Tipo de autenticação** for **PKI**, clique em **Escolher arquivo** e faça upload da chave privada para o TSA. Deve-se implementar externamente a chave pública nas máquinas virtuais do Linux.

     6) **Opcional:** insira o endereço IP ou nome do host de uma máquina virtual Linux no campo **Endereço IP** e clique em **Testar credencial** para testar as credenciais.

  c. Clique em **Salvar** para atualizar a credencial.

- Para excluir uma credencial para o VMware, Linux ou Windows, siga estas etapas:

  a. Na área de janela **Credenciais** apropriada, clique no ícone **Excluir** ( ) para a respectiva credencial. Por exemplo, para excluir a credencial do VMware, clique no ícone **Excluir** ( ) na área de janela **Credenciais do VMware** para a credencial a ser excluída. Uma mensagem de confirmação é exibida.

  b. Clique em **OK** para excluir a credencial.

- Para modificar a ordem de uma credencial para o VMware, Linux ou Windows, siga estas etapas:

a. Se existir mais de uma credencial para o VMware, Linux ou Windows, a ordem das credenciais para o VMwares ou máquinas virtuais poderá ser modificada. Quando existe uma única credencial, as setas para cima e para baixo não aparecem na coluna **Ações** do painel de credenciais.

b. Na área de janela **Credenciais** apropriada, clique nos ícones **Para cima** ( ) ou **Para baixo** ( ) para reorganizar a credencial.

Ativando ou desativando Conjuntos de escopos dinâmicos

É possível ativar ou desativar um Conjuntos de escopos dinâmicos do VMware.

Sobre Esta Tarefa

Um Conjuntos de escopos desativado é ignorado durante uma descoberta planejada.

Nota: Uma descoberta manual pode sempre ser executada, independentemente do estado do conjunto de escopos.

Desativando Conjuntos de escopos dinâmicos

Procedimento

Para desativar um conjunto de escopos dinâmicos do VMware, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**. A página **Escopos dinâmicos do VMware** é exibida.
2. Clique no ícone **Ativar** ( ) ao lado do conjunto de escopos que você deseja desativar.

Ativando os Conjuntos de escopos dinâmicos

Procedimento

Para ativar um conjunto de escopos dinâmicos do VMware, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**. A página **Escopos dinâmicos do VMware** é exibida.
2. Clique no ícone **Desativar** ( ) ao lado do conjunto de escopos que você deseja ativar.

Descobrindo um VMware vCenter ou ESXi

É possível iniciar manualmente uma descoberta de um único VMware vCenter Server ou ESXi dentro de um conjunto de escopos dinâmicos do VMware. A descoberta coleta informações sobre a instância do VMware junto com as suas máquinas virtuais associadas.

Procedimento

Para iniciar manualmente uma descoberta de um VMware vCenter Server ou ESXi, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**. A página **Escopos dinâmicos do VMware** é exibida.
2. Clique no ícone **Editar** ( ) para o Conjunto de escopos dinâmicos do VMware. A página **Conjunto de escopos dinâmicos do VMware** é exibida.
3. Clique no ícone **Executar** ( ) ao lado do endereço IP do VMware vCenter Server ou do ESXi que você deseja descobrir.

Descobrindo conjuntos de escopos dinâmicos

É possível iniciar manualmente uma descoberta para um conjunto de escopos dinâmicos do VMware. A descoberta coleta informações sobre todas as instâncias do VMware vCenter Server ou do ESXi definidas para o conjunto de escopos junto com suas máquinas virtuais associadas.

Procedimento

Para iniciar manualmente uma descoberta para um conjunto de escopos dinâmicos do VMware, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMware**.
   A página **Escopos dinâmicos do VMware** é exibida.
2. Clique no ícone **Executar** ( ) ao lado do conjunto de escopos que você deseja descobrir.

Excluindo escopos dinâmicos do VMware

É possível excluir um conjunto de escopos dinâmicos do VMware existente.

Procedimento

Para excluir um conjunto de escopos dinâmicos do VMware, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos dinâmicos do VMware**.
   A página **Escopos dinâmicos do VMware** é exibida.
2. Clique no ícone **Excluir** ( ) ao lado do conjunto de escopos que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir o conjunto de escopos dinâmicos do VMware.

   Nota: Quando você confirma a exclusão do conjunto de escopos dinâmicos do VMware, as informações de acesso associadas para máquinas virtuais Linux ou Windows também são excluídas.

Escopos gerais de descoberta

O processo de descoberta procura elementos de TI em sua infraestrutura. Um Escopo de descoberta define um único endereço IP, intervalo ou sub-rede que é descoberto durante o processo de descoberta. Os escopos de descoberta são agrupados em conjuntos de escopos com nomes dos usuários.

Exibindo escopos de descoberta e conjuntos de escopos

É possível exibir os escopos de descoberta e conjuntos de escopos existentes.

Sobre Esta Tarefa

Para exibir os conjuntos de escopos de descoberta existentes, clique em **Escopo da descoberta** > **Escopos gerais de descoberta** na área de janela de navegação. A página **Escopos gerais de descoberta** é exibida. A área de janela **Escopos de descoberta gerais** contém uma lista dos conjuntos de escopos.

Para exibir os escopos que um conjunto de escopos contém, clique no conjunto de escopos. A página **Conjunto de escopos de descoberta** é exibida.

- A área de janela **Geral** exibe o nome do conjunto de escopos.
- A área de janela **Contagem de endereços IP** exibe o número total de endereços IP no conjunto de escopos específico.
- A área de janela **Escopos** exibe detalhes sobre os escopos no conjunto de escopos.

Incluindo escopos da descoberta

É possível incluir um conjunto de escopos e um novo escopo nesse conjunto, incluir um escopo em um conjunto de escopos existente ou mover escopos para outros conjuntos de escopos. Para incluir um

escopo, especifique um endereço IP ou nome do host, um intervalo de endereços IP, uma rede ou uma sub-rede válida.

Sobre Esta Tarefa

Dicas: Existem algumas considerações práticas para configurar escopos de descoberta e conjuntos de escopos.

- Quanto mais endereços IP houver no escopo da descoberta, maior será a duração da descoberta. É possível modificar o tamanho da descoberta desativando ou ativando conjuntos de escopos ou excluindo endereços IP, intervalos de endereços IP, redes ou sub-redes de um escopo em um conjunto de escopos.

  Para minimizar o tempo que uma descoberta leva para ser executada, configure escopos de descoberta para segmentar apenas os elementos que você deseja descobrir e desativar os conjuntos de escopos ou excluir endereços IP, intervalos de endereços IP, redes ou sub-redes que você não deseja ou que não precisa descobrir.

  Nota: Para um melhor desempenho, limite o número cumulativo de endereços IP em um escopo definido para 400 ou menos. Para obter informações sobre como importar um conjunto de escopos, consulte a seção "Importando um conjunto de escopos" na página 74
- Nem todos os elementos são iguais. Por exemplo, um roteador com dezenas de interfaces pode levar mais tempo para ser completamente descoberto do que um único host.
- Se você estiver usando a autenticação PKI para descoberta de dispositivo, apenas uma chave SSH poderá ser associada a cada conjunto de escopos.

Para obter mais informações sobre melhores práticas para configurar escopos de descoberta, consulte o TSA Configuration Assistant Guide.

Para incluir um conjunto de escopos e um escopo, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.
   A página **Escopos gerais de descoberta** é exibida.
2. Para definir um novo conjunto de escopos de descoberta, clique em **Incluir novo conjunto de escopos**.
   A página **Conjunto de escopos de descoberta** é exibida.

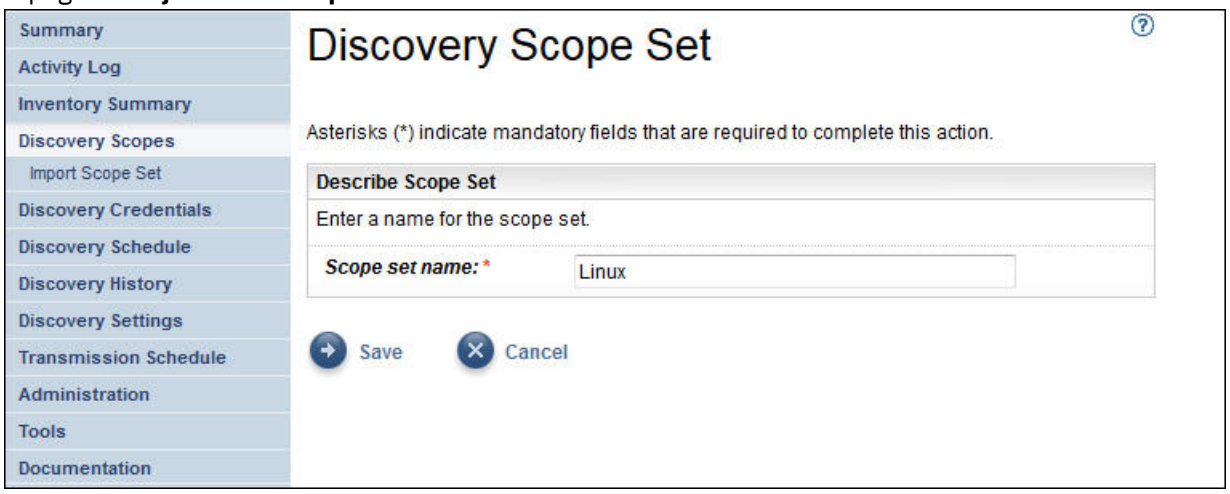

Figura 54. Conjunto de escopos de descoberta

   a) Insira um nome exclusivo de conjunto de escopos no campo de nome **Conjunto de escopos**
   b) Clique em **Salvar**.
      O novo conjunto de escopos é criado e a página **Escopos gerais de descoberta** é exibida.

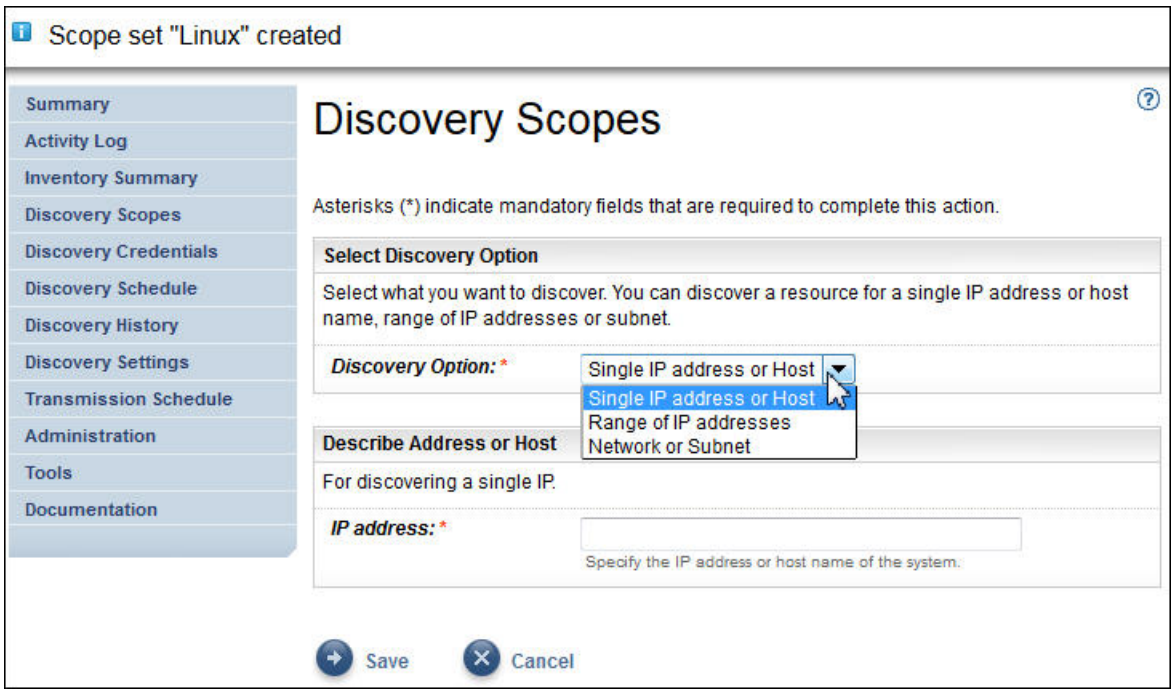

Figura 55. Escopos gerais de descoberta

3. Especifique uma das opções a seguir na área de janela **Selecionar opção de descoberta**:
   - `Endereço IP ou host único`

     Para **Descrever o endereço ou o host**, insira o endereço IP ou o nome do host.
   - `Intervalo de endereços IP`

     Para **Descrever intervalo de endereços**, insira o endereço IP inicial, o endereço IP final e, opcionalmente, uma descrição nos campos fornecidos.
   - `Rede ou sub-rede`

     Para **Descrever a rede ou a sub-rede**, insira o endereço IP, a máscara e, opcionalmente, uma descrição nos campos fornecidos.
4. Se você deseja excluir endereços IP, intervalo de endereços IP ou sub-redes da descoberta, clique em **Incluir exclusão** e siga estas etapas:
   a) Selecione **Host**, **Intervalo** ou **Sub-rede**.
   b) Especifique o endereço IP, o intervalo de endereços IP ou a sub-rede que você deseja excluir da descoberta.
   c) Opcional: Especifique uma descrição para o endereço IP, o intervalo de endereços IP ou a sub-rede que você está excluindo da descoberta.

      Nota: As exclusões são aplicáveis somente para um escopo definido com um intervalo de endereços IP ou uma sub-rede.

      Nota: Não é possível reutilizar um endereço IP, intervalo de endereços IP, sub-redes ou descrição em nenhum escopo ou exclusão em um conjunto de escopos.
   d) Para incluir mais exclusões, clique em **Incluir exclusão** e siga as etapas anteriores para definir mais exclusões.
5. Clique em **Salvar** para salvar o escopo e as exclusões. A página **Conjunto de escopos de descoberta** é exibida com o novo escopo na lista.
6. Para incluir mais escopos nesse conjunto de escopos, clique em **Incluir novo escopo** e siga as etapas anteriores para definir mais escopos.

   Nota: Para um melhor desempenho, limite o número cumulativo de endereços IP em um escopo definido para 400 ou menos.

Incluindo um escopo da descoberta em um conjunto de escopos existente

É possível incluir um escopo em um conjunto de escopos existente.

Procedimento

Para incluir um escopo em um conjunto de escopos existente, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.

   A página **Escopos gerais de descoberta** é exibida.
2. Na área de janela **Escopos gerais de descoberta**, clique no conjunto de escopos no qual deseja incluir um escopo.

   A página **Conjunto de escopos de descoberta** é exibida.
3. Clique em **Incluir novo escopo**.

   A página **Escopos gerais de descoberta** é exibida.
4. Na área de janela **Selecionar opção de descoberta**, especifique uma das seguintes opções.

   - `Endereço IP ou host único`

     Para **Descrever o endereço ou o host**, insira o endereço IP ou o nome do host.
   - `Intervalo de endereços IP`

     Para **Descrever intervalo de endereços**, insira o endereço IP inicial, o endereço IP final e, opcionalmente, uma descrição nos campos fornecidos.
   - `Rede ou sub-rede`

     Para **Descrever a rede ou a sub-rede**, insira o endereço IP, a máscara e, opcionalmente, uma descrição nos campos fornecidos.
5. Se você deseja excluir endereços IP, intervalo de endereços IP ou sub-redes da descoberta, clique em **Incluir exclusão** e siga estas etapas:

   a) Selecione **Host**, **Intervalo** ou **Sub-rede**.

   b) Especifique o endereço IP, o intervalo de endereços IP ou a sub-rede que você deseja excluir da descoberta.

   c) Opcional: Especifique uma descrição para o endereço IP, o intervalo de endereços IP ou a sub-rede que você está excluindo da descoberta.

   Nota: As exclusões são aplicáveis somente para um escopo definido com um intervalo de endereços IP ou uma sub-rede.

   Nota: Não é possível reutilizar um endereço IP, intervalo de endereços IP, sub-redes ou descrição em nenhum escopo ou exclusão em um conjunto de escopos.

   d) Para incluir mais exclusões, clique em **Incluir exclusão** e siga as etapas anteriores para definir mais exclusões.
6. Clique em **Salvar** para salvar o escopo e as exclusões.

   A página **Conjunto de escopos de descoberta** é exibida com o novo escopo na lista.

Modificando um conjunto de escopos de descoberta

É possível modificar um conjunto de escopos de descoberta existente, mudando as configurações do conjunto de escopos.

Sobre Esta Tarefa

Para modificar um conjunto de escopos de descoberta existente, siga estas etapas.

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.

A página **Escopos gerais de descoberta** é exibida.

2. Para editar o conjunto de escopos, clique no ícone **Editar** ( ) ao lado do conjunto de escopos.

   A página **Conjunto de escopos de descoberta** é exibida. É possível editar o conjunto de escopos editando um escopo, incluindo um escopo, movendo um escopo para outro conjunto de escopos ou excluindo um escopo.

   - Para incluir um escopo, siga estas etapas:
     a. Clique em **Incluir novo escopo**.
     b. Na área de janela **Selecionar opção de descoberta**, especifique uma das seguintes opções:
        – `Endereço IP/host único`

          Para **Descrever o endereço ou o host**, insira o endereço IP ou o nome do host.
        – `Intervalo de endereços IP`

          Para **Descrever intervalo de endereços**, digite o endereço IP inicial, o endereço IP final e, opcionalmente, uma descrição nos campos fornecidos.
        – `Rede ou sub-rede`

          Para **Descrever a rede ou a sub-rede**, digite o endereço IP, a máscara e, opcionalmente, uma descrição nos campos fornecidos.

        Nota: Forneça um nome exclusivo para **Descrição**. Se você especificar a descrição já existente para qualquer outro escopo dentro do conjunto de escopos, o TSA não permitirá que você crie um escopo. Se o campo **Descrição** for deixado em branco, o TSA criará automaticamente a descrição usando o intervalo de endereço IP/máscara de sub-rede.
     c. Se você desejar excluir endereços IP ou sub-redes da descoberta, clique em **Incluir exclusão** e siga estas etapas:
        1) Selecione **Host**, **Intervalo** ou **Sub-rede**.
        2) Especifique o endereço IP, o intervalo de endereços IP ou a sub-rede que você deseja excluir da descoberta.
        3) Para incluir mais exclusões, clique em **Incluir exclusão** e siga as etapas anteriores para definir mais exclusões.
     d. Clique em **Salvar** para salvar o escopo e as exclusões. A página **Conjunto de escopos de descoberta** é exibida com o novo escopo na lista.
   - Para mover um escopo para outro conjunto de escopos, siga estas etapas:
     a. Clique em **Mover escopos**.
     b. Na página **Mover escopos de um conjunto para outro**, selecione os escopos que você deseja mover da lista **Escopos**.
     c. Selecione o conjunto de escopos na lista **Conjunto de escopos de destino** para o qual você deseja mover os escopos.
     d. Clique em **Mover**.
   - Para editar um escopo, siga estas etapas:
     a. Clique no ícone **Editar** ( ) de um escopo específico.
     b. É possível modificar a **Opção de descoberta**, **Endereços IP**, **Exclusões** etc.
     c. Clique em **Salvar** para salvar o escopo e as exclusões. A página **Conjunto de escopos de descoberta** é exibida com o novo escopo na lista.
   - Para excluir um escopo, siga estas etapas:
     a. Clique no ícone **Excluir** ( ) ao lado do escopo que você deseja excluir.
     b. Clique em **OK** para confirmar que você deseja excluir o escopo da descoberta.

Excluindo escopos da descoberta

É possível excluir escopos de descoberta existentes em um conjunto de escopos ou excluir conjuntos de escopos inteiros.

Sobre Esta Tarefa

Procedimento

Para excluir um escopo da descoberta, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.
   A página **Escopos gerais de descoberta** é exibida.
2. Edite o conjunto de escopos que contém o escopo de descoberta que você deseja excluir clicando no ícone **Editar** ( ) ao lado do conjunto de escopo.
   A página **Conjunto de escopos de descoberta** é exibida.
3. Clique no ícone **Excluir** ( ) ao lado do escopo que você deseja excluir.
4. Clique em **OK** para confirmar que você deseja excluir o escopo da descoberta.

Excluindo conjuntos de escopos de descoberta

É possível excluir conjuntos de escopos de descoberta existentes.

Procedimento

Nota: Antes de excluir um conjunto de escopos, deve-se excluir todas as credenciais associadas ao conjunto de escopos.

Para excluir um conjunto de escopos de descoberta, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.
   A página **Escopos gerais de descoberta** é exibida.
2. Clique no ícone **Excluir** ( ) ao lado do conjunto de escopo que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir o conjunto de escopos de descoberta.

Importando um conjunto de escopos

É possível importar uma lista de endereços IP ou nomes de host para definir um novo conjunto de escopos.

Sobre Esta Tarefa

Um novo conjunto de escopos é criado com base no nome especificado e na lista de endereços IP ou nomes de host do arquivo de entrada. O TSA executa as seguintes validações quando você importa um conjunto de escopos:

- Verifica se o nome do conjunto de escopos já existe.
- Valida cada linha do arquivo para verificar se é ou não um endereço IP/nome de host válido.
- Ignora os espaços em branco à direita e à esquerda ao validar o endereço IP ou nome do host.
- Ignora os endereços IP ou nomes de host duplicados.

Procedimento

Para importar os endereços IP ou nomes do host, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Importar escopos gerais de descoberta**.
   A página **Importar conjunto de escopos gerais** é exibida.

2. Insira o **Nome do novo conjunto de escopos**.

   Nota: Insira um nome exclusivo que não seja usado por nenhum conjunto de escopos existente. Uma mensagem de erro será exibida se o nome de um conjunto de escopos existente for inserido: `Scope set name already exists`.
3. Clique em **Escolher arquivo** para selecionar o arquivo de texto.

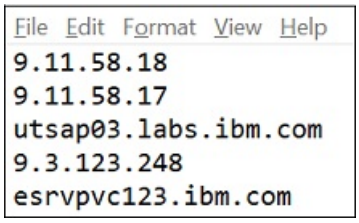

   Figura 56. Importar conjunto de escopos

   Nota: O arquivo de texto deve ser formatado como uma única coluna, em que cada linha contém um único endereço IP ou nome de host e nenhum outro dado.
4. Clique em **Importar arquivo de conjunto de escopos** para importar o conjunto de escopos. Uma mensagem de status é exibida quando a importação é concluída com sucesso: **`Successfully imported Scope Set`**.

   Nota: Se o arquivo do conjunto de escopos tiver mais de 400 endereços IP, uma mensagem de aviso será exibida: **`Successfully imported Scope Set. But the number of scope elements is beyond the recommended guidelines, limit it to 400 for better performance.`**
5. Após importar o conjunto de escopos, será possível editar o conjunto de escopos na seção **Escopos gerais de descoberta** da interface com o usuário e associar as credenciais na seção **Credenciais de descoberta**.

Configurações de descoberta

Use a página **Configurações de descoberta** para ajustar as configurações avançadas de descoberta.

Definindo configurações de conexão

Use a página **Configurações de conexão** para configurar a descoberta SLP e descobrir os dispositivos de armazenamento EMC por meio de provedores EMC SMI-S.

Sobre Esta Tarefa

Por padrão, a tarefa de descoberta tenta encontrar provedores EMC SMI-S executando uma consulta SLP para determinar o endereço IP e a porta deles. Se o SLP não estiver disponível na sua rede (por exemplo, se houver políticas de segurança que bloqueiam as mensagens SLP), a descoberta de dispositivos de armazenamento EMC ainda poderá ser feita desativando a Descoberta SLP e configurando as portas nas quais o Provedor SMI-S do EMC atende às solicitações de consulta.

Procedimento

1. Selecione as opções **Ativar** ou **Desativar** para ativar ou desativar a descoberta SLP.

   Nota: Por padrão, a descoberta SLP está ativada.
2. Se você desativar a descoberta SLP, deverá configurar uma ou mais portas de conexão do Provedor SMI-S do EMC
   a) **Porta(s) HTTPS SMI-S do EMC:** 5989 é a porta HTTPS padrão na qual o Provedor SMI-S do EMC atende às solicitações de consulta. Se você especificar várias portas, separe-as com vírgulas. O

SMI-S de EMC atende nessas portas para solicitações de conexão (tais como do TSA). O TSA precisa conhecer essa porta para iniciar a conexão.

b) **Porta(s) HTTP SMI-S do EMC:** 5988 é a porta HTTP padrão na qual o Provedor SMI-S de EMC atende às solicitações de consulta. O TSA tenta primeiro uma conexão HTTPS (se configurada) e, se falhar, tenta se conectar através das portas HTTP definidas. Se você deseja evitar conexões HTTP, não defina portas HTTP. Se você especificar várias portas HTTP, separe-as com vírgulas. O SMI-S de EMC atende nessas portas para solicitações de conexão (tais como do TSA). O TSA precisa conhecer essa porta para iniciar a conexão.

3. Clique em **Salvar** para salvar as configurações de conexão. Você receberá uma mensagem: *The discovery connection settings were successfully saved.*

Credenciais de descoberta

As credenciais de descoberta consistem nos nomes de usuário, nas senhas ou nas chaves SSH e nas sequências de comunidade de SNMP (Protocolo Simples de Gerenciamento de Rede) que o TSA usa para acessar recursos configurados nos **Escopos de descoberta geral** durante a descoberta.

Exibindo credenciais

O processo de descoberta requer credenciais, tais como IDs dos usuários e senhas, para acessar recursos.

Sobre Esta Tarefa

Importante: As informações de acesso especificadas devem corresponder às informações de acesso do recurso de destino da descoberta. Se você alterar as informações de acesso, como a senha, em um recurso de destino, também altere as informações de acesso do Technical Support Appliance associado.

É possível exibir as credenciais existentes clicando em **Credenciais de descoberta** na área de janela de navegação. A página **Credenciais de descoberta** é exibida.

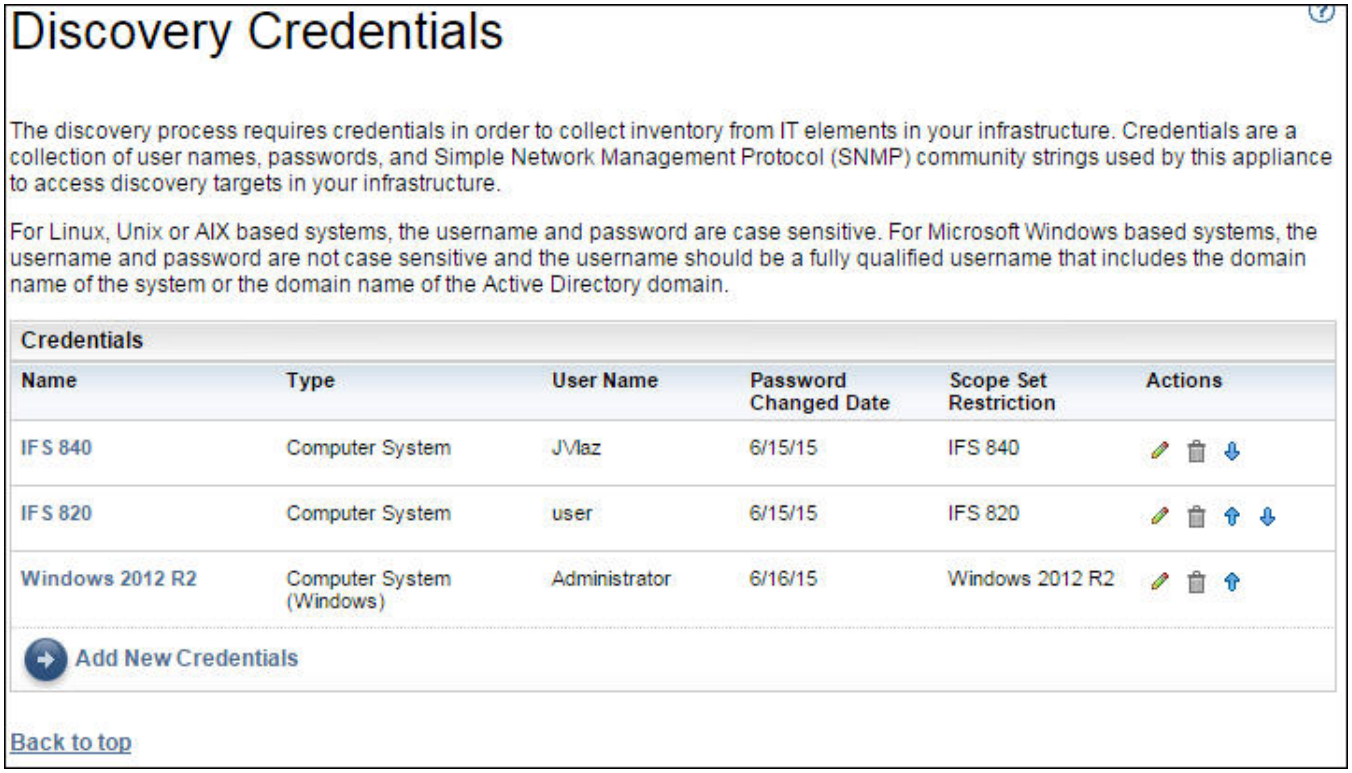

Figura 57. Novas credenciais de descoberta

Visualizando detalhes da credencial

É possível visualizar informações detalhadas sobre uma credencial de descoberta específica.

Sobre Esta Tarefa

Para visualizar os detalhes da credencial, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Credenciais de descoberta**.
   A página **Credenciais de descoberta** é exibida com todas as credenciais existentes listadas.
2. Para visualizar detalhes de uma credencial específica, clique no nome da credencial.
   A página **Credenciais de descoberta** é exibida com informações para a credencial selecionada.

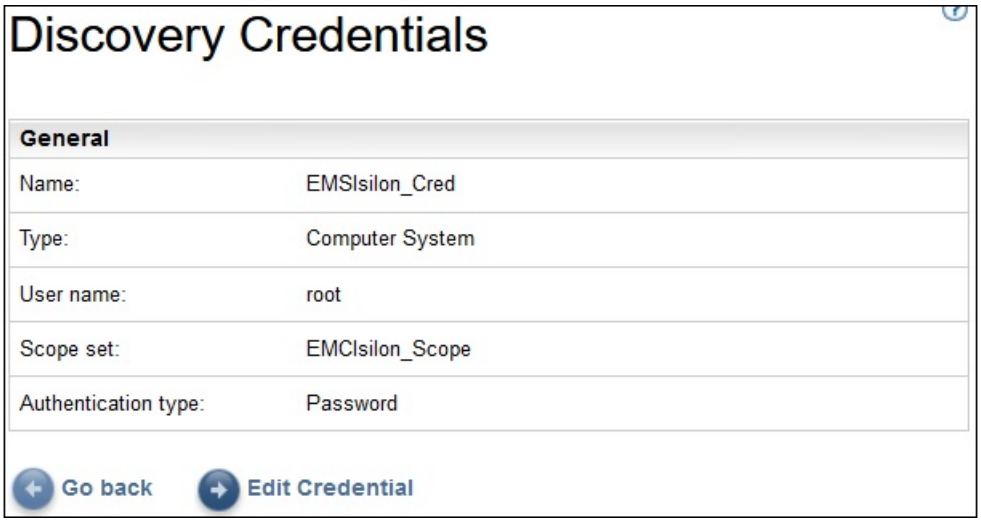

Figura 58. Detalhes das credenciais de descoberta

Tarefas relacionadas

Modificando credenciais

É possível modificar credenciais existentes para fornecer controle de acesso para o processo de descoberta.

Incluindo credenciais

Inclua credenciais para fornecer controle de acesso para o processo de descoberta.

Sobre Esta Tarefa

Para incluir credenciais, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Credenciais de descoberta**.
   A página **Credenciais de descoberta** é exibida.
2. Para criar uma credencial, clique em **Incluir novas credenciais**.
   A página **Novas credenciais de descoberta** é exibida.

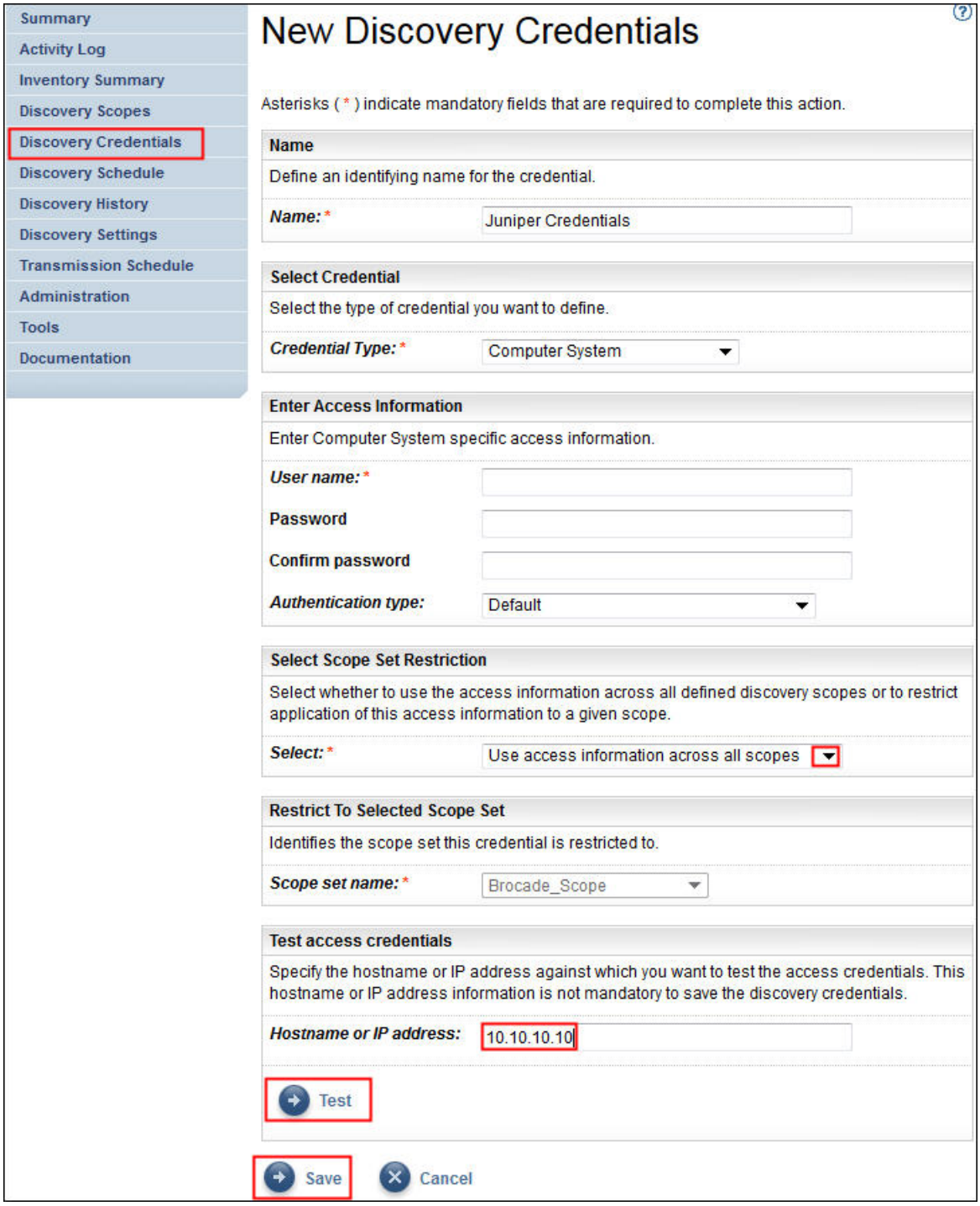

Figura 59. Novas credenciais de descoberta

a) No campo **Nome**, digite um nome de identificação para a credencial.

b) Na lista suspensa **Tipo de credencial**, selecione o tipo de credencial que você deseja criar.

c) Na área de janela **Inserir informações de acesso**, especifique as informações para o tipo de credencial que você selecionou:

   As informações necessárias dependem do tipo de credencial. Para obter as informações de acesso necessárias para cada tipo de credencial, consulte “Credencial e requisitos de software para o ambiente de descoberta ” na página 6.

   Importante: As informações de acesso especificadas devem corresponder às informações de acesso do recurso de destino da descoberta. Se você mudar as informações de acesso sobre o

recurso de destino, mude também as informações de acesso do TSA associadas. Para obter mais informações, consulte o IBM Technical Support Appliance Configuration Assistant Guide.

Dica: A página **Credenciais de descoberta** exibe a última vez que a senha foi mudada. Se você mudar regularmente a senha no recurso de destino, será possível usar essas informações para também garantir a mudança da senha no TSA para corresponder à nova senha do recurso de destino. Para obter informações sobre como exibir as credenciais de descoberta, consulte "Exibindo credenciais" na página 76.

d) A área de janela **Selecionar restrição de conjunto de escopos** é usada para especificar se uma credencial é limitada a um único conjunto de escopos ou é aplicada a todos eles. Se **Tipo de credencial** for **Sistema de computador** e **Tipo de autenticação** for **PKI**, essa área de janela não será exibida. As credenciais de PKI devem sempre ter o escopo definido para um único conjunto de escopos.

Dica: Criar credenciais de descoberta restritas a um conjunto de escopos específico pode melhorar o desempenho, reduzindo o número de credenciais que são tentadas para os recursos que estão sendo descobertos.

e) A área de janela **Restringir ao conjunto de escopos selecionado** é usada para limitar uma credencial a um único conjunto de escopos. Essa área de janela é visível em uma destas duas condições.

- A opção **Limitar informações de acesso ao escopo especificado** foi selecionada na área de janela **Selecionar restrição de conjunto de escopo** ou
- **Tipo de credencial** é **Sistema de computador** e **Tipo de autenticação** é **PKI**.

A credencial é usada apenas para descobrir o conjunto de escopos selecionado. Ao descobrir com um conjunto de escopos diferente, a credencial não será usada. Esse método evita tentativas inválidas de login que podem fazer com que sua conta seja bloqueada.

f) Se o seu tipo de credencial for **Sistema de computador**, **Sistema de computador (Windows)**, **SNMP** ou **SNMPV3**, será possível verificar se as credenciais estão corretas. A função **Testar** do tipo de credencial de **Sistema de computador** dá suporte aos seguintes dispositivos:

- Dispositivos que usam autenticação baseada em SSH ou Telnet
- XIV
- DS6000 & DS8000
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON / VNX / VMAX via EMC SMI-S
- IBM TS3100 / TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4300
- IBM TS4500
- IBM TS7700
- IBM DS3000, DS4000 e DS5000 se a senha for protegida
- Windows
- Palo Alto Networks (PAN-OS)

Para testar as credenciais, digite um endereço IP ou um nome de host para o dispositivo de destino no qual você deseja testar as credenciais e clique em **Testar**.

Nota:

- O nome do host digitado não deve conter sublinhado ("_").

- Para executar ou testar a credencial em sistemas que executam os sistemas operacionais Linux, AIX, IBM i ou HP-UX, ative o SSH.

g) Clique em **Salvar**.

A nova credencial é exibida na página **Credenciais de descoberta**.

Nota: É uma prática recomendada fazer backup da configuração do TSA ao criar ou modificar a credenciais de descoberta.

3. Para mudar a ordem na qual uma credencial é usada pelo TSA para acessar um recurso, clique no ícone **Seta para cima** ou no ícone **Seta para baixo** ao lado da credencial para movê-la para cima ou para baixo na lista.

Para obter informações sobre como a ordem é usada, consulte “Credenciais de descoberta” na página 2.

A lista da página **Credenciais de descoberta** é exibida novamente com a nova ordem.

Modificando credenciais

É possível modificar credenciais existentes para fornecer controle de acesso para o processo de descoberta.

Sobre Esta Tarefa

Para modificar as credenciais, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Credenciais de descoberta**.

A página **Credenciais de descoberta** é exibida com todas as credenciais existentes listadas.

2. Edite a credencial clicando no ícone **Editar** ( ) ao lado da credencial.

A página **Editar credenciais de descoberta** é exibida.

a) Na área de janela **Modificar informações de acesso**, é possível mudar as informações de acesso para essa credencial.

Importante: As informações de acesso especificadas devem corresponder às informações de acesso do recurso de destino da descoberta. Se você mudar as informações de acesso sobre o recurso de destino, mude também as informações de acesso do TSA associadas. Para obter mais informações, consulte o IBM Technical Support Appliance Configuration Assistant Guide.

Dica: A página **Credenciais de descoberta** exibe a última vez que a senha foi mudada. Se você mudar regularmente a senha no recurso de destino, será possível usar essas informações para também garantir a mudança da senha no TSA para corresponder à nova senha do recurso de destino. Para obter informações sobre como exibir as credenciais de descoberta, consulte “Exibindo credenciais” na página 76.

b) A área de janela **Selecionar restrição de conjunto de escopos** é usada para especificar se uma credencial é limitada a um único conjunto de escopos ou é aplicada a todos eles. Se **Tipo de credencial** for **Sistema de computador** e **Tipo de autenticação** for **PKI**, ela não será exibida. As credenciais de PKI devem sempre ter o escopo definido para um único conjunto de escopos.

Dica: Criar credenciais de descoberta restritas a um conjunto de escopos específico pode melhorar o desempenho, reduzindo o número de credenciais que são tentadas para os recursos que estão sendo descobertos.

c) A área de janela **Restringir ao conjunto de escopos selecionado** é usada para limitar uma credencial a um único conjunto de escopos. Essa área de janela é visível sob uma destas duas condições:

- A opção **Limitar informações de acesso ao escopo especificado** foi selecionada na área de janela **Selecionar restrição de conjunto de escopo** ou

- **Tipo de credencial** é **Sistema de computador** e **Tipo de autenticação** é **PKI**.

  A credencial é usada somente ao descobrir o conjunto de escopos selecionado. Essa credencial não é usada com nenhum outro conjunto de escopos. Esse método evita tentativas inválidas de login que podem fazer com que sua conta seja bloqueada.

d) Se o seu tipo de credencial for **Sistema de computador**, **Sistema de computador (Windows)**, **SNMP** ou **SNMPV3**, será possível verificar se as credenciais estão corretas. Para testar essas credenciais, insira um endereço IP ou nome de host para o destino com o qual você deseja testar as credenciais e clique em **Testar**.

   Nota: O nome do host digitado não deve conter sublinhado ("_").

e) Clique em **Salvar**.

   A credencial mudada é exibida na página **Credenciais de descoberta**.

3. Para mudar a ordem de prioridade na qual uma credencial é usada pelo TSA para acessar um recurso, clique no ícone **Seta para cima** ( ) ou no ícone **Seta para baixo** ( ) ao lado da credencial para movê-la para cima ou para baixo na lista.

   Para obter informações sobre como a ordem é usada, consulte “Credenciais de descoberta” na página 2.

   A lista da página **Credenciais de descoberta** é exibida novamente com a nova ordem.

Conceitos relacionados

Credenciais de descoberta

As credenciais de descoberta são uma coleção de nomes de usuário, senhas ou chaves SSH e sequências de comunidades de Protocolo Simples de Gerenciamento de Rede (SNMP) que o TSA usa para acessar recursos durante a descoberta.

Credencial e requisitos de software para o ambiente de descoberta

Para descobrir terminais ou recursos de descoberta em seu ambiente, o TSA deve ter acesso a esses recursos. É recomendado criar uma conta de serviço em cada recurso especificamente para o TSA usar ao acessar esse recurso.

Excluindo credenciais

É possível excluir credenciais que o TSA usa ao acessar seus recursos.

Sobre Esta Tarefa

Para excluir uma credencial, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Credenciais de descoberta**.

   A página **Credenciais de descoberta** é exibida.

2. Clique no ícone **Excluir** ( ) ao lado da credencial que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir a credencial.

Planejamento de descoberta

As descobertas estão planejadas para garantir que os dados descobertos sejam sempre atuais e precisos. É possível visualizar o planejamento de descoberta e os detalhes das últimas descobertas, modificar os planejamentos de descoberta e desativar as descobertas planejadas. Também é possível executar uma descoberta sempre que desejar.

Antes de Iniciar

Por padrão, o TSA usa o planejamento de Descoberta Completa para descobrir todos os elementos de TI definidos nos escopos dinâmicos do VMware e do HMC, bem como nos escopos de descoberta geral. O

TSA distribui automaticamente a detecção de elementos de TI durante o processo de descoberta para minimizar o impacto.

Uma alternativa é criar diversos planejamentos definidos pelo usuário. Isso permite que a descoberta de escopos de descoberta específicos seja distribuída para diferentes datas e horas durante as quais o impacto em sua rede e nos elementos de TI seja mínimo (ou ideal). Neste caso, o planejamento de descoberta completa deve ser desativado em favor dos planejamentos definidos pelo usuário.

No início de qualquer descoberta planejada, o dispositivo executa a tarefa de manutenção de pré-descoberta, durante a qual algumas funções, como Resumo do inventário, Escopos de descoberta, Planejamentos de descoberta e Credenciais, não estão disponíveis. Durante a tarefa de manutenção de pré-descoberta, o status do **Discovery Manager** na tela **Resumo** é definido como o símbolo de aviso ( ). Além disso, uma mensagem de aviso é exibida nas telas do TSA indicando que algumas funções estão temporariamente indisponíveis: `As part of Pre-Discovery Maintenance, the Discovery Manager is temporarily offline. Some UI functions related to discovery or inventory could display partial or no information during this time (typically up to 10 minutes).`

Após a manutenção de pré-descoberta ser concluída com sucesso, o status do **Discovery Manager** passa para o estado *OK*( ) na página **Resumo** e retoma a atividade de descoberta completa (em 10 minutos).

Visualizando o planejamento de descoberta

É possível visualizar as informações resumidas sobre um planejamento de descoberta.

Sobre Esta Tarefa

Para visualizar o planejamento de descoberta, siga estas etapas:

Procedimento

Na área de janela de navegação, clique em **Planejamento de descoberta**.

A página **Planejamento de descoberta** é exibida.

A área de janela **Planejamento** exibe o nome do planejamento, a próxima execução planejada, o planejamento da execução e as ações (Editar ( ), Excluir ( ), Ativar/Desativar (/), Executar) para cada planejamento.

Clique no ícone **Expandir** ( ) para visualizar todos os conjuntos de escopos que são designados para o planejamento. Para o planejamento de descoberta completa, o ícone lista todos os conjuntos de escopos definidos no TSA e designados ao planejamento por padrão.

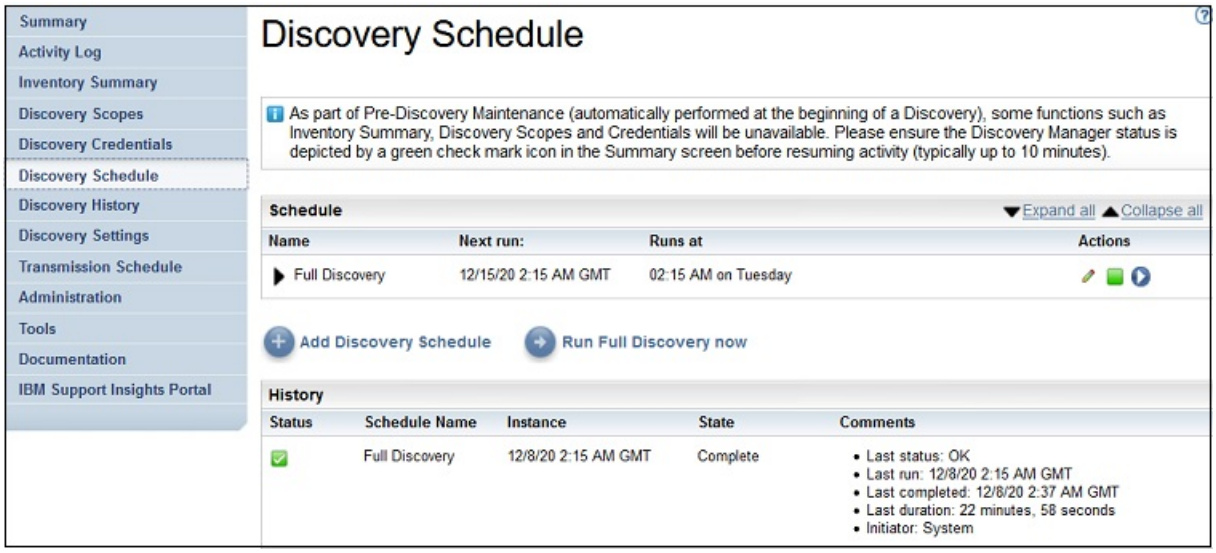

Figura 60. Programação de descoberta

Nota: Se uma nova instalação, migração ou upgrade do TSA existir para a versão mais recente, o novo TSA terá um planejamento de descoberta chamado **Descoberta Completa** criado com a data padrão (2h15 da terça-feira). Esse planejamento pode ser editado ou desativado, mas não pode ser excluído. Se você tiver planejamentos de descoberta predefinidos (ativados/desativados), os mesmos valores serão restaurados após a migração.

A área de janela **Histórico** exibe o status, o nome do planejamento e mais detalhes das tarefas em execução atualmente e das tarefas descobertas anteriormente.

Incluindo o planejamento de descoberta

É possível incluir novos planejamentos para que o processo de descoberta seja executado em um horário especificado. Os novos planejamentos permitem que o TSA descubra um subconjunto de seus elementos de TI na data e na hora planejadas.

Procedimento

1. Na área de janela de navegação, clique em **Planejamento de descoberta**.
   A página **Planejamento de descoberta** é exibida.
2. Clique em **Incluir planejamento de descoberta**. A página **Incluir planejamento de descoberta** é exibida.

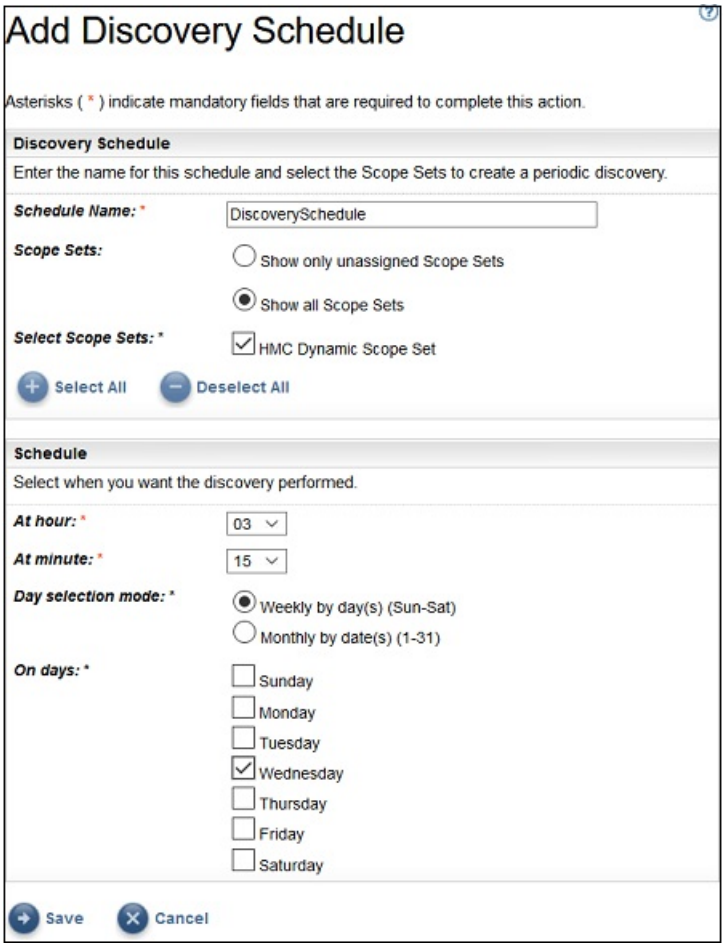

Figura 61. Incluir a programação de descoberta

3. No campo **Nome do planejamento**, digite um nome de identificação para o planejamento.
4. **Conjunto de escopos**
   a) Selecione a opção **Mostrar somente conjuntos de escopos não designados** para visualizar somente conjuntos de escopos não designados a nenhum outro planejamento de descoberta definido pelo usuário.
   b) Selecione a opção **Mostrar todos os conjuntos de escopos** para visualizar todos os conjuntos de escopos.
5. Selecione os conjuntos de escopos desejados na lista **Selecionar conjuntos de escopos**.
   É possível usar **Selecionar todos** / **Cancelar a seleção de todos** para selecionar todos ou nenhum dos conjuntos de escopos.
6. Use as listas **Na hora** e **No minuto** para selecionar um novo horário.
7. Selecione o **Modo de seleção de dia**.

   Semanalmente por dia(s) (de domingo a sábado)
   Para planejar a descoberta em um determinado dia da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)**.

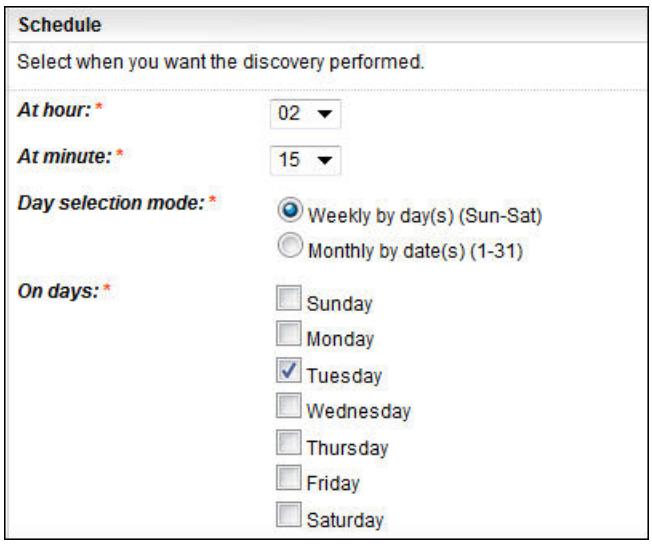

Figura 62. Semanalmente por dia(s) (de domingo a sábado)

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias da semana.

Mensalmente por data(s) (de 1 a 31)
Para planejar a descoberta em determinados dias de um mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias do mês.

Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.

8. Clique em **Salvar**.
   A página **Planejamento de descoberta** é exibida novamente com o novo planejamento exibido.

Modificando o planejamento de descoberta

O TSA fornece um planejamento padrão para o processo de descoberta ser executado em horários especificados. É possível modificar o planejamento padrão ou usar planejamentos customizados de acordo com suas necessidades.

Procedimento

1. Na área de janela de navegação, clique em **Planejamento de descoberta**.
   A página **Planejamento de descoberta** é exibida.
2. Clique no ícone **Editar planejamento** ( ).
   A página **Editar planejamento de descoberta** é exibida.
   a) Edite **Nome de Planejamento**, **Conjuntos de escopos** e **Selecionar conjuntos de escopos** conforme necessário na área de janela **Planejamento de descoberta**.

      Nota: Não é possível editar esses campos para a descoberta completa padrão.

   b) Edite **Na hora**, **No minuto**, **Modo de seleção de dia** e **Nos dias** conforme necessário na área de janela **Planejamento**.
3. Clique em **Salvar**.
   A página **Planejamento de descoberta** é exibida novamente com o planejamento modificado exibido.

Desativando o planejamento de descoberta

É possível desativar descobertas planejadas.

Antes de Iniciar

Nota: Quando planejamentos de descoberta definidos pelo usuário estão configurados, recomenda-se que o planejamento de **Descoberta Completa** seja desativado para que não ocorram descobertas duplicadas dos mesmos elementos de TI.

Procedimento

Para desativar descobertas planejadas, siga estas etapas:

1. Na área de janela de navegação, clique em **Planejamento de descoberta**.

   A página **Planejamento de descoberta** é exibida.

2. Clique no ícone **Ativar/desativar** (/) para o respectivo planejamento para desativar/ativar o planejamento de descoberta.

Excluindo o planejamento de descoberta

É possível excluir descobertas planejadas.

Procedimento

Para excluir descobertas planejadas, siga estas etapas:

1. Na área de janela de navegação, clique em **Planejamento de descoberta**.

   A página **Planejamento de descoberta** é exibida.

2. Clique no ícone Excluir ( ) para o respectivo planejamento a ser excluído.

   Nota: Não é possível excluir o planejamento **Descoberta completa**, mas é possível desativar esse planejamento, se desejado.

   Uma mensagem de confirmação é exibida para excluir o planejamento de descoberta selecionado.

3. Clique em **OK** para excluir o planejamento.

Executando a descoberta

É possível executar uma descoberta sob demanda em vez de aguardar a próxima descoberta planejada. É possível executar uma descoberta em todos os escopos de descoberta definidos, um planejamento de descoberta específico ou em escopos ou conjuntos de escopos de descoberta específicos".

Procedimento

Para executar uma descoberta em todos os escopos definidos, siga estas etapas:

1. Na área de janela de navegação, clique em **Planejamento de descoberta**. A página **Planejamento de descoberta** é exibida.
2. Clique em **Executar a descoberta completa agora**. A seção Histórico é atualizada indicando que a descoberta está em execução.

   Nota: O TSA tenta minimizar os impactos no ambiente de rede. Como resultado, o processo de descoberta usa uma abordagem iterativa e medida que pode fazer com que uma descoberta completa demore até 72 horas. É possível monitorar o processo de descoberta na seção **Resumo da tarefa** na página **Resumo**.

3. Para executar uma descoberta em um escopo específico, clique no ícone **Executar** ( ) desse escopo.
4. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta nos conjuntos de escopos gerais

Procedimento

Para executar uma descoberta em um conjunto de escopos específico, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**.
   A página **Escopos gerais de descoberta** é exibida. Essa página exibe uma lista de todos os conjuntos de escopos definidos para este TSA.

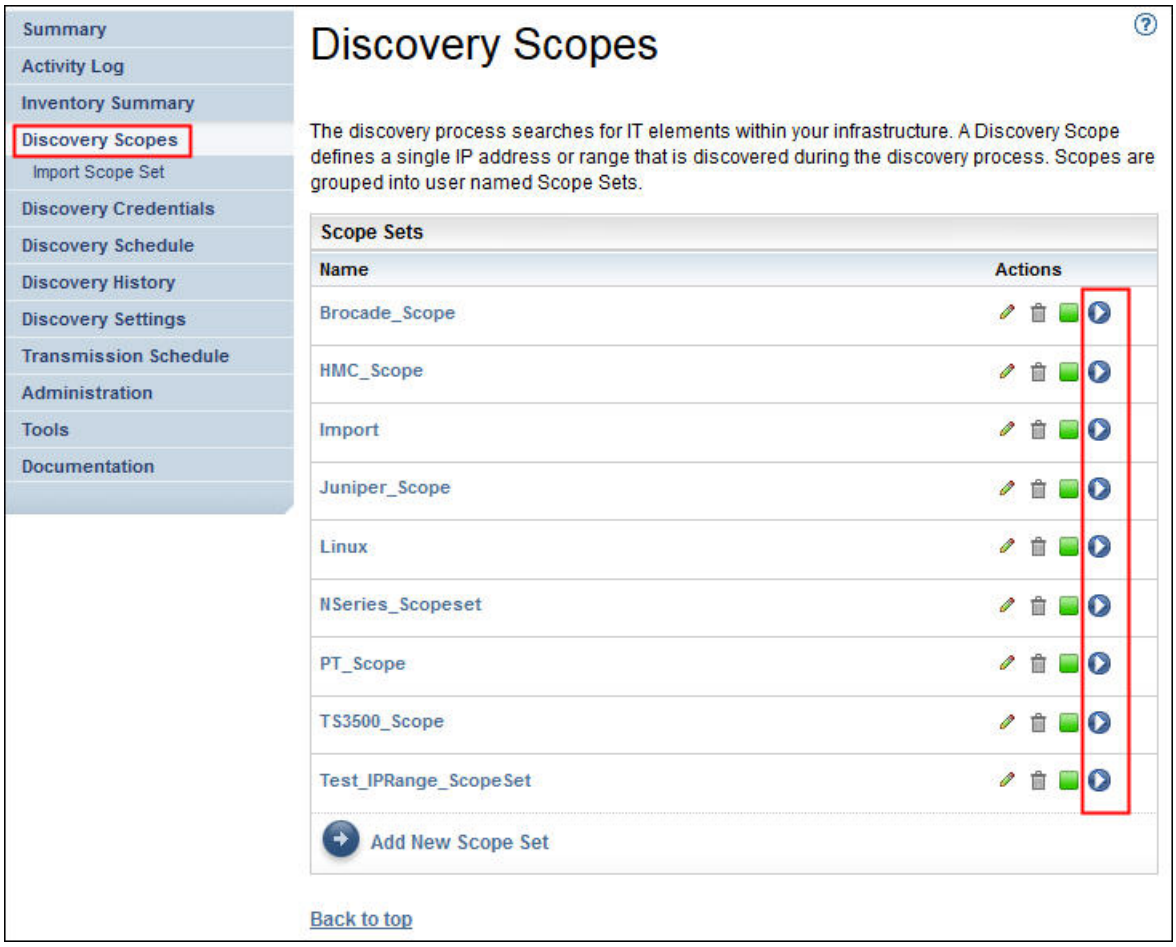

Figura 63. Executar a descoberta em escopos específicos

2. Para executar uma descoberta em um conjunto de escopos específico, clique no ícone **Executar** ( ) para esse conjunto de escopos.
3. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta nos conjuntos de escopo dinâmicos do HMC

Procedimento

Para executar uma descoberta em um conjunto de escopos específico, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**.
   A página **Escopos dinâmicos de HMC** é exibida. Essa página exibe uma lista de todos os conjuntos de escopos definidos para este TSA.

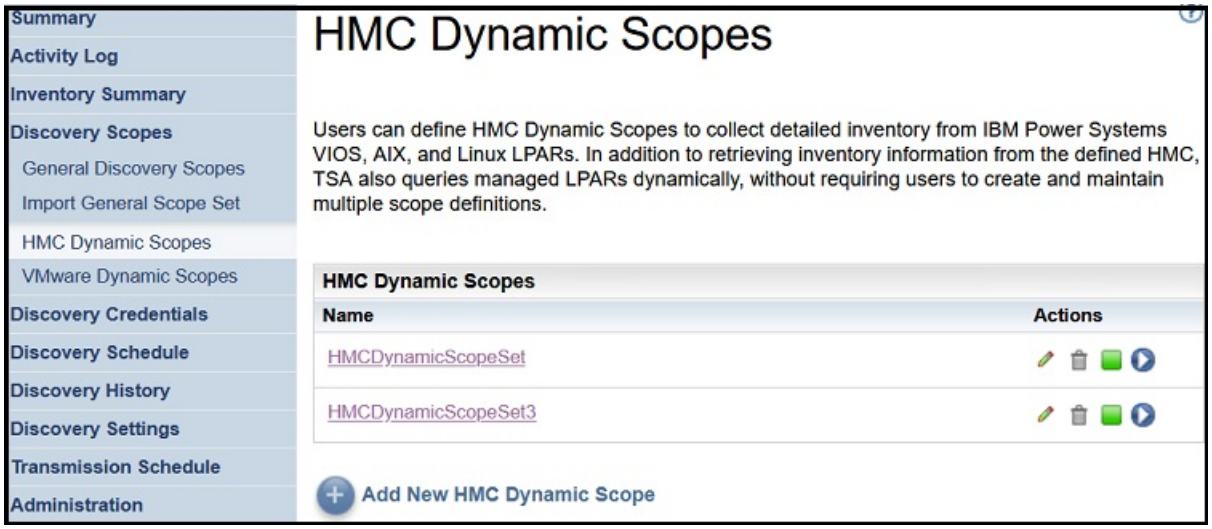

Figura 64. Escopos dinâmicos de HMC

2. Para executar uma descoberta em um conjunto de escopos específico, clique no ícone **Executar** ( ) para esse conjunto de escopos.
3. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta em conjuntos de escopo do VMWare

Procedimento

Para executar uma descoberta em um conjunto de escopos específico, siga estas etapas:

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Conjunto de escopos dinâmicos do VMWare**.

   A página **Escopos dinâmicos do VMWare** é exibida. Essa página exibe uma lista de todos os conjuntos de escopos definidos para este TSA.

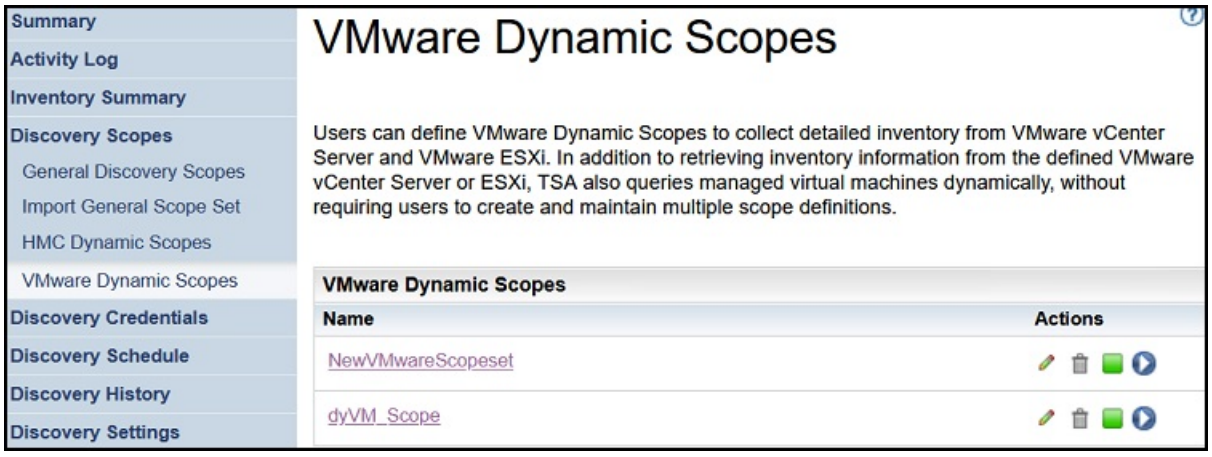

Figura 65. Executar a descoberta em escopos dinâmicos do VMware

2. Para executar uma descoberta em um conjunto de escopos específico, clique em **Executar** ( ) para esse conjunto de escopos.
3. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para

mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta em escopos

É possível executar uma descoberta sob demanda em vez de aguardar a próxima descoberta planejada. É possível executar uma descoberta em todos os escopos de descoberta definidos, um planejamento de descoberta específico ou em escopos ou conjuntos de escopos de descoberta específicos".

Executando a descoberta em escopos gerais

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos gerais de descoberta**. A página **Escopos gerais de descoberta** é exibida.

Figura 66. Escopos de descoberta

2. Clique no conjunto de escopos que contém o escopo a ser descoberto.

   A página **Conjunto de escopos de descoberta** é exibida. Essa página exibe todos os escopos definidos para esse conjunto de escopos.

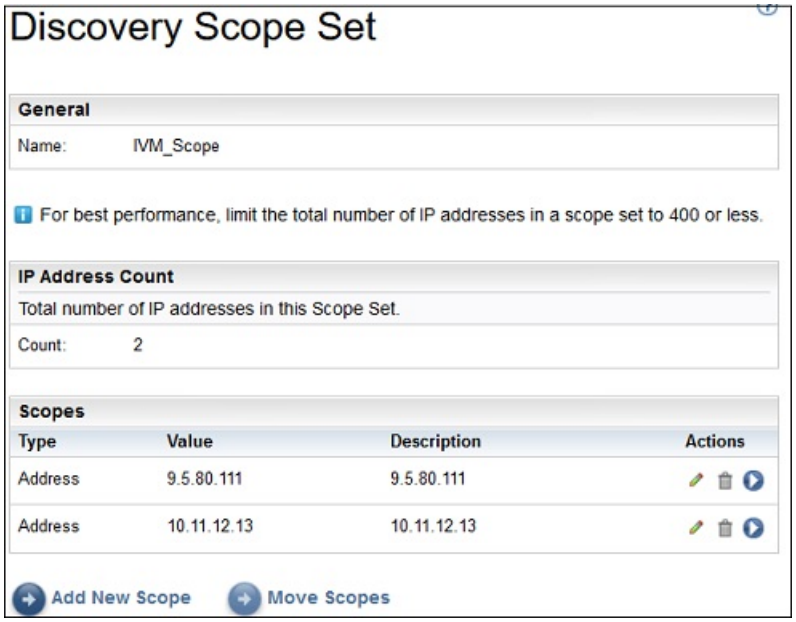

Figura 67. Executar a descoberta em escopos específicos

3. Para executar uma descoberta em um escopo específico, clique no ícone **Executar** ( ) para esse escopo.
4. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta em escopos dinâmicos do HMC

Procedimento

1. Na área de janela de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos de HMC**. A página **Escopos dinâmicos de HMC** é exibida.

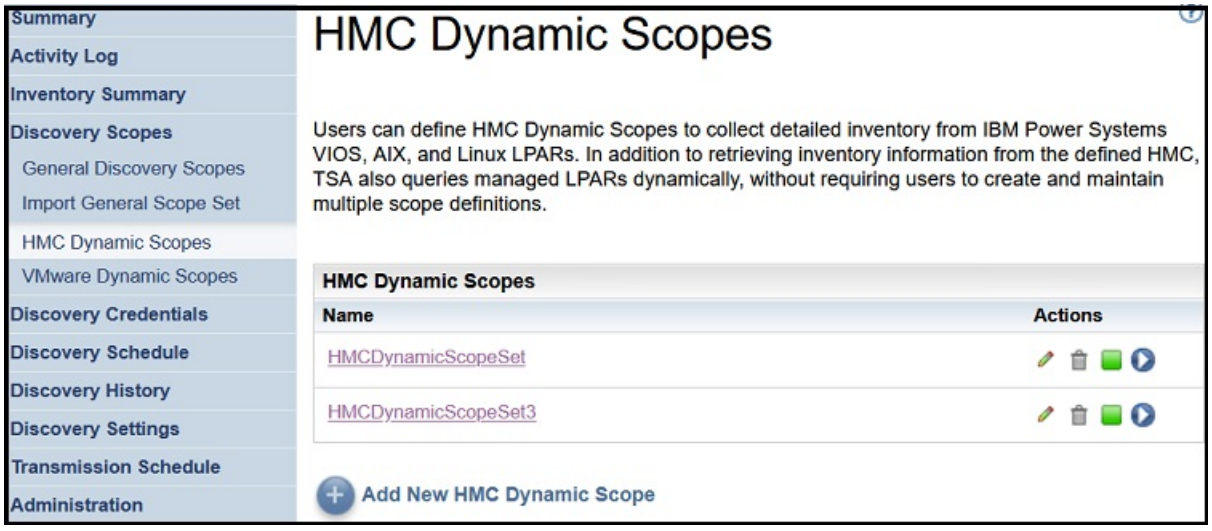

Figura 68. Escopos dinâmicos de HMC

2. Clique no conjunto de escopos que contém o escopo a ser descoberto.

   A página **Conjunto de escopos dinâmicos de HMC** é exibida. Essa página exibe todos os escopos definidos para esse conjunto de escopos.

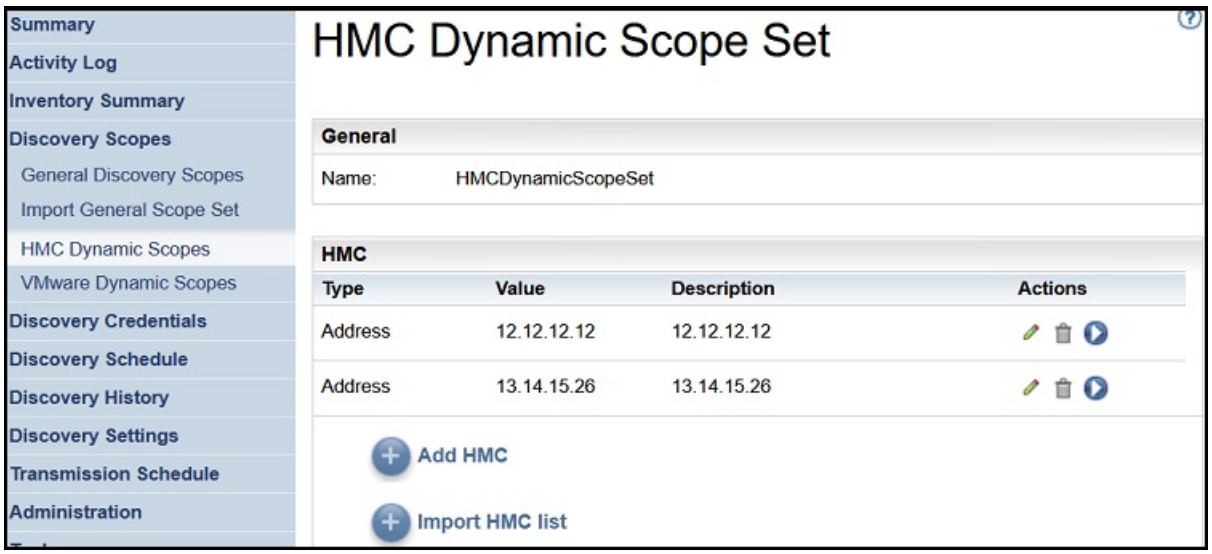

Figura 69. Executar a descoberta em escopos específicos

3. Para executar uma descoberta em um escopo específico, clique no ícone **Executar** ( ) desse escopo.
4. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Executando a descoberta em escopos dinâmicos do VMWare

Procedimento

1. No painel de navegação, clique em **Escopos de descoberta** > **Escopos dinâmicos do VMWare**. A página **Escopos dinâmicos do VMWare** é exibida.

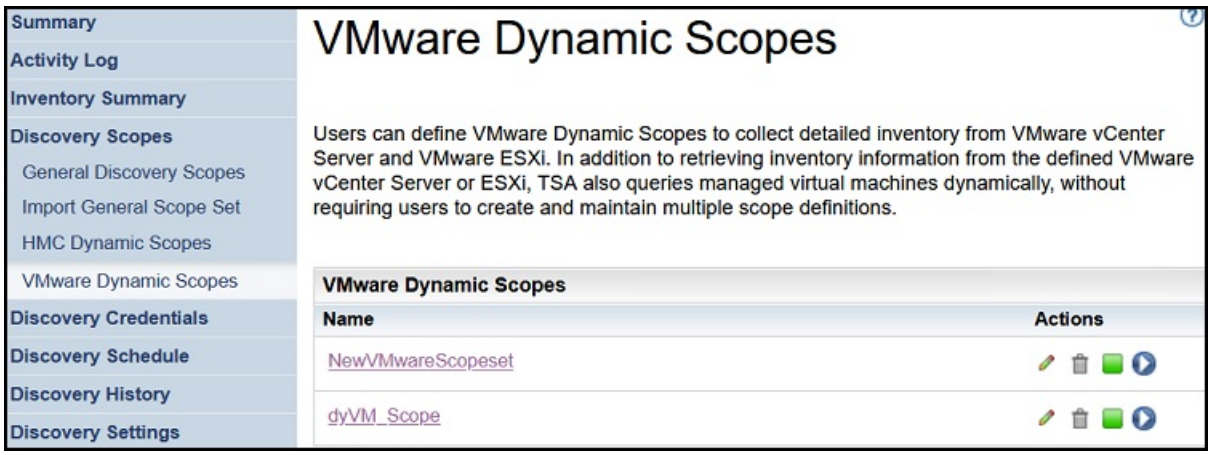

Figura 70. Escopos dinâmicos do VMWare

2. Clique no conjunto de escopos que contém o escopo a ser descoberto.

   A página **Conjunto de escopos dinâmicos do VMWare** é exibida. Essa página exibe todos os escopos definidos para esse conjunto de escopos.

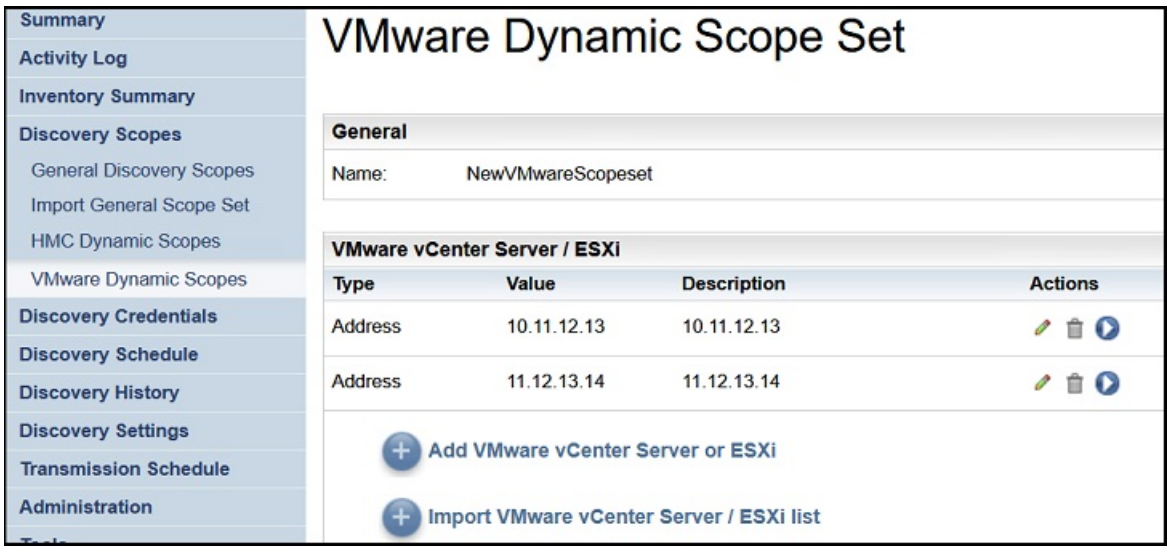

Figura 71. Executar a descoberta em escopos dinâmicos do VMware

3. Para executar uma descoberta em um escopo específico, clique no ícone **Executar** ( ) para esse escopo.
4. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A descoberta é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A descoberta deve ser concluída sem erros.

Histórico de descobertas

É possível visualizar os detalhes de uma descoberta após sua conclusão e fazer download de um arquivo de log de diagnóstico da descoberta.

Procedimento

Para visualizar o histórico de descoberta ou fazer o download de um arquivo de log de diagnóstico, siga estas etapas:

1. Na área de janela de navegação, clique em **Histórico de descoberta**.

   A página **Histórico de descoberta** é exibida. Uma lista de entradas de descobertas é exibida. Cada entrada exibe o status, o nome e os horários de início e término de uma descoberta.

   

   Figura 72. Histórico de descobertas
2. Para exibir mais informações sobre uma entrada na lista **Entradas do histórico**, clique no nome da entrada do histórico.

   A área de janela **Informações da entrada** exibe informações sobre a descoberta selecionada.
3. Para fazer download de um arquivo de diagnóstico para uma descoberta, clique no ícon **Download** ( ) para a descoberta.
4. Para excluir um arquivo de log de diagnóstico para uma descoberta, clique no ícone **Excluir** ( ) para a descoberta.

Planejamento de transmissão

A transmissão de dados está planejada para garantir que os dados descobertos sejam enviados regularmente para o Suporte IBM. É possível visualizar o planejamento de transmissão e os detalhes das

últimas transmissões, modificar o planejamento de transmissão e desativar as transmissões planejadas. Também é possível enviar os dados para a IBM sempre que você desejar.

Visualizando o planejamento de transmissão

É possível visualizar as informações resumidas sobre um planejamento de transmissão.

Sobre Esta Tarefa

Para visualizar o planejamento de transmissão, siga estas etapas:

Procedimento

Na área de janela de navegação, clique em **Planejamento de transmissão**.

A página **Planejamento de transmissão** é exibida.

O painel **Planejamento** exibe a próxima execução planejada e os tempos de execução planejados. A área de janela **Histórico** exibe o status e os detalhes adicionais das tarefas de transmissão em execução e anteriores.

Modificando o planejamento de transmissão

O TSA fornece um planejamento padrão para o processo de transmissão ser executado em horários especificados. É possível modificar esse planejamento de acordo com suas necessidades.

Procedimento

1. Na área de janela de navegação, clique em **Planejamento de transmissão**.

   A página **Planejamento de transmissão** é exibida.

   O painel **Planejamento** exibe a próxima execução planejada e os tempos de execução planejados. A área de janela **Histórico** exibe o status e os detalhes adicionais das tarefas de transmissão em execução e anteriores.
2. Clique em **Editar planejamento**.

   A página **Planejamento de transmissão** é exibida.

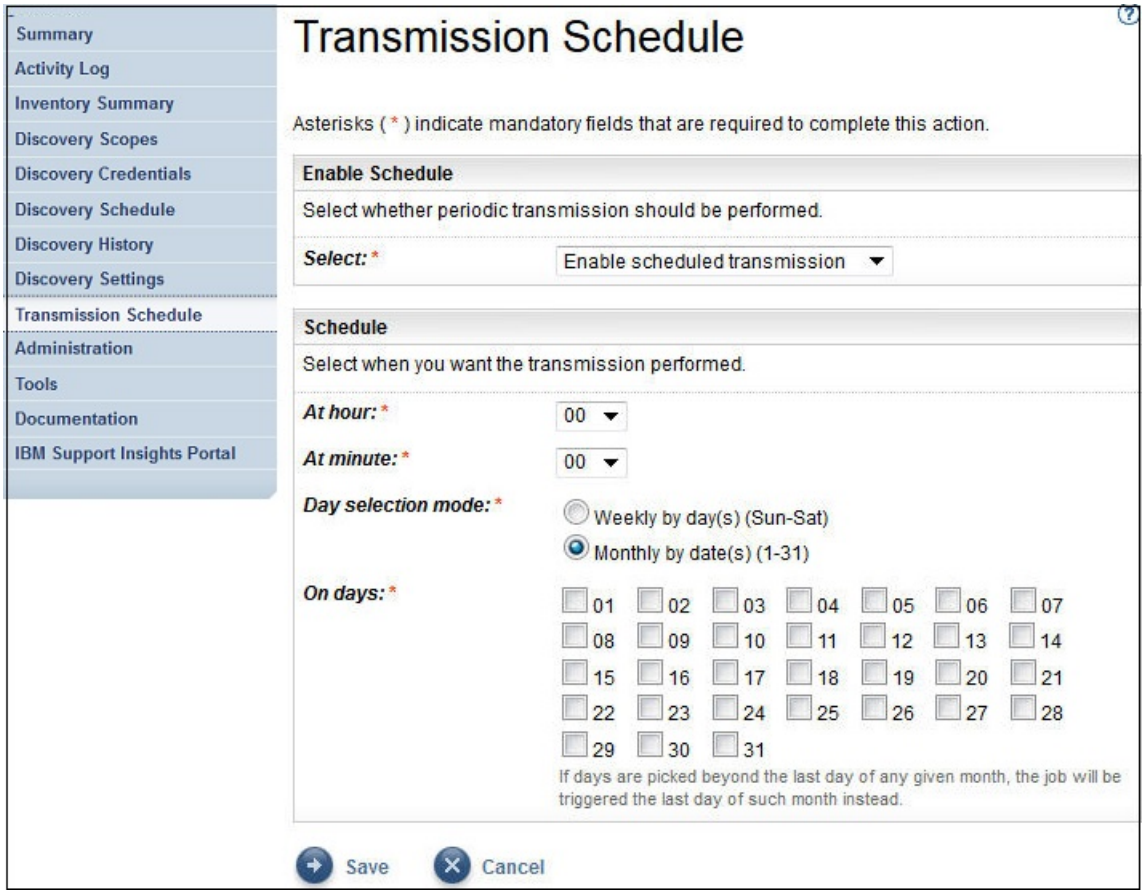

Figura 73. Editar planejamento de transmissão

a) Use as listas suspensas **Na hora** e **No minuto** para selecionar um novo horário.

b) Selecione o **Modo de seleção de dia**.

Semanalmente por dia(s) (de domingo a sábado)

Para planejar a transmissão em um determinado dia da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)**.

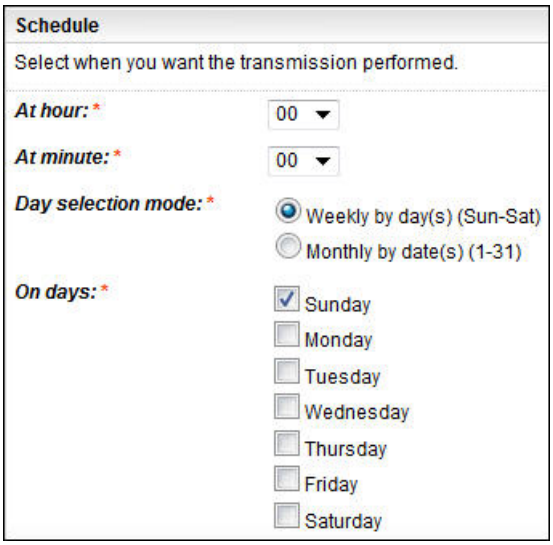

Figura 74. Semanalmente por dia(s) (de domingo a sábado)

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias da semana.

Mensalmente por data(s) (de 1 a 31)
Para planejar a transmissão em determinados dias de um mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias do mês.

Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.

3. Clique em **Salvar**.
   A página **Planejamento de transmissão** é exibida novamente com o novo planejamento exibido.

Desativando o planejamento de transmissão

É possível desativar transmissões de dados planejadas.

Procedimento

Para desativar transmissões de dados planejadas, siga estas etapas:

1. Na área de janela de navegação, clique em **Planejamento de transmissão**.
   A página **Planejamento de transmissão** é exibida.
2. Clique em **Editar planejamento**.
   A página **Planejamento de transmissão** é exibida.
3. Na área de janela **Ativar planejamento**, selecione **Desativar transmissão planejada**.
4. Clique em **Salvar**.
   A página **Planejamento de descoberta** é exibida e a área de janela **Planejamento** mostra que a descoberta planejada está desativada. É possível ativar transmissões planejadas clicando em **Ativar transmissão planejada**.

Executando a transmissão

É possível executar uma transmissão sob demanda, em vez de aguardar a próxima transmissão planejada.

Procedimento

1. Na área de janela de navegação, clique em **Planejamento de transmissão**.
   A página **Planejamento de transmissão** é exibida.

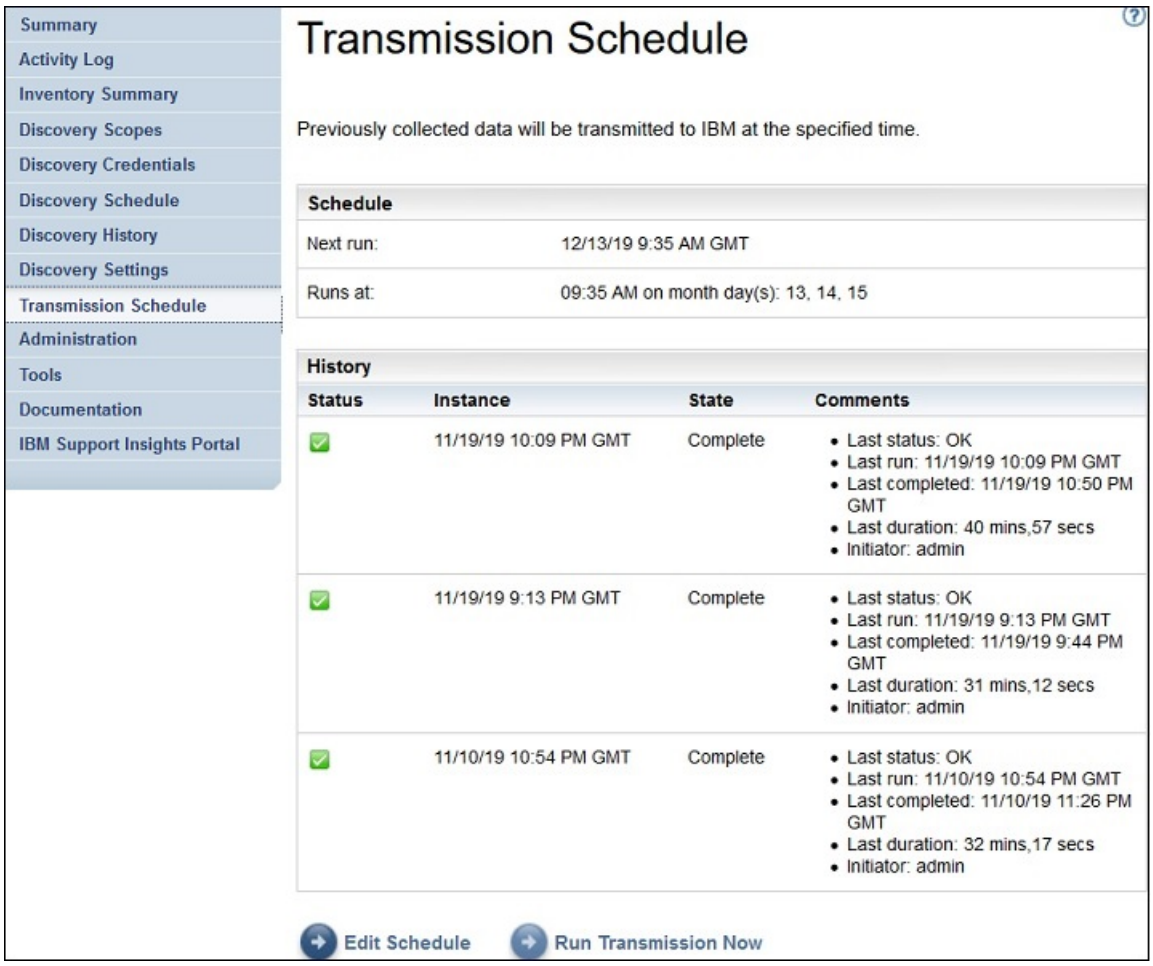

Figura 75. Executar transmissão agora

2. Clique em **Executar transmissão agora**.

   A área de janela **Histórico** é atualizada, indicando que a transmissão está em execução.

3. Verifique a página **Resumo** (clique em **Resumo** na área de janela de navegação). A transmissão é mostrada na área de janela **Resumo da tarefa**. A página **Resumo** é atualizada periodicamente para mostrar o estado atual do TSA. Quando a tarefa não estiver mais listada na área de janela **Resumo da tarefa**, verifique o **Log de atividades** (clique em **Log de atividade** na área de janela de navegação). A transmissão deve ser concluída sem erros.

Captura instantânea de dados

É possível gerar e salvar uma cópia local dos dados brutos não formatados que são coletados pelo TSA sem transmitir os dados para a IBM. Também é possível ver os últimos dados transmitidos à IBM.

1. Na área de janela de navegação, clique em **Administração** > **Captura instantânea de dados**. A página **Captura instantânea de dados** é exibida.

Figura 76. Captura instantânea de dados

Nota: O botão **Fazer download da última captura instantânea de dados** é ativado apenas quando existe uma transmissão concluída ou uma captura instantânea de dados.

2. Clique em **Gerar captura instantânea de dados agora** para coletar os dados mais recentes descobertos pelo TSA e gerar uma nova captura instantânea de dados. A seguinte mensagem é exibida - `Captura instantânea de dados em andamento. Isso pode levar até duas horas. Visualize o log de atividades ou a página Resumo para obter o status.` Clique em **Resumo** no menu de navegação para visualizar a página **Resumo**. A área de janela **Resumo da tarefa** mostra o status da coleção de captura instantânea de dados até que ela seja concluída. Clique em **Log de atividades** no menu de navegação para visualizar o status de conclusão da solicitação de captura instantânea de dados.
3. Se o serviço de transmissão ou de captura instantânea de dados for concluído, a **Data da captura instantânea de dados** será exibida.

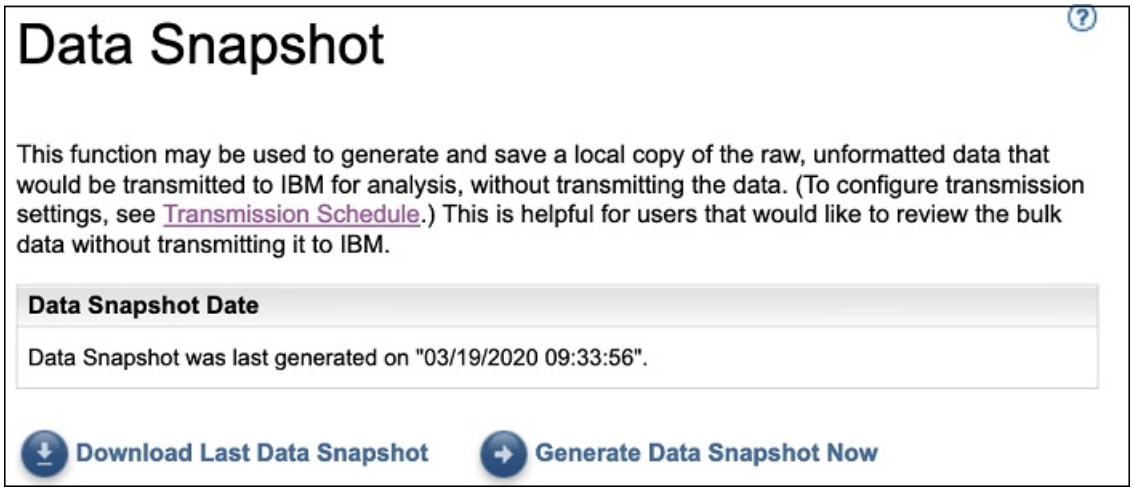

Figura 77. Data da captura instantânea de dados

4. Clique em **Fazer download da captura de tela de dados mais recente** para fazer download da captura instantânea de dados mais recente. Especifique um local para o arquivo resultante (*collection.tar.xz*). Dependendo da quantia de dados, a operação de download pode levar algum tempo. Para extrair o conteúdo do archive *.tar.xz*, use o utilitário *tar* (para o Linux) ou o utilitário *7-Zip* (disponível para Linux e Windows).

   Nota:

   - Se uma tarefa de transmissão ou coleta estiver em andamento, a seguinte mensagem será exibida - `Uma tarefa de coleta está em execução no momento. A captura instantânea de dados mais recente foi gerada em <<timestamp>>. Tem certeza de que deseja fazer download da coleção?`
     - Clique em **OK** para continuar com o download.
     - Clique em **Cancelar** para cancelar o download e aguarde a tarefa de coleta em execução no momento ser concluída.

- Se uma tarefa de transmissão ou coleta não estiver em andamento, a seguinte mensagem será exibida: `A captura instantânea de dados mais recente foi gerada em <<timestamp>>. Tem certeza de que deseja fazer download da coleção?` Clique em **OK** para continuar com o download.

Visualizando o resumo do inventário

Use a página **Resumo do inventário** para visualizar o resumo de elementos de TI, como sistemas de computador, sistemas operacionais e subsistemas de armazenamento, que são descobertos.

Clique em **Resumo do inventário** na área de janela de navegação para exibir a página **Resumo do inventário**.

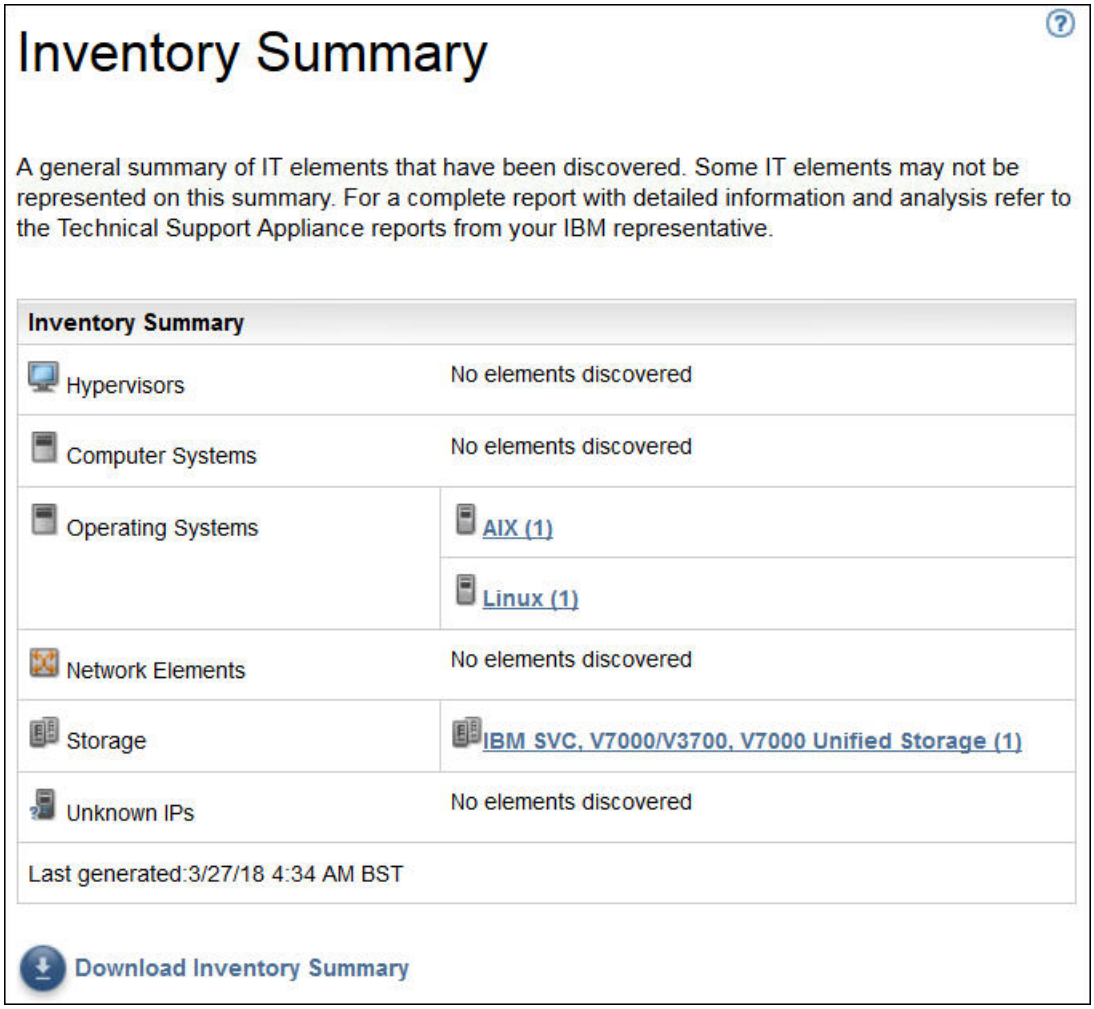

Figura 78. Resumo do inventário

A página Resumo do inventário mostra seis grupos diferentes de elementos de TI:

- **Hypervisores**: inclui hypervisores como o HMC, o IBM Flex System Manager, o VMware, o VIOS etc.
- **Sistemas de computador**: inclui sistemas físicos de computador.
- **Sistemas operacionais**: inclui os sistemas operacionais, como o AIX, o Linux etc., em execução em bare metal (servidores físicos dedicados) ou em um ambiente virtualizado.
- **Elementos de rede**: inclui comutadores e roteadores.
- **Armazenamento**: inclui subsistemas de armazenamento, como os dispositivos de armazenamento IBM XIV, IBM FlashSystem, EMC e HP. Além disso, inclui os dispositivos de fita.
- **IPs desconhecidos**: dispositivos que talvez não estejam classificados por motivos que incluem os seguintes:

- Há um firewall bloqueando o acesso ao dispositivo.
- Não há credenciais definidas para o dispositivo. Visualize a página **Status da autenticação** (**Ferramentas→ Status de autenticação**) para obter informações sobre os endereços IP e as credenciais associadas.
- Não existem sensores para o tipo de dispositivo.

• A linha **Última geração** indica a última vez em que a tarefa de resumo de inventário foi concluída.

Nota: Os dados nessa área de janela são exibidos logo depois que o TSA é iniciado. Se você visualizar a página nesse período, uma mensagem informativa será exibida: **`A geração do resumo do inventário está em andamento`**. Depois que as informações do resumo forem preenchidas inicialmente, elas serão atualizadas a cada 30 minutos aproximadamente. Para atualizar manualmente, clique no ícone **Atualizar** do navegador.

Cada grupo exibe a lista de tipos de dispositivo e a contagem de cada um deles.

1. Clique em um dos hyperlinks de dispositivo para visualizar a página **Detalhe do resumo do inventário**.

Figura 79. Detalhe do resumo do inventário

2. Selecione um dos dispositivos na lista para visualizar as **Informações do elemento**, como *Context IP address*, *Manufacturer*, *Model* e *Serial number*.

   Nota: Para dispositivos detectados pelo TSA para os quais nenhuma credencial válida foi definida, as **Informações do elemento** não são preenchidas. O TSA requer um login bem-sucedido no dispositivo para fornecer esses detalhes.

Clique em **Fazer download do resumo do inventário** para fazer download de um arquivo contendo um resumo dos dispositivos que foram descobertos.

Depuração de problemas de descoberta

Status da autenticação

Use a página **Status de autenticação** para visualizar um resumo dos elementos de TI definidos nos conjuntos de escopos que estão apresentando problemas com as credenciais.

Para visualizar o status de autenticação, clique em **Ferramentas** > **Status de autenticação** na área de janela de navegação. A página **Status de autenticação** é exibida.

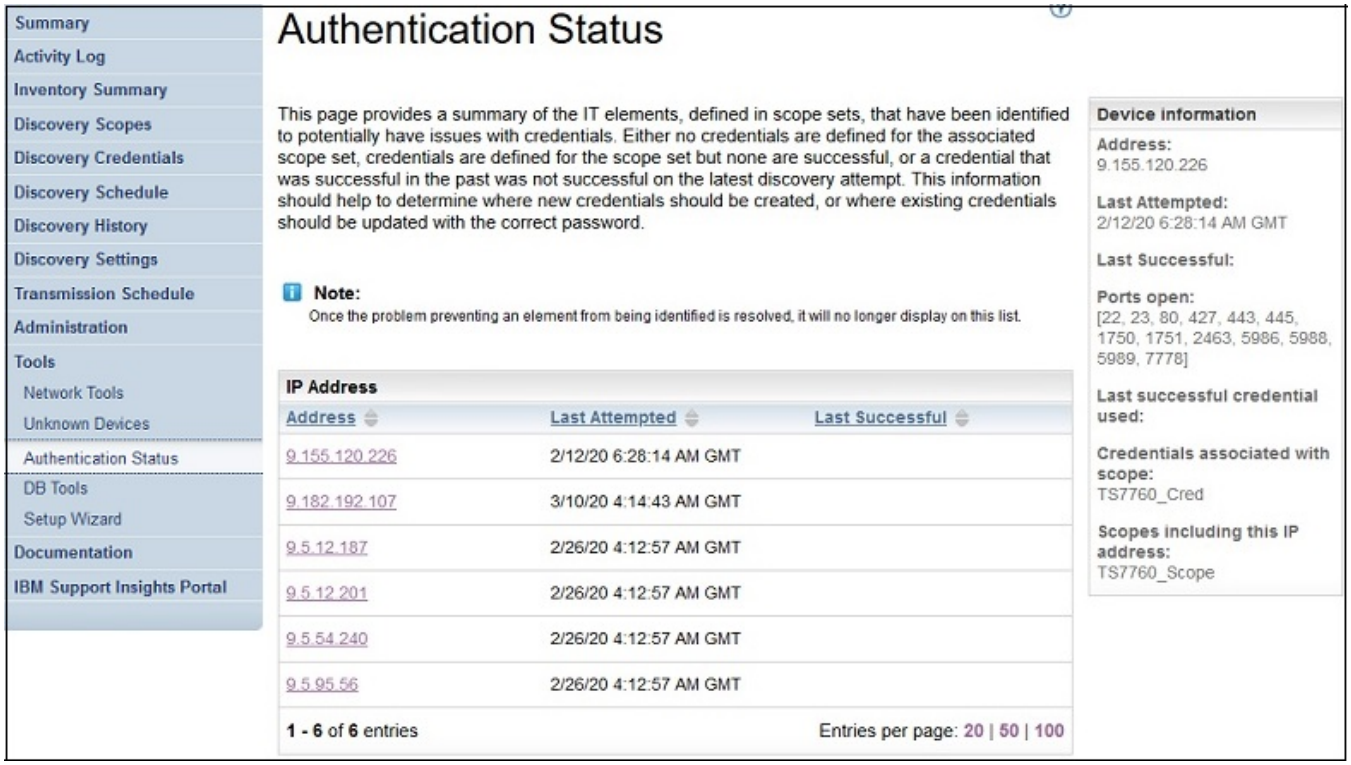

Figura 80. Status da autenticação

O status exibe todos os IPs de dispositivo que relataram problemas com credenciais. Os problemas podem ser causados pelos motivos a seguir:

- As credenciais não estão definidas para o conjunto de escopos associado.
- As credenciais estão definidas para o conjunto de escopos, mas não foram bem-sucedidas.
- As credenciais que foram bem-sucedidas anteriormente não foram bem-sucedidas na tentativa de descoberta mais recente.

Clique no link do respectivo endereço IP para visualizar as informações sobre o dispositivo, como *Última tentativa*, *Última bem-sucedida*, *Portas abertas*, *Últimas credenciais usadas com sucesso*, *Data da última mudança de credenciais*, *Credenciais associadas ao escopo* e *Escopos que incluem este endereço IP*. Essas informações serão úteis para determinar onde as novas credenciais devem ser criadas ou onde as credenciais existentes devem ser atualizadas com a senha correta.

Nota: Quando o problema com a credencial for resolvido, o respectivo IP do dispositivo não será mais exibido na lista.

Dispositivos desconhecidos

É possível exibir informações sobre dispositivos que o TSA descobriu, mas não é possível identificar completamente.

Para exibir esses dispositivos desconhecidos, clique em **Ferramentas** > **Dispositivos desconhecidos** na área de janela de navegação. A página **Dispositivos desconhecidos** é exibida.

É possível clicar em qualquer entrada da lista IPs desconhecidos para exibir informações adicionais sobre esse dispositivo.

Capítulo 6. Configurando tarefas administrativas

Informações do status

O TSA fornece informações resumidas, logs e relatórios para permitir que você encontre rapidamente informações sobre tarefas, inventário descoberto e produtos.

É possível exibir as informações resumidas de alto nível sobre tarefas, inventário e produtos clicando em **Resumo** na área de janela de navegação. A página **Resumo** atualiza frequentemente para mostrar as informações de resumo mais atualizadas. A página **Resumo** inclui as informações a seguir:

- **Status do sistema**

  A área de janela **Status do sistema** exibe o status dos serviços atuais e tarefas sendo executadas. É possível exibir as páginas dos serviços exibidos clicando no nome do serviço na área de janela **Status do sistema**.
- **Resumo da tarefa**

  A área de janela **Resumo de tarefas** exibe um resumo das tarefas atuais.
- **Resumo do inventário**

  A área de janela **Resumo de inventário** exibe uma lista de inventários descobertos.
- **Informações do produto**

  A área de janela **Informações do produto** exibe o nome do host e o ID do TSA.

Visualizando o log de atividades

O log de atividades exibe mensagens de log para os processos de descoberta e transmissão. É possível clicar nas entradas no log de atividades para visualizar mais informações.

É possível exibir o log de atividades clicando em **Log de atividades** na área de janela de navegação. Uma lista de entradas de log é exibida. Cada entrada exibe a mensagem, a severidade e a hora em que a atividade ocorreu.

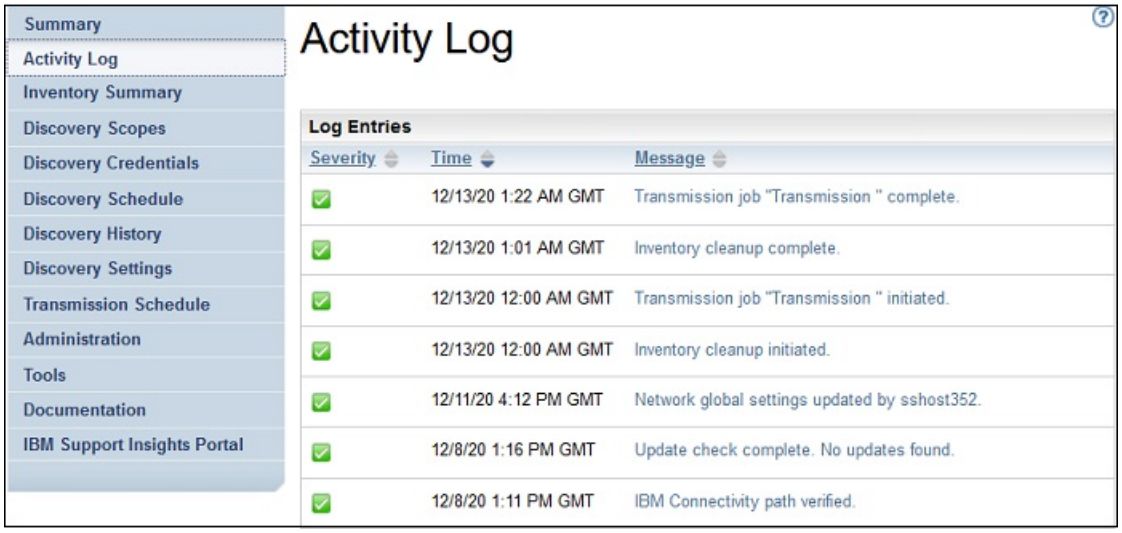

Figura 81. Log de atividades

Nota: Como as descobertas são executadas em conjuntos de escopos individuais, pode haver várias entradas de log para uma descoberta completa.

Para exibir mais detalhes sobre qualquer entrada de log de atividades, clique na mensagem para essa entrada.

Para salvar os arquivos de log em seu computador, clique em **Fazer download de todos os logs**.

Para limpar o log, clique em **Limpar log**.

Visualizando o archive de limpeza de inventário

É possível visualizar o inventário que é limpo de acordo com o prazo de inatividade que você especificou no **Planejamento de limpeza de inventário**

Sobre Esta Tarefa

Para visualizar o inventário excluído, siga estas etapas:

Procedimento

1. Na página **Planejamento de limpeza de inventário**, clique em **Mostrar archive de limpeza**. A página **Archive de limpeza de inventário** é exibida.

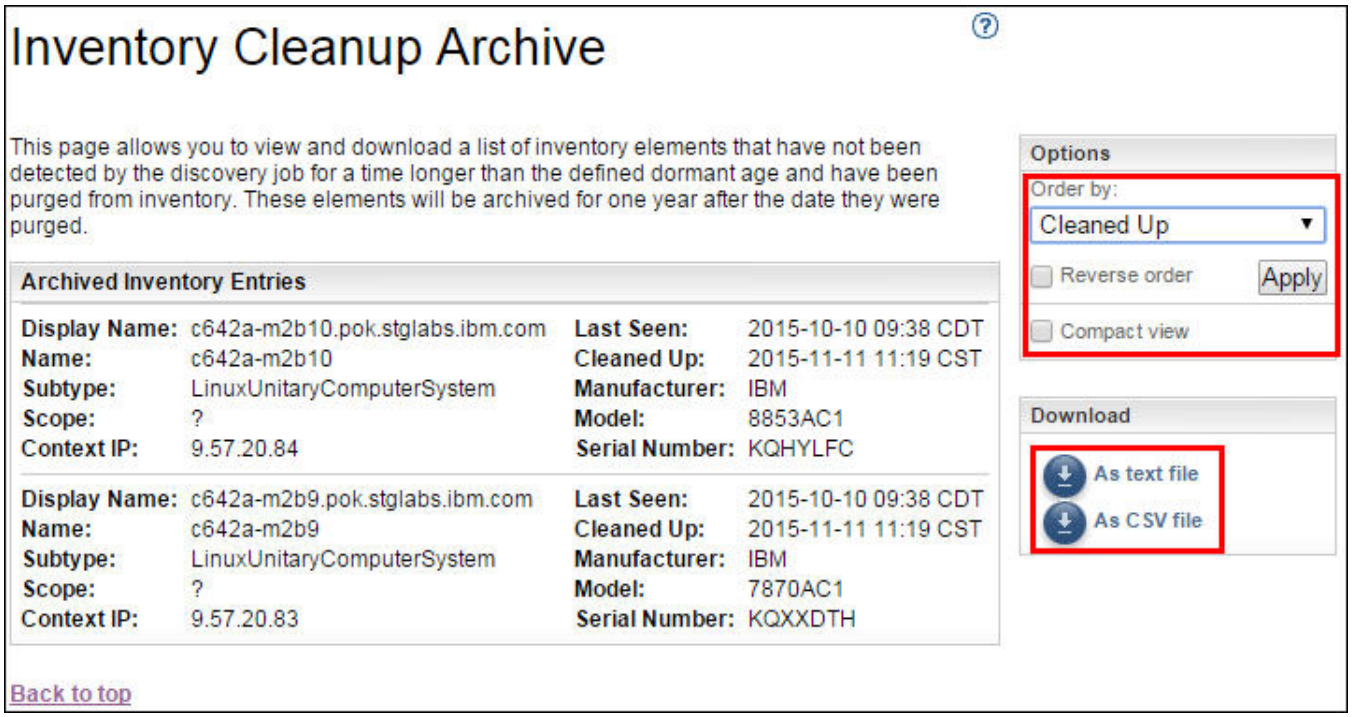

Figura 82. Arquivo de limpeza de inventário

2. Na página **Archive de limpeza de inventário**, é possível visualizar os elementos que são limpos do inventário como parte de um processo de limpeza.

   Nota:

   - É possível ver as informações sobre o inventário neste archive apenas por um ano. Após um ano, as informações do archive são excluídas.
   - O archive ficará vazio (ou seja, nenhum objeto será limpo), se todos os destinos definidos estiverem sendo descobertos ativamente no último ano.

3. Use a área de janela **Opções** para reordenar os detalhes do inventário.
   a) Selecione a propriedade **Ordenar por** na área de janela **Opções** e clique em **Aplicar** para ordenar a visualização dos detalhes do inventário.
   b) Selecione a opção **Reverter ordem** para visualizar os detalhes na ordem reversa da propriedade selecionada.

c) Selecione a opção **Visualização compacta** para visualizar um resumo do inventário.

4. Clique em **Como arquivo de texto** ou **Como arquivo CSV** para fazer download dos detalhes do inventário. Salve os detalhes do inventário para manipular os dados localmente e também preservar os dados no seu computador por um período mais longo (mais de um ano). Os dados que são preservados neste archive são mantidos apenas por um ano e depois são limpos.

Senhas

Use senhas para proteger as contas do usuário do TSA.

Mudando sua senha

Mude a senha do usuário do TSA.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Senha**.
   A página **Senha** é exibida.
2. Insira sua senha atual no campo **Senha atual**.
3. Insira a nova senha no campo **Nova senha**.
   A senha deve obedecer às seguintes regras:
   - Deve ter pelo menos oito caracteres
   - Deve conter pelo menos um caractere alfabético e um não alfabético
   - Não deve conter o nome do usuário
   - Não deve ser igual a nenhuma das oito últimas senhas
   - Deve ser mudada pelo menos a cada 90 dias, mas não deve ser mudada mais de uma vez por dia.
4. Insira a nova senha novamente no campo **Confirmar senha**.
   As duas senhas inseridas são comparadas para confirmar a correspondência antes que a senha seja salva.
5. Clique em **Salvar**.

O que Fazer Depois

Importante: Não é possível recuperar uma senha, portanto, se você perder ou esquecer a senha, não será possível efetuar login no TSA para mudar as credenciais. Se você perder ou esquecer sua senha de uma conta de usuário ou de administrador (se você tiver várias contas), entre em contato com o administrador do TSA. Se você perder ou esquecer sua senha da conta de administrador padrão (fornecida com o TSA), entre em contato com o Suporte IBM. Para obter mais informações, consulte a seção “Efetuando login no Technical Support Appliance” na página 21.

Segurança

É possível acessar e modificar funções e utilitários de segurança para o TSA.

A página **Segurança** lista os utilitários de segurança disponíveis. Nesta página, é possível modificar as configurações de tempo limite da sessão ou modificar a idade máxima da senha para todas as contas de usuário.

Modificando as configurações de tempo limite de sessão

Para segurança, o usuário é desconectado do TSA após um período de inatividade. É possível impedir que o TSA efetue logout automático do usuário ou mude a quantidade de tempo antes que o usuário seja desconectado.

Desativando o tempo limite de sessão

É possível impedir que o TSA efetue logout automático do usuário após um período de inatividade, desativando o tempo limite de sessão.

Procedimento

1. Marque a caixa de seleção **Desativar o tempo limite de sessão**.
2. Clique em **Mudar as configurações de tempo limite de sessão**.

Modificando o valor de tempo limite de sessão

Por padrão, o usuário é desconectado após 20 minutos de inatividade. É possível aumentar a quantidade de tempo antes da desconexão do usuário modificando o valor do tempo limite de sessão.

Procedimento

1. Limpe a caixa de seleção **Desativar o tempo limite de sessão**.
2. No campo **Tempo limite de sessão**, insira o tempo em segundos antes de o TSA efetuar logout do usuário.

   Nota: Esse tempo limite de sessão não pode ser menor que 20 minutos.
3. Clique em **Mudar as configurações de tempo limite de sessão**.

Modificando a duração da senha

Como medida de segurança, cada usuário deve alterar a senha de login do TSA após um número específico de dias. Por padrão, a duração máxima de uma senha é 90 dias, mas é possível alterar para 30 ou 60 dias.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Segurança**. A página **Segurança** é exibida.
2. Na página **Segurança**, role para baixo para visualizar a área de janela **Idade máxima da senha**.
3. Na área de janela **Idade máxima da senha**, selecione a idade (30, 60 ou 90 dias) na lista suspensa **Idade máxima**.
4. Clique em **Alterar a duração máxima da senha** para atualizar. A mensagem de confirmação **-** *Maximum password age updated.* é exibida.

Backup e restauração

É possível fazer backup e restaurar a configuração do TSA.

Importante: É altamente recomendável fazer backups regularmente. Além disso, um backup deve ser executado após mudanças serem feitas nos conjuntos de escopos ou nas credenciais.

Data do backup

Exibe a data e a hora do backup mais recente.

Resumo da configuração

Use essa opção para visualizar um resumo da configuração atual do TSA antes de salvá-la.

Para exibir o resumo da configuração do TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Backup e Restauração**. A página **Backup e Restauração** é exibida.

2. Clique em **Visualizar resumo** para visualizar o resumo da configuração atual do TSA. As informações exibidas mostram as configurações que o TSA salva se um backup for executado.

   Nota: Essas informações são mostradas em uma janela pop-up. Se o seu navegador da web bloquear janelas pop-up, talvez seja necessário permitir que o navegador exiba pop-ups do TSA.

   Na página **Resumo**, a seção **Backup** exibe informações relacionadas a status de backup com as seguintes mensagens:

   - Um ícone *OK* (), se o último backup foi realizado em 60 dias.
   - Um ícone *Warning* (), se o backup não foi realizado no período de 60 a 90 dias.
   - Um ícone *Error* (), se o backup não foi realizado por mais de 90 dias.

Backup

Use essa opção para salvar uma cópia da configuração do TSA.

Para fazer backup da configuração do TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Backup e Restauração**. A página **Backup e Restauração** é exibida.

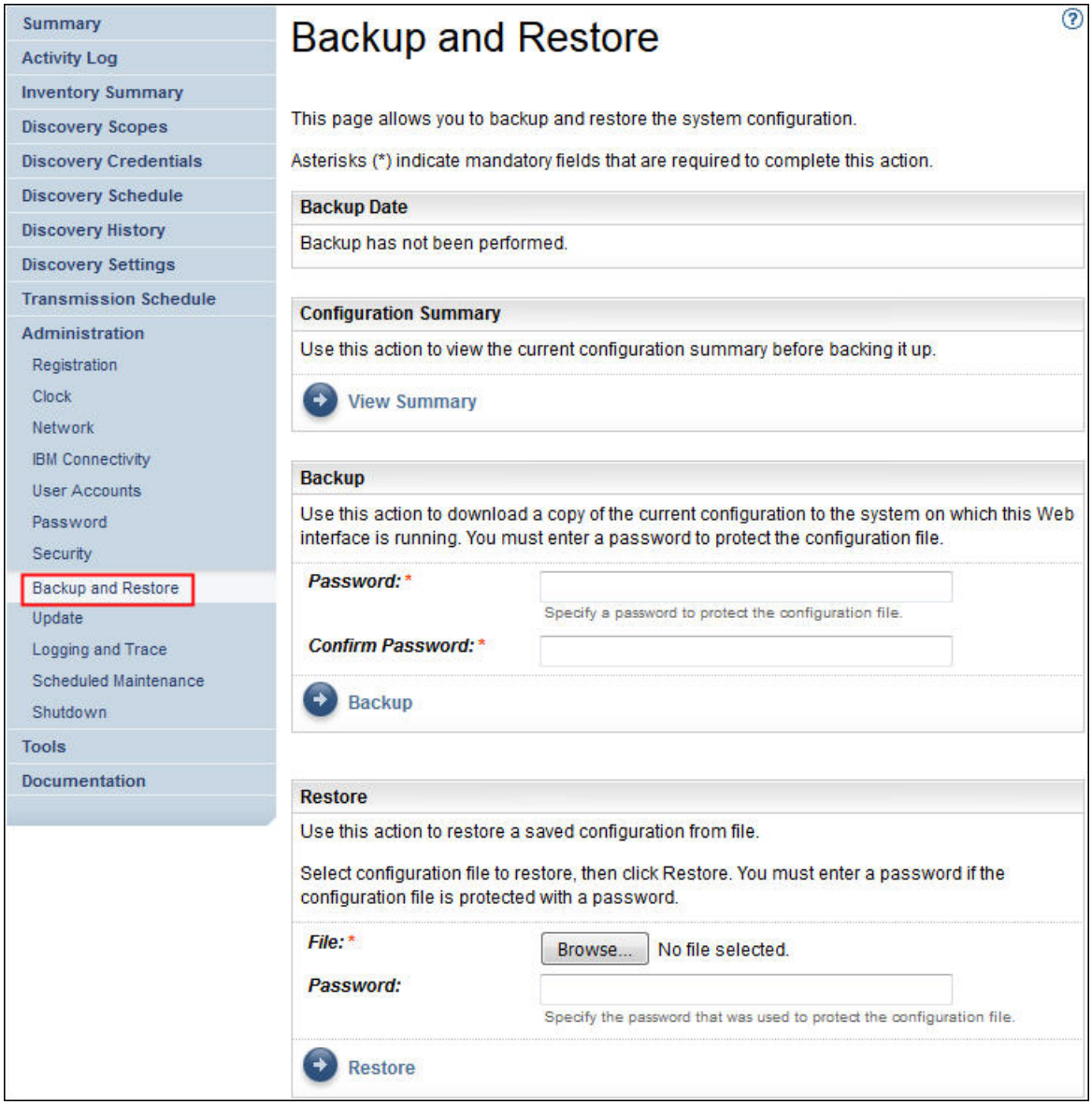

Figura 83. Backup e restauração

2. Insira uma senha na área de janela **Backup** para proteger o arquivo de configuração.
3. Insira a senha novamente no campo **Confirmar senha**. As duas senhas inseridas são comparadas para confirmar a correspondência antes que a senha seja salva.

   Nota: É necessário salvar a senha com segurança, pois ela é necessária durante a restauração.
4. Clique em **Backup** e salve o arquivo compactado da configuração de backup no sistema.

   Nota: O arquivo de configuração de backup gerado pode ser aberto apenas pelo TSA.

   Nota: Se você mudou sua senha de administrador recentemente, faça um backup após mudar a senha e use o arquivo de backup mais recente para restaurar.

Restaurar

Use essa opção para restaurar uma cópia da configuração salva anteriormente.

Para restaurar uma configuração do TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Backup e Restauração**. A página **Backup e Restauração** é exibida.

2. Clique em **Escolher arquivo** para localizar e selecionar o arquivo de configuração que você deseja restaurar.
3. Insira a senha usada para fazer backup do arquivo de configuração.
4. Clique em **Restaurar**.

   A tarefa de restauração é exibida no painel Resumo da tarefa da página **Resumo**. Quando a restauração estiver concluída, você será solicitado a reiniciar o sistema.

   Nota: A restauração de um backup exclui as configurações existentes. Todas as configurações, incluindo as definições de escopo e as credenciais, são substituídas pelas contidas no arquivo de backup.

Nota: Certifique-se de que o status do Discovery Manager esteja no estado OK ( ) na página **Resumo** para executar operações de backup ou restauração. Se o Discovery Manager não estiver em execução, você receberá uma mensagem: "`Discovery Manager is not running. Please ensure the Discovery Manager status is depicted by the green check mark icon in the Summary screen before resuming activity (typically up to 10 minutes).`" Após 10 minutos, se o Discovery Manager não estiver em execução, entre em contato com o suporte IBM.

Atualizar

É possível verificar e fazer download de atualizações do TSA.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Atualizar**.
   A página **Atualizar** é exibida.

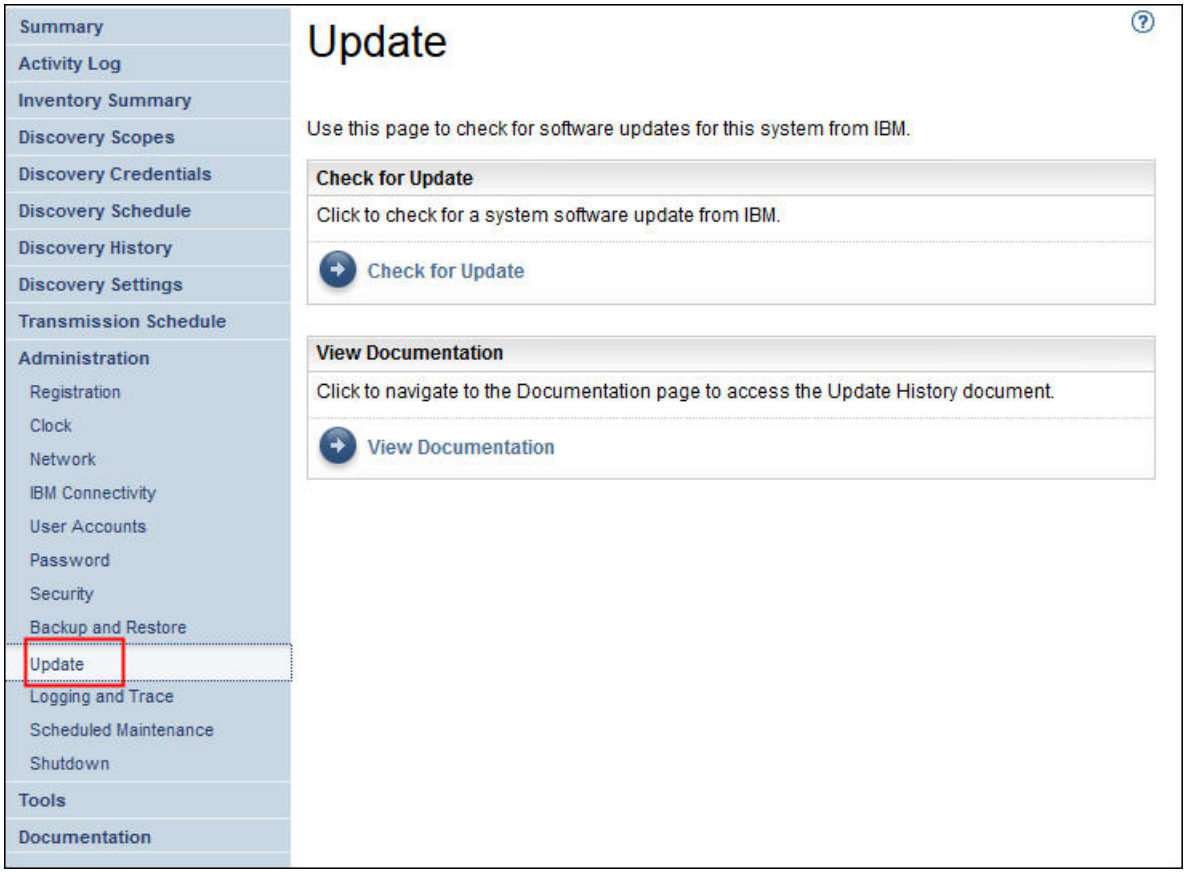

Figura 84. Atualizar

2. Clique em **Verificar atualização**.

A página **Atualizar disponibilidade** lista todas as atualizações disponíveis.

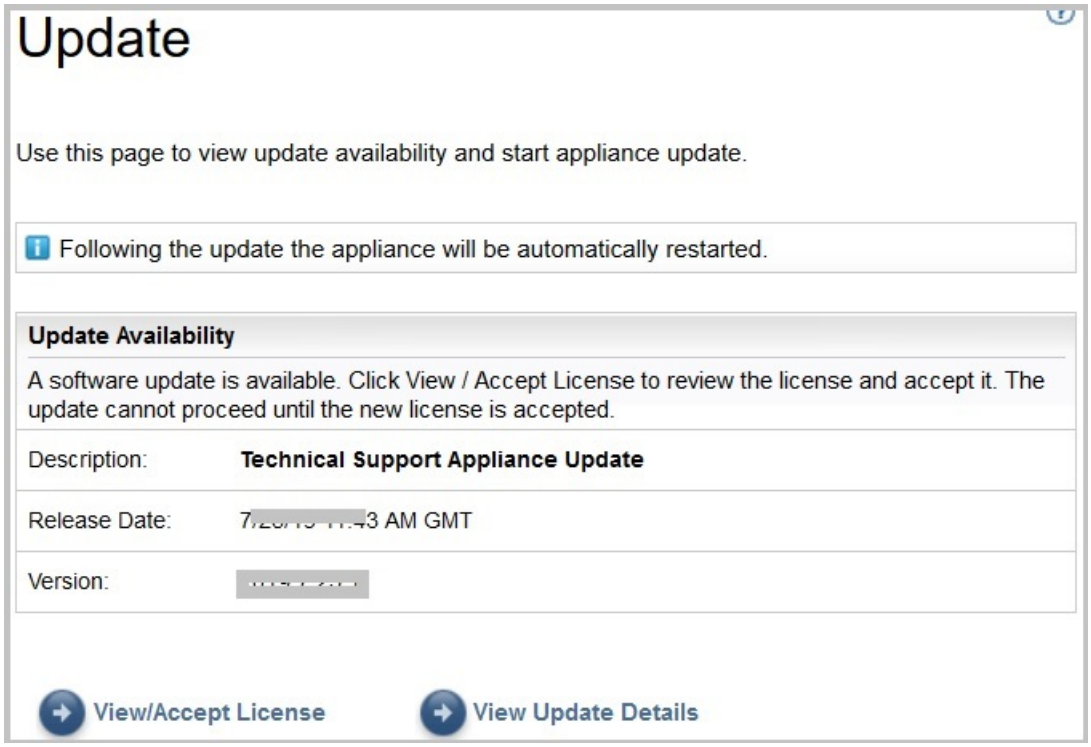

Figura 85. Atualizar disponibilidade

a) Para algumas novas liberações do TSA, deve-se aceitar um novo contrato de licença antes de continuar com a atualização. Se houver uma nova licença, clique em **Visualizar/aceitar licença**, a página **Contrato de licença** é exibida.

b) Clique no botão **Aceitar** na página **Contrato de Licença** para aceitar o novo Contrato de Licença. A página **Atualizar** é exibida novamente com o botão **Executar atualização agora**. Se não houver requisito para aceitar um novo contrato de licença, o botão **Visualizar/Aceitar licença** não será exibido. Clique em **Executar atualização agora** para continuar.

   Nota:

   - Depois de aceitar a licença, o botão **Visualizar/aceitar licença** não será mais exibido.
   - Na área de janela de navegação, clique em **Administração** > **Licença** para visualizar o contrato de licença mais recente que você aceitou.

c) Para instalar as atualizações, clique em **Executar atualização agora**.

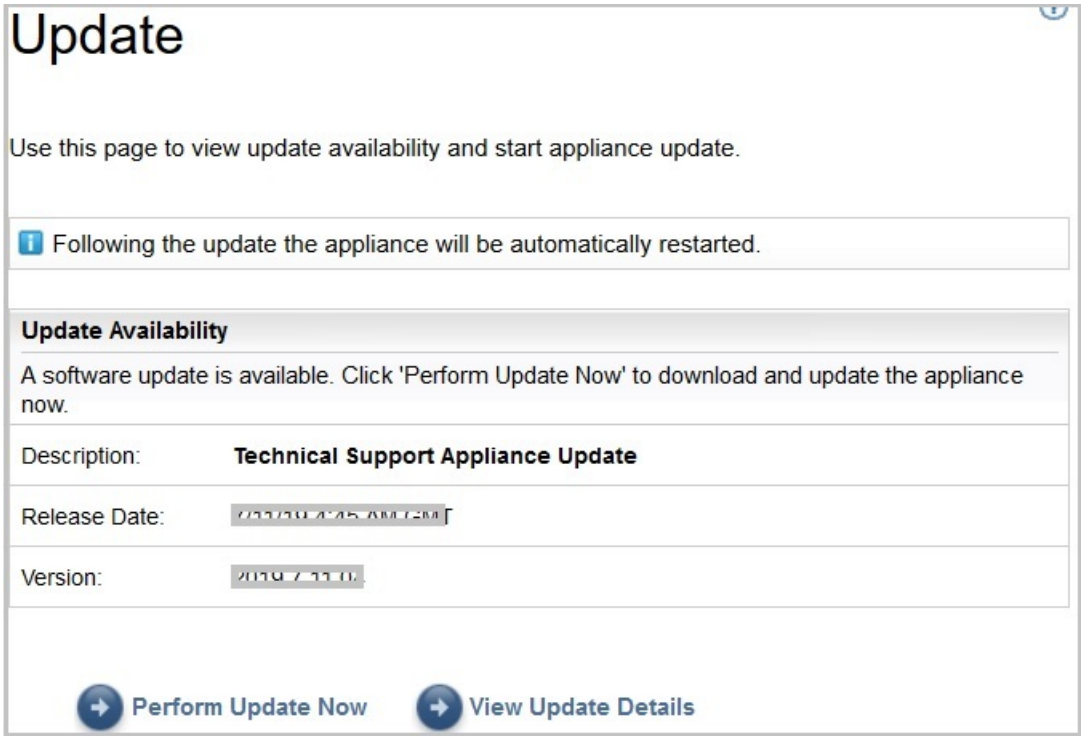

Figura 86. Executar a atualização agora

Após a conclusão da atualização, o TSA é reiniciado automaticamente.

d) Para visualizar informações sobre o conteúdo da atualização, clique em **Visualizar detalhes da atualização**.

Ativando manutenção planejada

Para manter o TSA em execução com desempenho ideal, recomenda-se ativar o recurso de manutenção planejada.

Sobre Esta Tarefa

A tarefa de manutenção planejada garante o desempenho ideal do TSA. É possível ativar ou desativar esse recurso a qualquer momento. Se você ativar a manutenção planejada, será possível definir o dia e a hora para executar automaticamente a manutenção. O status da manutenção planejada é exibido na seção **Status do sistema** da página **Resumo**.

Se você planejar a tarefa de manutenção, o sistema reiniciará automaticamente após a manutenção e você será notificado sobre a reinicialização do sistema uma hora antes de ocorrer. Por exemplo, `Devido à manutenção programada, uma tarefa de reinicialização do sistema será enfileirada em 59 minutos.`

Importante: Não agende a manutenção do dispositivo no período de 30 minutos de outras tarefas planejadas, como Descoberta, Transmissão e Limpeza de inventário. Se você planejar a manutenção dentro de 30 minutos de outras tarefas planejadas, o TSA não poderá executar essas tarefas.

Procedimento

Para editar o agendamento da manutenção, execute as seguintes etapas:

1. Na área de janela de navegação, clique em **Manutenção planejada**.

   A página **Manutenção planejada** exibe o **Agendamento** para a próxima execução planejada e o tempo de execução planejado. A seção **Histórico** exibe o status e mais detalhes das tarefas de manutenção em execução e anteriores.

2. Na página **Manutenção planejada**, clique em **Editar planejamento**.
   a) Na área de janela **Ativar planejamento**, selecione se deseja ativar ou desativar a manutenção planejada.
   b) Se você optar por ativar a tarefa de manutenção planejada, selecione as listas suspensas **Na hora** e **No minuto** para selecionar um novo horário.
   c) Selecione o **Modo de seleção de dia**. Para planejar a manutenção em determinados dias da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)** ou para planejar a manutenção em determinados dias do mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.
   d) Marque a caixa de seleção adequada para o campo **Nos dias** para selecionar dias diferentes ou adicionais da semana ou mês.

      Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.
3. Clique em **Salvar**.

   A página **Manutenção planejada** é exibida novamente com o novo planejamento.

Criação de log e rastreio

É possível visualizar e modificar as configurações de rastreio de diagnóstico do TSA. Também é possível modificar as configurações dos níveis de rastreamento do Discovery Manager. A modificação dessas configurações pode afetar o desempenho, portanto, faça isso apenas se orientado pelo Suporte IBM.

1. Na área de janela de navegação, clique em **Administração** > **Criação de log e rastreio**. A página **Criação de log e rastreio** é exibida. A área de janela **Nível de rastreio do TSA** mostra a configuração de rastreio atual (erro, aviso, informações, depuração ou rastreamento).

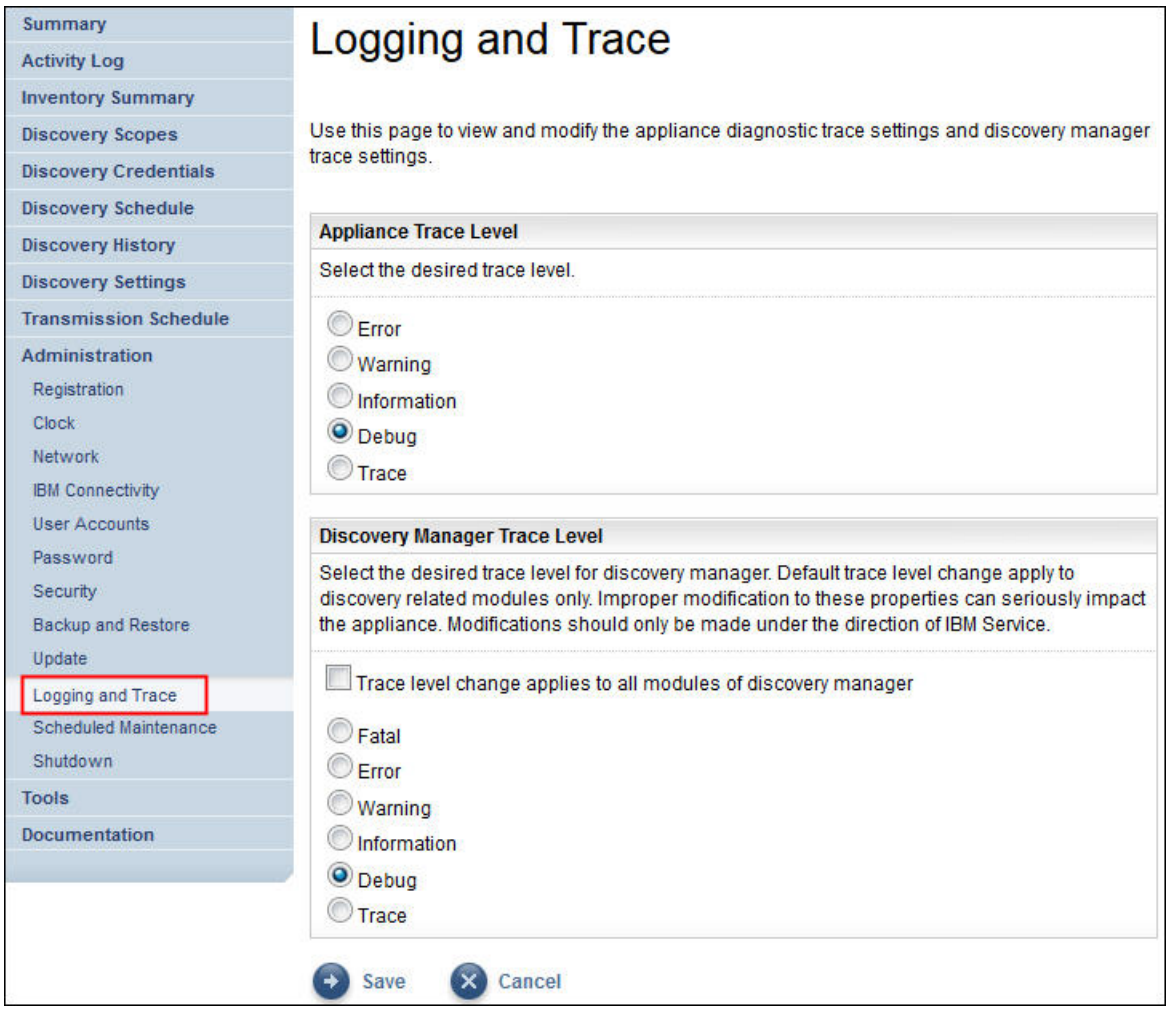

Figura 87. Gravação em log e rastreamento

2. Se necessário, será possível mudar a configuração de rastreio na seção **Nível de rastreio do TSA** clicando no botão de opções ao lado da configuração de rastreio desejada.
3. Clique em **Salvar**.

Nota: Por padrão, o nível de rastreio para o *TSA Trace Level* e suas áreas de janela *Discovery Manager Trace Level* é configurado para o nível de **Depuração**.

Para visualizar e modificar as configurações do **Discovery Manager Trace Level**, siga estas etapas:

Importante: Faça modificações nesta seção somente sob orientação do serviço da IBM.

1. Na área de janela de navegação, clique em **Administração** > **Criação de log e rastreio**. A página **Criação de log e rastreio** é exibida indicando a configuração de rastreio atual.
2. Marque **A mudança do nível de rastreio aplica-se a todos os módulos do gerenciador de descoberta** se você deseja que o nível de rastreio seja aplicado para todos os módulos do Discovery Manager.
3. Selecione o botão de opções ao lado da configuração de rastreio que você deseja.
4. Clique em **Salvar**.

Desligar

É possível suspender ou retomar as operações do TSA ou encerrar e, em seguida, reiniciar ou desligar o TSA.

O encerramento leva alguns minutos para ser concluído.

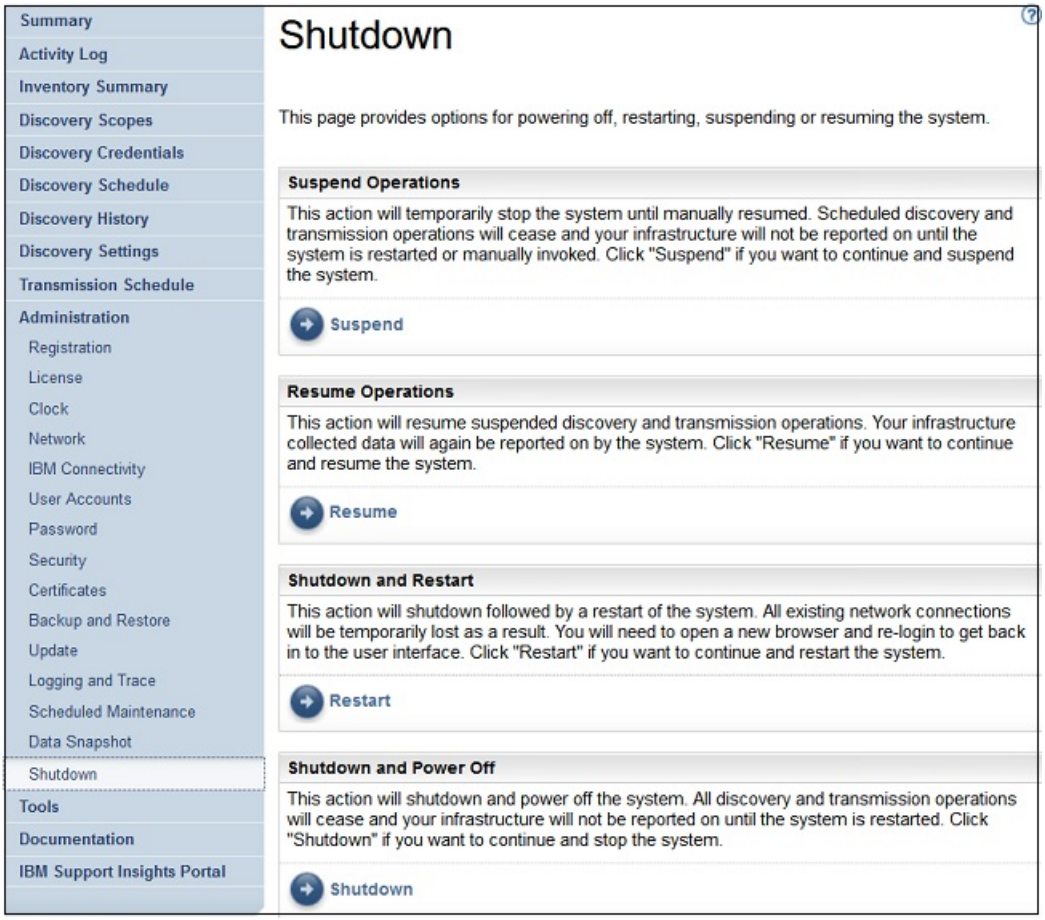

Figura 88. Desligar

Suspender operações

Essa ação para temporariamente o TSA. Todas as operações de descoberta e transmissão são interrompidas e nenhuma informação será relatada à IBM até que as operações sejam retomadas.

Para suspender as operações do TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Encerramento**. A página **Encerramento** é exibida.
2. Clique em **Suspender**.

   Nota: É possível verificar o status do TSA na página **Resumo**. Quando o TSA é suspenso, a área de janela **Status do sistema** mostra que o TSA foi suspenso.

Continuar operações

Essa ação retoma temporariamente o TSA interrompido. Todas as operações de descoberta e transmissão são retomadas e as informações são relatadas à IBM conforme planejado.

Para retomar as operações do TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Encerramento**. A página **Encerramento** é exibida.
2. Clique em **Retomar**.

Encerrar e reiniciar

Esta ação encerra e, em seguida, reinicia o TSA. Todas as conexões de rede existentes são temporariamente perdidas. Deve-se abrir um novo navegador e efetuar login novamente.

Para encerrar e reiniciar o TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Encerramento**. A página **Encerramento** é exibida.
2. Clique em **Reiniciar**.

Encerrar e desligar

Essa ação encerra e desliga o TSA. Todas as operações de descoberta e transmissão cessam e sua infraestrutura não será relatada até que o TSA seja reiniciado.

Para encerrar e desligar o TSA, siga estas etapas:

1. Na área de janela de navegação, clique em **Administração** > **Encerramento**. A página **Encerramento** é exibida.
2. Clique em **Encerrar**.

Nota: Depois de encerrar o dispositivo, deve-se ligar o TSA usando a interface da web do VMware ESXi ou o Hyper-V Manager.

Ferramentas

O TSA fornece ferramentas para ajudá-lo a configurar o ambiente do TSA.

É possível acessar essas ferramentas clicando em **Ferramentas** na área de janela de navegação.

Ferramentas de rede

Use a página **Ferramentas de rede** para obter ferramentas e informações de diagnóstico para os protocolos de rede que o TSA usa.

Para acessar essas ferramentas de diagnóstico, clique em **Ferramentas** > **Ferramentas de rede** na área de janela de navegação. A página **Ferramentas de rede** é exibida.

A página Ferramentas de rede é dividida em páginas com guias. Clique em qualquer guia para exibir a página que corresponde a essa guia.

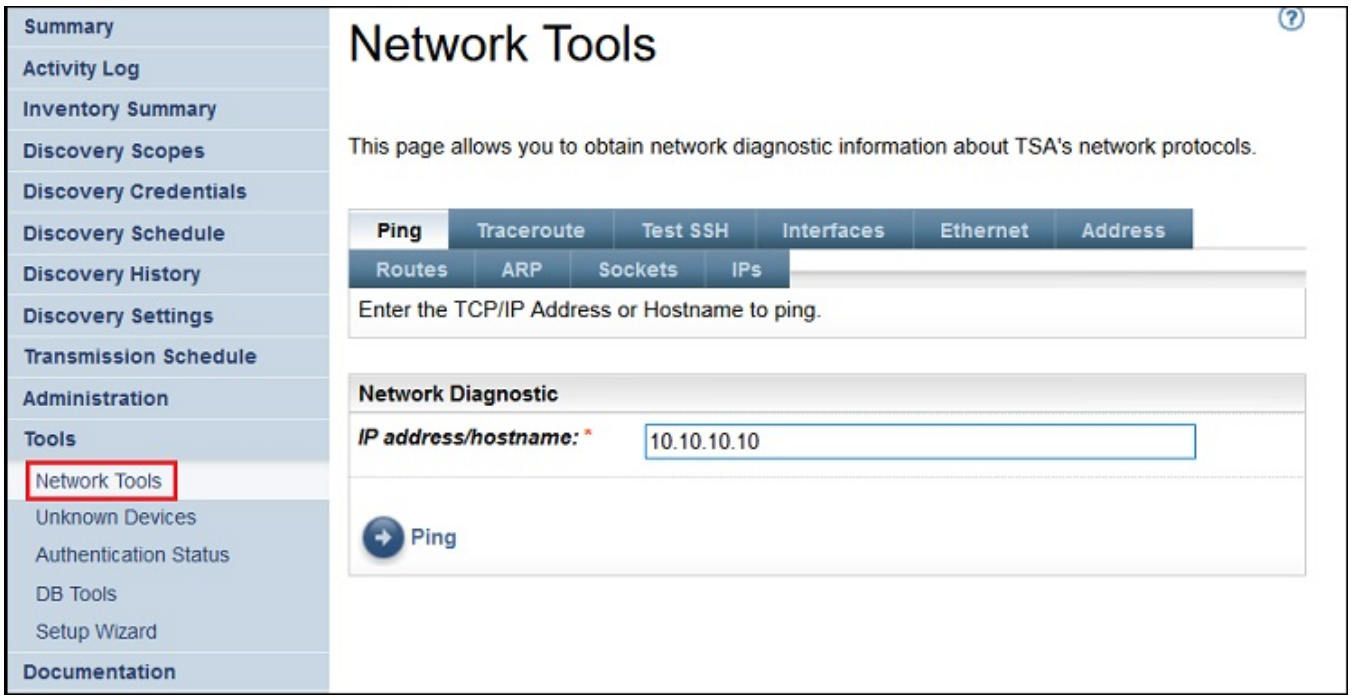

Figura 89. Ferramentas de rede

Ping
Use essa página para enviar uma solicitação de eco a um host remoto para verificar se o host está acessível e receber informações sobre o nome do host ou o endereço IP.

Rastrear rota
Use essa página para exibir o caminho que os pacotes percorrem para um host remoto.

Testar SSH
Use essa página para testar se um host remoto está acessível com SSH usando as credenciais de descoberta definidas para o host.

Interfaces
Use essa página para exibir as estatísticas para as interfaces de rede configuradas atualmente.

Ethernet
Use essa página para exibir as configurações das placas Ethernet que estão definidas atualmente.

Endereço
Use esta página para exibir os endereços IP das interfaces de rede que estão configuradas atualmente.

Rotas
Use essa página para exibir as tabelas de roteamento de IP do Kernel e as interfaces de rede correspondentes.

ARP
Use essa página para exibir o conteúdo das conexões de Address Resolution Protocol (ARP).

Soquetes
Use essa página para exibir informações sobre os soquetes de TCP/IP.

IPs
Use essa página para exibir informações sobre as regras de filtragem de pacotes de IP.

Nota: O nome do host digitado não deve conter sublinhado ("_").

Ferramentas de banco de dados

Use a página **Ferramentas de banco de dados** para executar operações de manutenção de dados. Recomenda-se o uso dessas funções somente quando solicitado pelo Suporte IBM.

É possível executar as seguintes operações no banco de dados:

Recriar o banco de dados do inventário

Ao recriar o banco de dados do inventário, todos os dados do inventário serão perdidos. Além disso, as credenciais serão perdidas se a caixa de seleção **Preservar credenciais** estiver desmarcada ou o Discovery Manager não estiver disponível.

Para recriar o banco de dados, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Ferramentas** > **Ferramentas do banco de dados**.
2. Marque a caixa de seleção **Preservar credenciais e escopos** na seção **Recriar banco de dados do inventário** para manter todas as credenciais de descoberta. Se você não selecionar a opção **Preservar credenciais e escopos**, as credenciais serão perdidas e será necessário configurar todas elas novamente. Para obter mais informações sobre as credenciais de descoberta, consulte "Credenciais de descoberta" na página 76.

   Nota: As credenciais e escopos poderão ser preservados apenas se o Discovery Manager estiver em execução (status verde).
3. Clique em **Recriar banco de dados do inventário**. A seguinte mensagem de aviso será exibida: `Taking this action will temporarily shutdown the Discovery Manager. Are you sure you want to recreate the inventory database?`
4. Clique em **OK** para recriar o banco de dados do inventário. A seguinte mensagem é exibida - `Recriar banco de dados iniciado`. Pode levar aproximadamente seis horas para recriar o banco de dados. Enquanto isso, a seguinte mensagem é exibida: `dbinit starting` na página Resumo. Após seis horas, será possível verificar o **Log de atividades** para visualizar o status como `Recreate inventory database successful`.

   Nota: Ao recriar o banco de dados do inventário, o Discovery Manager será encerrado temporariamente e *Inventory Clean-up Archive* será desmarcado.

Executando RUNSTATS

Para executar o comando **RUNSTATS**, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Ferramentas** > **Ferramentas do banco de dados**.
2. Clique em **Executar RUNSTATS**. A seguinte mensagem de aviso será exibida: `Are you sure you want to perform RUNSTATS on the inventory database tables?`
3. Clique em **OK**. A seguinte mensagem é exibida: `RUNSTATS iniciado`. Após aproximadamente 30 minutos, será possível verificar o log de atividades. Quando a tarefa for concluída, a seguinte mensagem será incluída no log de atividades: `RUNSTATS para banco de dados de inventário bem-sucedido`.

Executando REORG

Para executar o comando **REORG**, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Ferramentas** > **Ferramentas do banco de dados**.
2. Clique em **Executar REORG**. A seguinte mensagem de confirmação será exibida: `Are you sure you want to perform REORG on the inventory database tables?`
3. Clique em **OK**. A seguinte mensagem é incluída no log de atividades: `REORG Started`. Após aproximadamente 30 minutos, será possível verificar o log de atividades. Quando a tarefa for concluída, a seguinte mensagem será incluída no log de atividades: `REORG para banco de dados de inventário bem-sucedido`.

Documentação

Use a página **Documentação** para começar a usar o IBM Technical Support Appliance. É possível acessar guias de configuração e a documentação de segurança, visualizar relatórios de amostra e fazer download do código de instalação do TSA no website do TSA em: https://ibm.biz/TSAdemo.

Procedimento

Para visualizar a documentação e saber mais sobre o Technical Support Appliance, siga estas etapas:

1. Clique em **Documentação** no menu de navegação à esquerda.

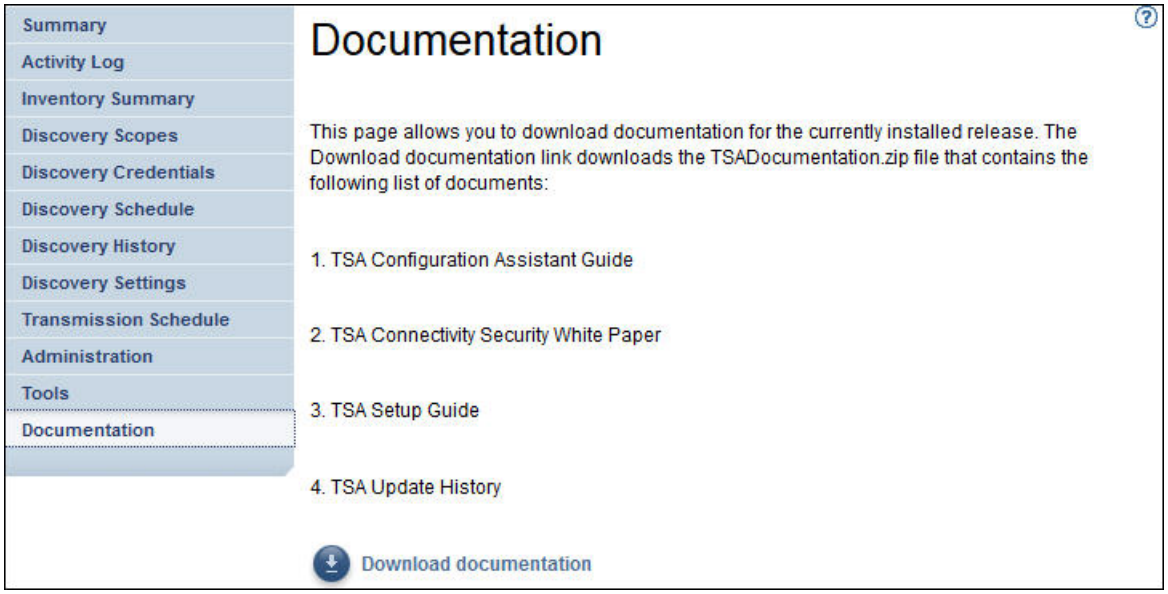

Figura 90. Documentação

2. Para saber mais sobre o Technical Support Appliance, clique no link: https://ibm.biz/TSAdemo
3. Na página **Instalar o TSA**, você encontrará links para a imagem do TSA, o guia de instalação, o guia de configuração e tutoriais relevantes.

Capítulo 7. Contatando o Suporte IBM para o Technical Support Appliance (TSA)

O Suporte IBM está disponível de segunda a sexta-feira, durante o horário comercial do seu fuso horário.

Sobre Esta Tarefa

É possível entrar em contato com o Suporte IBM de qualquer uma das duas maneiras a seguir:

1. Abra um chamado no Portal de Suporte IBM
2. Criando uma solicitação de serviço por meio da central de atendimento da IBM

Abrindo um chamado no Portal de Suporte IBM

Procedimento

1. Efetue logon no https://www.ibm.com/mysupport/s/

   Nota: Deve-se primeiro criar uma conta para acessar o Portal de Suporte IBM.
2. Clique em **Abrir um chamado** no lado direito superior do portal. A página **Abrir um chamado** é exibida.
3. Selecione o **Tipo de suporte**.
4. Insira o **Título**, o **Fabricante do produto** e o **Produto**.

   Nota: Para encaminhar sua solicitação diretamente para a equipe de suporte técnico, insira `Technical Support Appliance` no campo **Produto**.
5. Selecione a **Severidade**
6. Insira a **Descrição** e selecione seu idioma preferencial.
7. Se um agente que fala seu idioma não estiver disponível e você estiver interessado em se comunicar em inglês, selecione **Yes**.
8. Clique em **Enviar chamado**.

Criando uma solicitação de serviço por meio da central de atendimento da IBM

Procedimento

1. Disque o número de telefone correto para o país de origem: https://www.ibm.com/planetwide
2. Selecione o idioma.
3. Selecione 1 (produtos IBM).
4. Selecione 2 (produto de software).
5. Use o ID do produto *5621IZX01* ou o nome do produto *Technical Support Appliance*.
6. Serão solicitadas as seguintes informações:
   - Número/localização geográfica da empresa
   - Nome do cliente/empresa
   - Endereço/cidade/estado/código postal
   - Prédio/sala do piso
   - Número de telefone no qual o TSA está localizado.

- Nome/e-mail/número do telefone do contato
- Descrição do problema
- Nível de severidade

Apêndice A. Configurando o Technical Support Appliance

Se você sair ou ignorar a configuração de qualquer uma das definições no **Assistente de configuração**, será possível configurá-las manualmente no menu de navegação esquerdo do TSA.

Registrando o Technical Support Appliance

O registro coleta as informações necessárias para identificar o TSA quando ele relata informações à IBM para análise.

Sobre Esta Tarefa

Para registrar, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Registro**.
   A página de **Registro** é exibida.

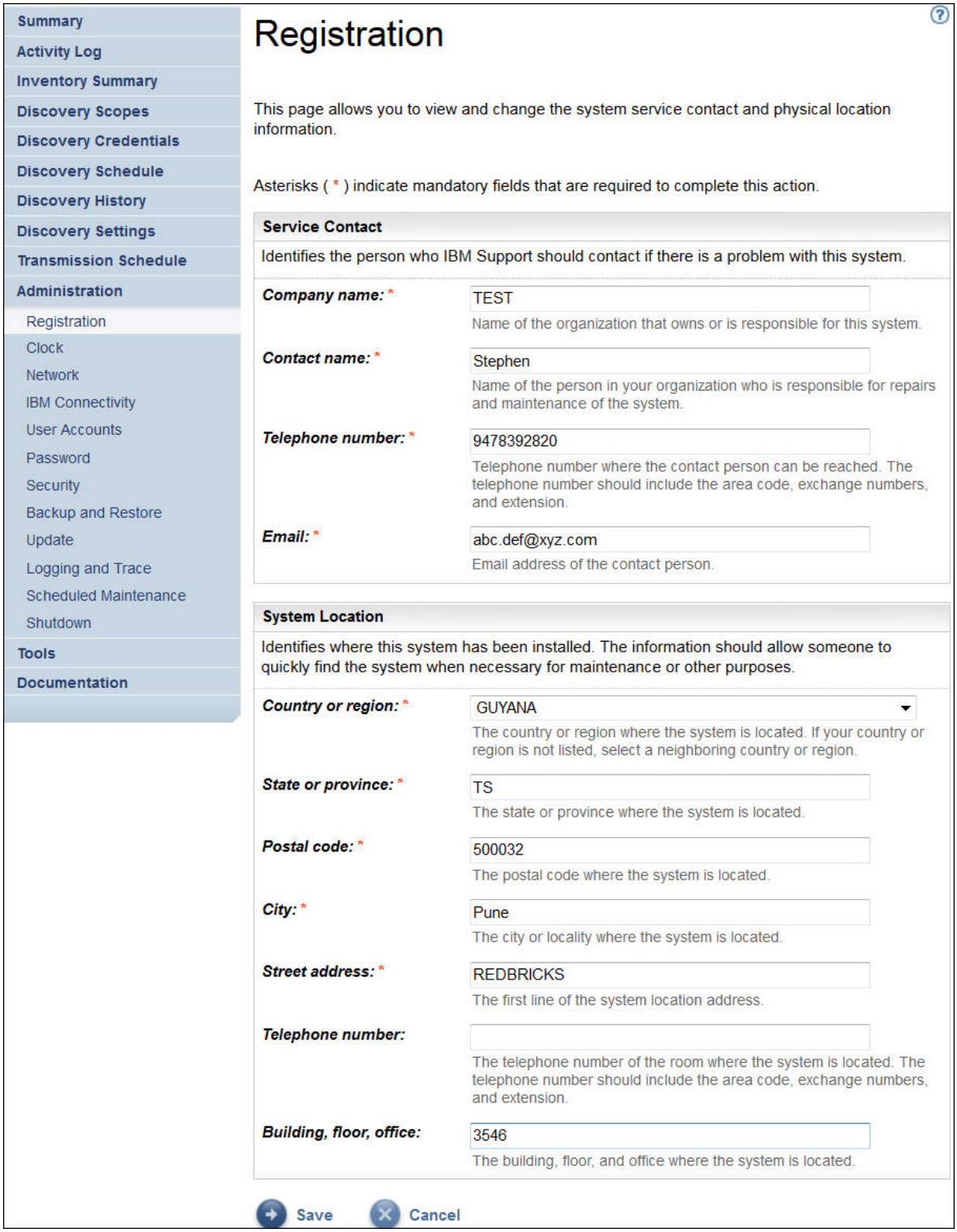

Figura 91. Registro

2. Especifique as informações de contato de serviço nos seguintes campos:

Nome da empresa
O nome da organização que usa o TSA.

Nome do contato
(Opcional) o nome da pessoa na organização que é responsável pelo TSA.

Número de telefone
(Opcional) O número de telefone da pessoa para contato. O número de telefone deve incluir o código de área, os números da central telefônica e o ramal. Não use parênteses no número de telefone.

E-mail
(Opcional) O endereço de e-mail da pessoa para contato.

IBMid
(Opcional) O IBMid da pessoa que você deseja autorizar para visualizar os relatórios no IBM Client Insights Portal.

Nota: É possível efetuar logon no https://clientinsightsportal.ibm.com/ com o IBMid associado para fazer o download dos seus TSA Reports em um a dois dias após cada transmissão de dados. Para se inscrever em um IBMid, acesse https://www.ibm.com/account.

Nota: O contato de serviço identifica a pessoa que o Suporte IBM deverá contatar caso haja algum problema com o sistema. As informações de contato são usadas para ajudar a IBM a fornecer à sua empresa os resultados da análise do Technical Support Appliance.

3. Especifique as informações de contato do TSA nos seguintes campos:

País ou região
O país ou a região em que o TSA está localizado.

Estado ou província
O estado ou o município em que o TSA está localizado. Se você não tiver certeza de qual estado é, digite *Unknown*

CEP
O código postal em que o TSA está localizado.

Cidade
A cidade ou localidade em que o TSA está localizado.

Endereço
Endereço da localização do TSA.

Número de telefone
(Opcional) O número de telefone da sala em que o TSA está localizado. O número de telefone deve incluir o código de área, os números da central telefônica e o ramal. Não use parênteses no número de telefone.

Prédio, piso, escritório
(Opcional) O prédio, andar e escritório em que o TSA está localizado.

4. Clique em **Salvar** para salvar as informações do registro.

Configurando a conectividade IBM

Especifique as informações de conexão com a Internet a serem usadas quando conectar à IBM.

Antes de Iniciar

Assegure-se de que seu firewall permita conexões com o nome do host e os endereços IP do servidor IBM, conforme explicado em Tabela 1 na página 6. Se sua rede não permitir acesso aos servidores IBM, as transações do TSA para o Suporte IBM falharão.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Conectividade IBM**.

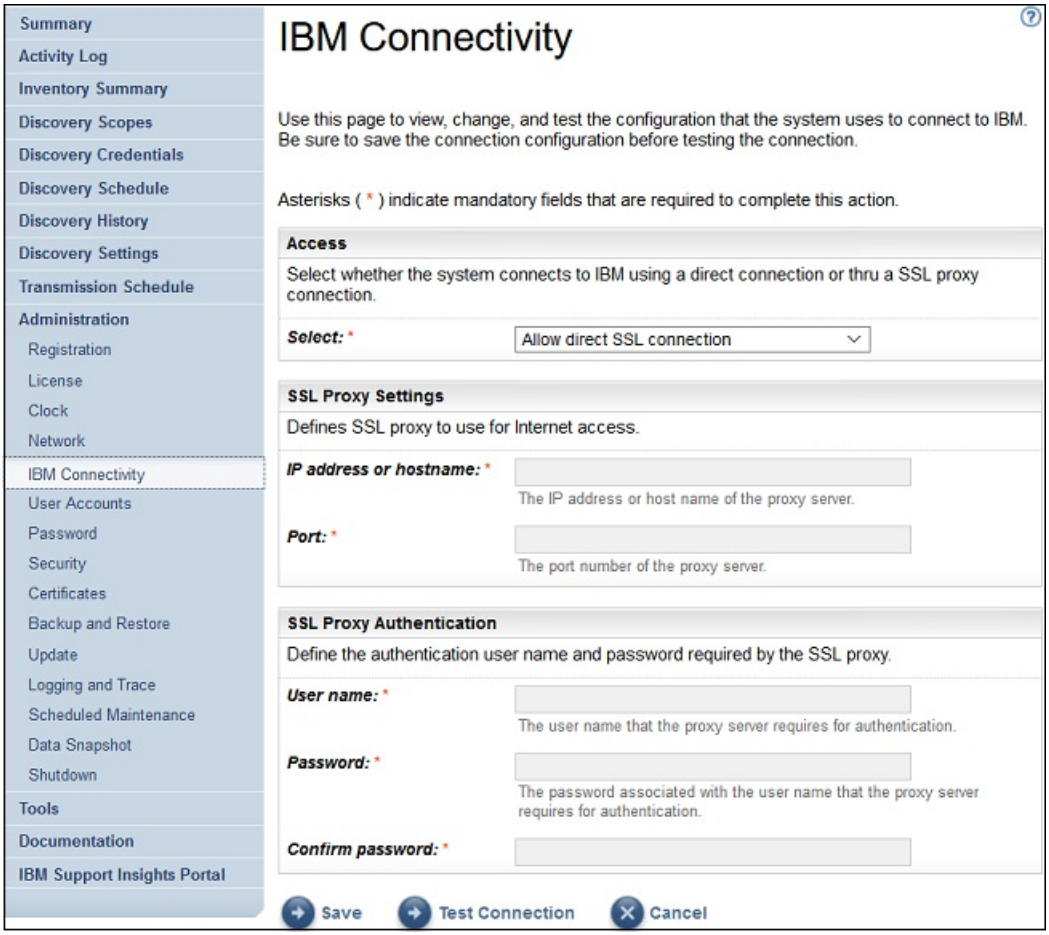

Figura 92. Conectividade IBM

2. Na área de janela **Acesso**, selecione um dos tipos de acesso à Internet a seguir:

   Permitir a conexão SSL direta
   O TSA se conecta à IBM usando uma conexão direta.

   Usar a conexão proxy SSL
   O TSA se conecta à IBM usando uma conexão proxy SSL.

   Usar a conexão proxy SSL de autenticação
   O TSA se conecta à IBM usando uma conexão proxy SSL de autenticação.

3. Se você selecionou **Usar conexão de proxy SSL** ou **Usar conexão de proxy SSL de autenticação**, especifique as seguintes informações para o servidor proxy.

   Endereço IP ou nome do host
   O endereço IP ou o nome do host do servidor proxy.

   Nota: O nome do host digitado não deve conter sublinhado ("_").

   Porta
   O número da porta do servidor proxy.

4. Se você selecionou **Usar conexão de proxy SSL de autenticação**, especifique as seguintes informações para o servidor proxy:

   Nome do usuário
   O nome do usuário que o servidor proxy requer para autenticação.

   Senha
   A senha associada ao nome de usuário que o servidor proxy requer para autenticação.

Confirmar senha
Insira a senha novamente. As duas senhas inseridas são comparadas para confirmar se são correspondentes antes que a senha seja salva.

5. Clique em **Salvar** para salvar as informações de conexão da IBM.
6. Clique em **Conexão de teste** para testar a conexão especificada.

Importante:

- Salve as configurações de conexão antes de testar a conexão.
- Deve-se ter uma conexão ativa com a IBM ou as funções do TSA não funcionarão.

Conceitos relacionados

Requisitos de configuração para conexões com o Suporte IBM

O TSA pode conectar-se ao Suporte IBM através de uma conexão direta ou através de um proxy fornecido pelo usuário que deve ser configurado para permitir a comunicação com a IBM. Se você estiver usando um proxy, a inspeção TLS/SSL não será suportada. Qualquer solicitação por meio de um proxy deve ser permitida para fluir diretamente para a IBM sem terminação TLS/SSL.

Configurando o clock

Deve-se definir a hora, a data e o fuso horário local do sistema TSA durante a configuração.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Relógio**.
   A página **Relógio** é exibida.

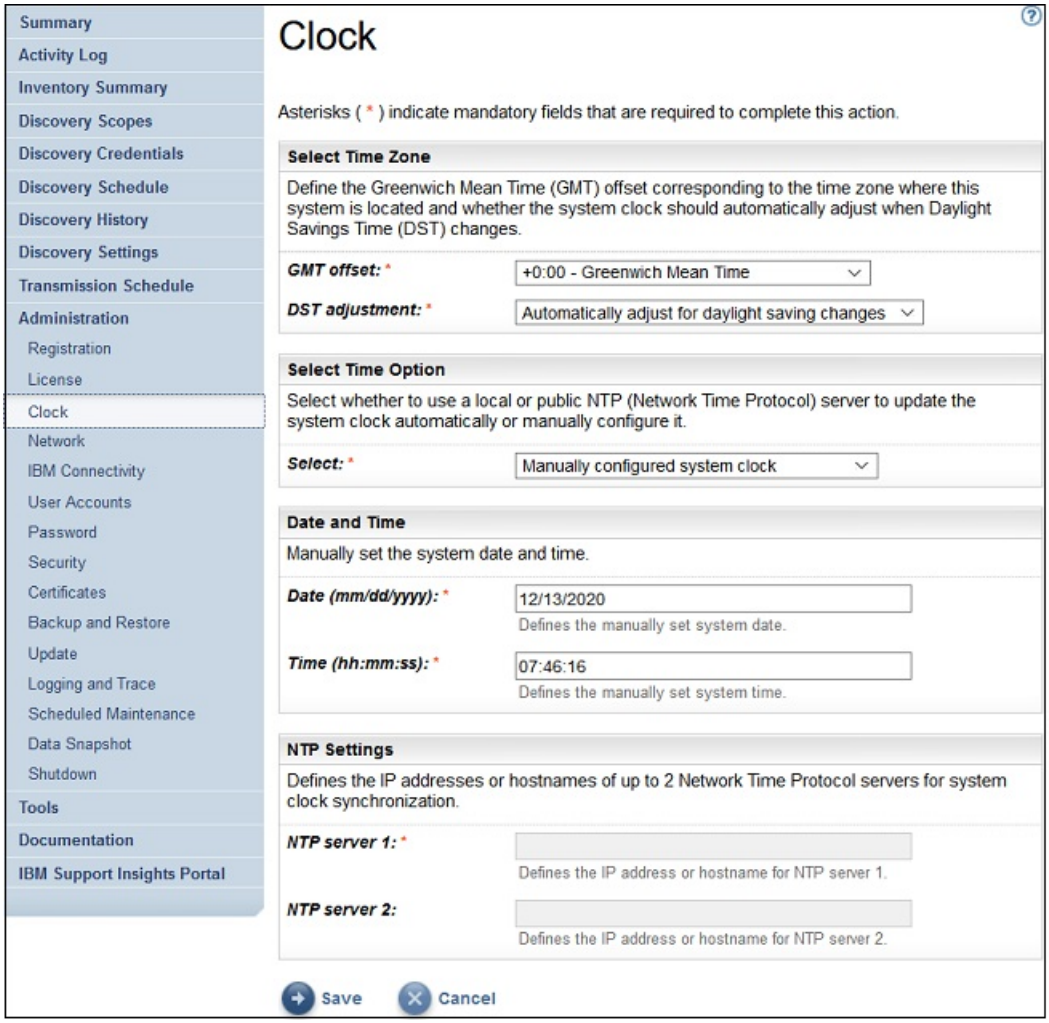

Figura 93. Relógio

2. Selecione seu fuso horário local na lista suspensa **Deslocamento do GMT**.
3. Selecione o ajuste de horário de verão na lista suspensa **Ajuste de horário de verão**.

   Nota: Nem todos os fusos horários permitem o DST. Se essa opção estiver selecionada para um fuso horário que não permitir horário de verão, uma mensagem de erro será exibida.
4. Selecione um método para atualizar o relógio do sistema na lista suspensa **Selecionar opção de horário**.

   As opções incluem a sincronização do relógio do sistema com um servidor Network Time Protocol (NTP) para atualizar o relógio do sistema automaticamente ou configurar manualmente.

   a) Se você selecionou configurar manualmente o relógio do sistema, deverá definir a data e a hora do sistema. Insira as informações de data e hora nos campos **Data** e **Hora**.

   b) Se a opção de sincronizar o clock do sistema com um servidor Network Time Protocol (NTP) para atualizar o clock do sistema automaticamente foi selecionada, os endereços IP e os nomes de host deverão ser especificados para os servidores NTP. Digite as informações de endereço IP ou do nome do host para até dois servidores nos campos **Servidor NTP**.

   Nota: Verifique se o servidor NTP está acessível através da rede para o TSA.
5. Clique em **Salvar** para salvar as informações do relógio.

Resultados

Nota: Algumas mudanças requerem uma reinicialização para que entrem em vigor. Por exemplo, se você definir a data ou a hora ou mudar da configuração manual para a configuração do servidor NTP, você será solicitado a reiniciar o sistema.

Configurando o planejamento de transmissão

O TSA fornece um planejamento padrão para o processo de transmissão ser executado em horários especificados. É possível modificar esse planejamento de acordo com suas necessidades.

Procedimento

1. Na área de janela de navegação, clique em **Planejamento de transmissão**.

   A página **Planejamento de transmissão** é exibida.

   O painel **Planejamento** exibe a próxima execução planejada e os tempos de execução planejados. A área de janela **Histórico** exibe o status e os detalhes adicionais das tarefas de transmissão em execução e anteriores.
2. Clique em **Editar planejamento**.

   A página **Planejamento de transmissão** é exibida.

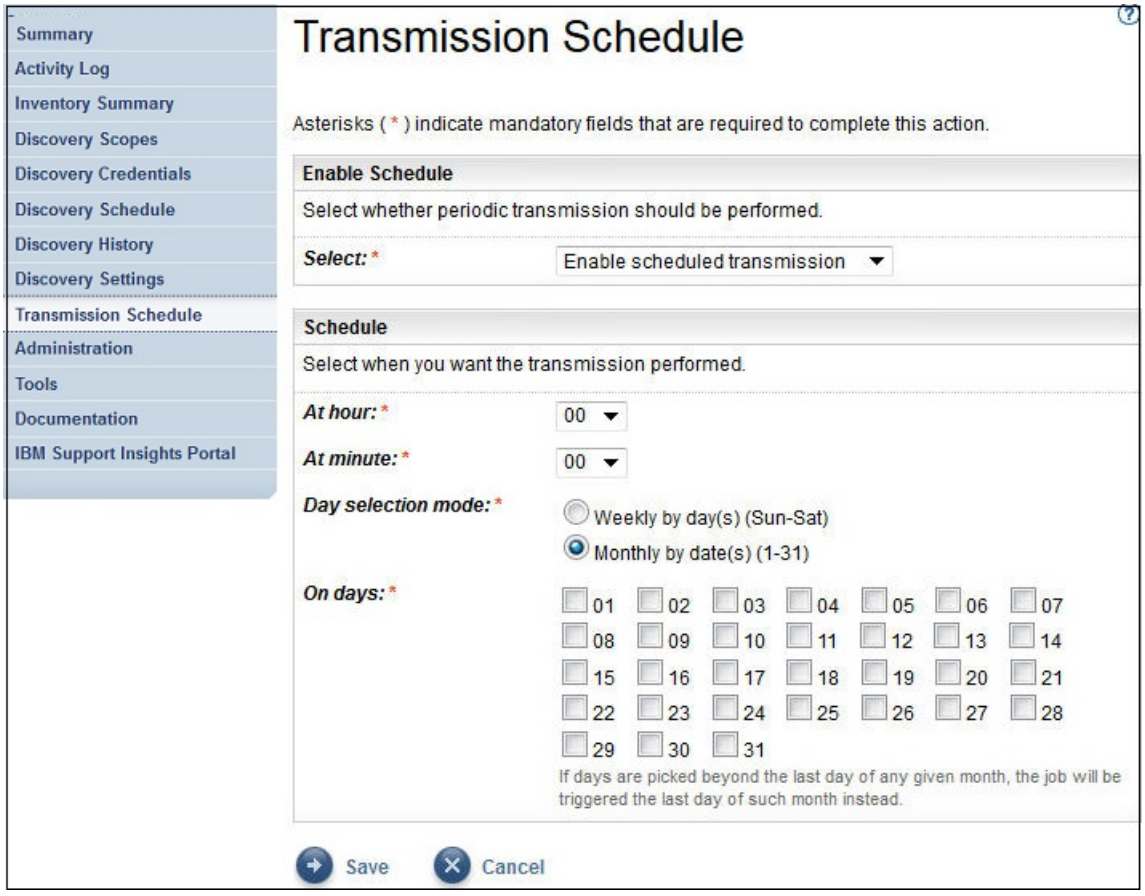

Figura 94. Editar planejamento de transmissão

   a) Use as listas suspensas **Na hora** e **No minuto** para selecionar um novo horário.

   b) Selecione o **Modo de seleção de dia**.

   Semanalmente por dia(s) (de domingo a sábado)
   Para planejar a transmissão em um determinado dia da semana, selecione a opção **Semanalmente por dia(s) (de domingo a sábado)**.

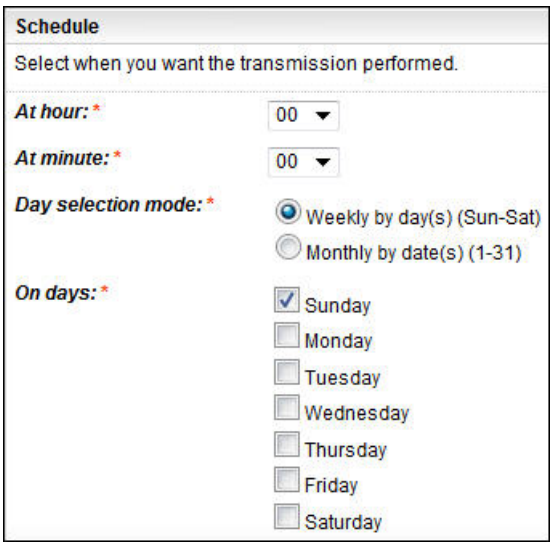

Figura 95. Semanalmente por dia(s) (de domingo a sábado)

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias da semana.

Mensalmente por data(s) (de 1 a 31)

Para planejar a transmissão em determinados dias de um mês, selecione a opção **Mensalmente por data(s) (de 1 a 31)**.

No campo **Nos dias**, marque a caixa de seleção adequada para selecionar um ou mais dias do mês.

Nota: Se você selecionar os dias além do último dia de um mês específico, a tarefa será acionada no último dia desse mês específico.

3. Clique em **Salvar**.
   A página **Planejamento de transmissão** é exibida novamente com o novo planejamento exibido.

Atualizar

É possível verificar e fazer download de atualizações do TSA.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Atualizar**.
   A página **Atualizar** é exibida.

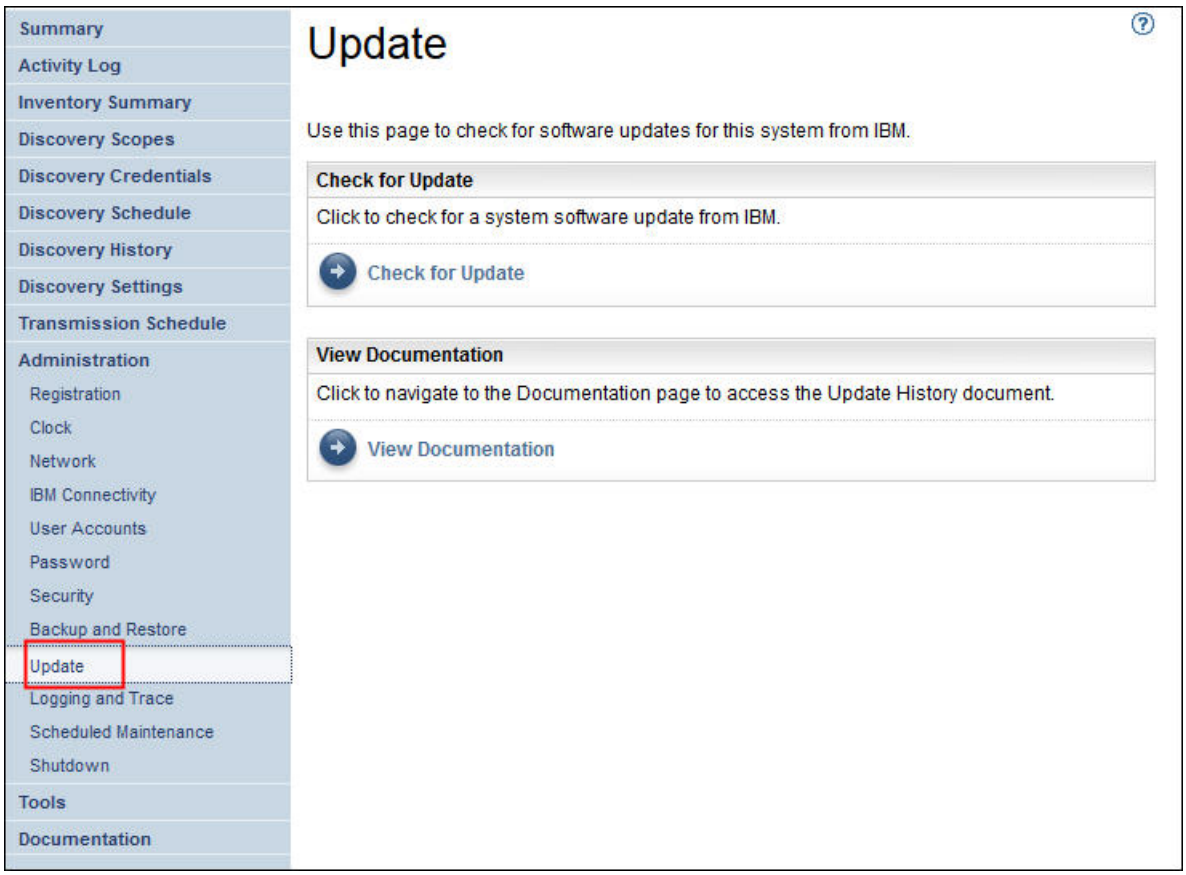

Figura 96. Atualizar

2. Clique em **Verificar atualização**.
   A página **Atualizar disponibilidade** lista todas as atualizações disponíveis.

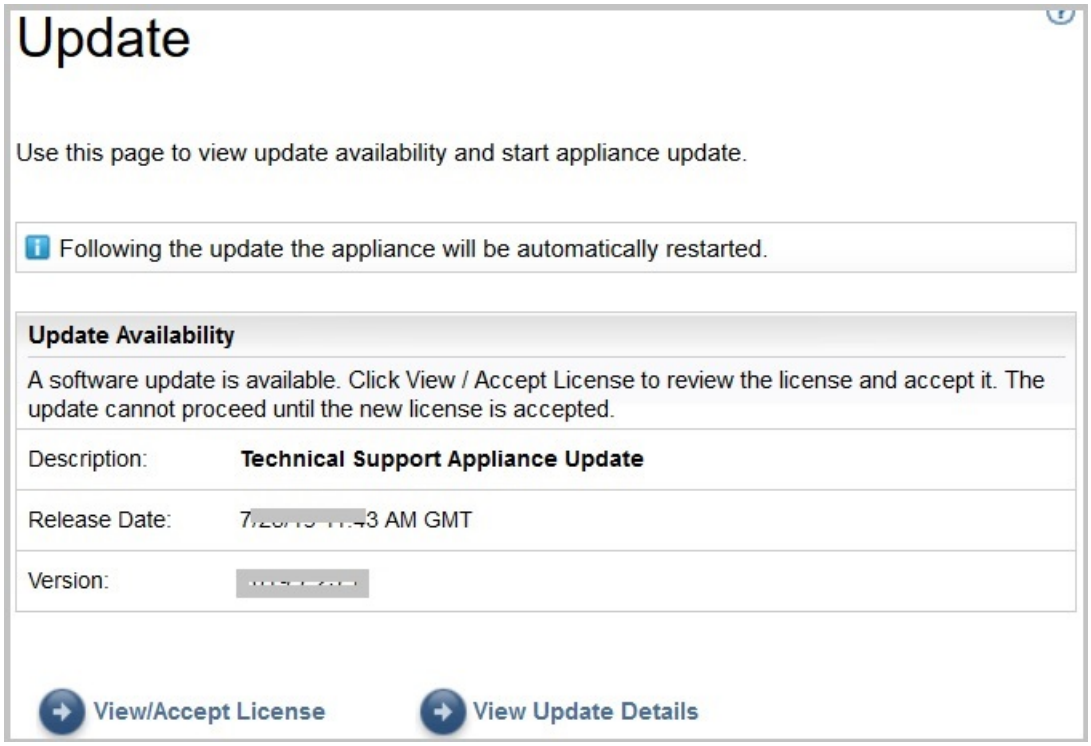

Figura 97. Atualizar disponibilidade

a) Para algumas novas liberações do TSA, deve-se aceitar um novo contrato de licença antes de continuar com a atualização. Se houver uma nova licença, clique em **Visualizar/aceitar licença**, a página **Contrato de licença** é exibida.

b) Clique no botão **Aceitar** na página **Contrato de Licença** para aceitar o novo Contrato de Licença. A página **Atualizar** é exibida novamente com o botão **Executar atualização agora**. Se não houver requisito para aceitar um novo contrato de licença, o botão **Visualizar/Aceitar licença** não será exibido. Clique em **Executar atualização agora** para continuar.

Nota:

- Depois de aceitar a licença, o botão **Visualizar/aceitar licença** não será mais exibido.
- Na área de janela de navegação, clique em **Administração** > **Licença** para visualizar o contrato de licença mais recente que você aceitou.

c) Para instalar as atualizações, clique em **Executar atualização agora**.

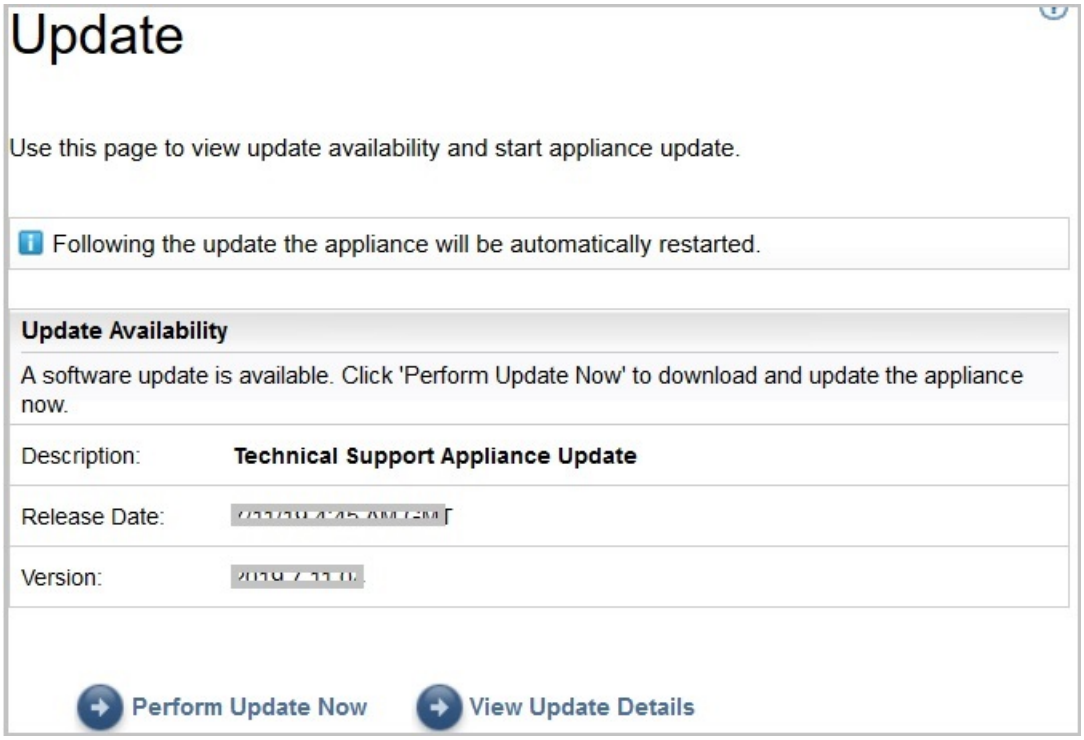

Figura 98. Executar a atualização agora

Após a conclusão da atualização, o TSA é reiniciado automaticamente.

d) Para visualizar informações sobre o conteúdo da atualização, clique em **Visualizar detalhes da atualização**.

Apêndice B. Configurando os detalhes de rede do DHCP

Siga estas etapas para configurar os detalhes de rede do DHCP:

Procedimento

1. Selecione a opção **1) Definir a configuração da rede** no **Menu de configuração do TSA**.

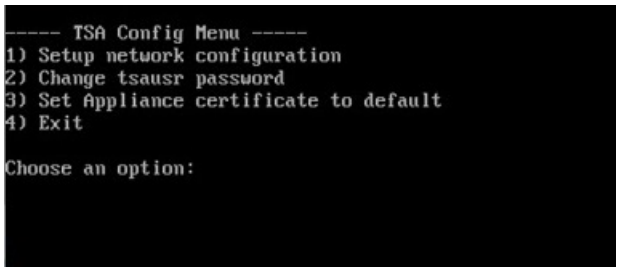

Figura 99. Definir a configuração de rede

2. Insira os detalhes da configuração de rede seguinte.

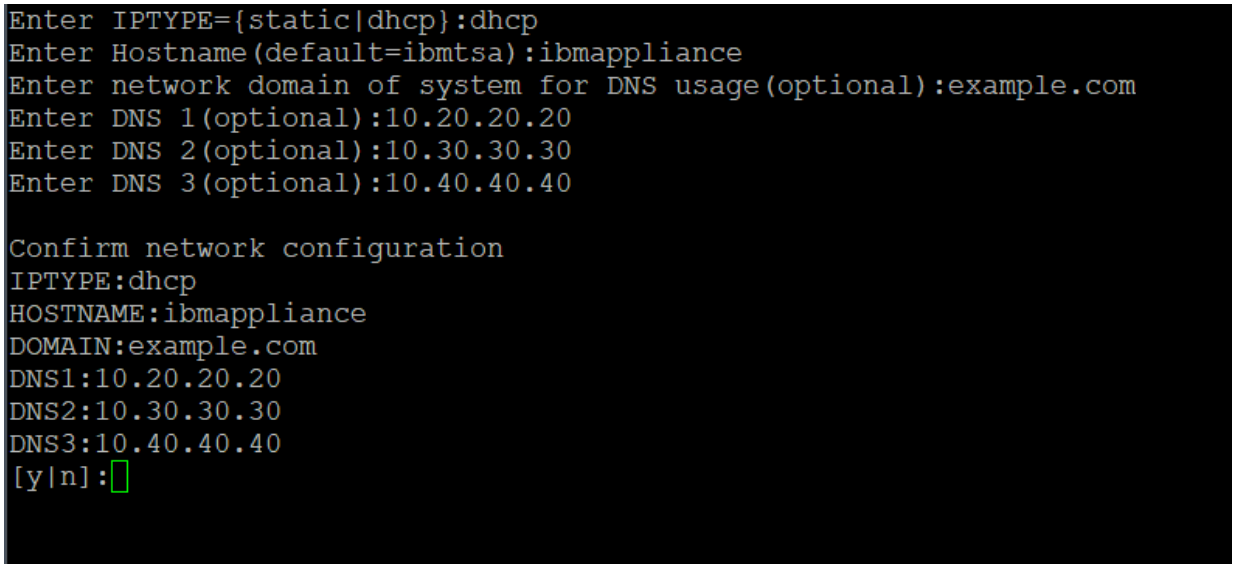

Figura 100. Configuração de rede

a) **Insira IPTYPE = {static|dhcp}**. Insira dhcp.

IPTYPE: dhcp

Enter Hostname(default=ibmtsa). É possível mudar o nome do host padrão. Assegure-se de que o nome do host usado seja exclusivo.

Enter network domain of system for DNS usage (optional).

Enter DNS 1(optional), **Enter DNS 2(optional)** e **Enter DNS 3(optional)**.

Os detalhes de configuração de rede especificados são exibidos para confirmação.

b) Insira **[y|n]** para confirmar ou descartar a configuração de rede. Inserir **y** salva a configuração de rede e reinicia o sistema automaticamente.

Nota: Para qualquer configuração incorreta, é possível mudar os detalhes. Insira **n** para ignorar as configurações atuais e reiniciar a configuração na etapa “2.a” na página 129

c) O sistema é reinicializado em 15 segundos para que a nova configuração de rede entre em vigor.

d) Após a reinicialização do sistema, efetue login no gerenciador de virtualização e anote o **Endereço IP** na guia **Resumo**.

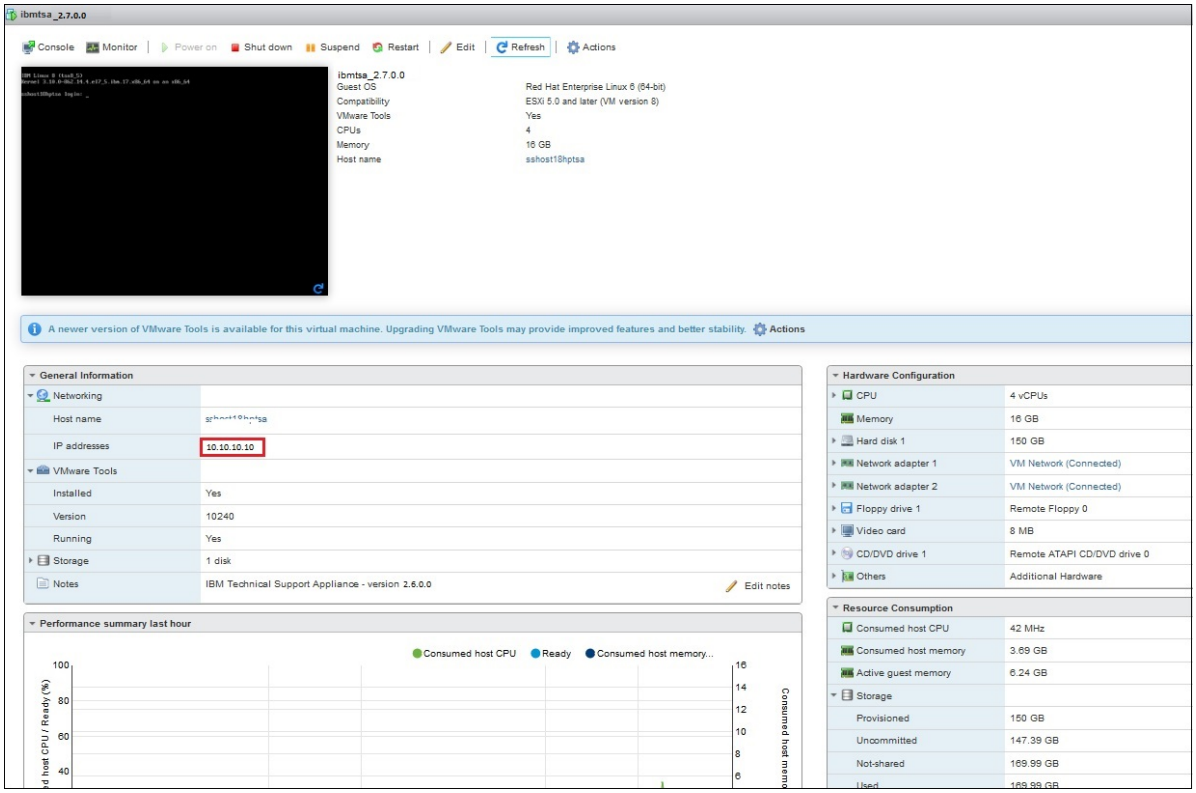

Figura 101. Endereço IP do DHCP

e) Acesse o TSA no navegador com a URL que você obteve na etapa anterior.
Por exemplo, `https://newhost1.new.abclabs.example.com`

Nota: Na primeira conexão, seu navegador pode exibir uma exceção de segurança. Deve-se aceitar o certificado de segurança e continuar para efetuar logon no TSA.

Apêndice C. Contas do usuário e grupos de usuários

É possível usar contas do usuário e grupos de usuários para conceder acesso às funções do TSA.

Antes de Iniciar

O TSA é instalado com uma conta de usuário chamada **administrador**. Ela tem autoridade para executar qualquer função do TSA. É possível incluir contas de usuário pelos motivos a seguir:

- Para permitir que outro usuário atue como um backup do usuário **administrador**.
- Para permitir que alguns usuários acessem uma quantidade limitada de funções no TSA.

Sobre Esta Tarefa

Executar qualquer função do TSA requer um determinado nível de autoridade. Se um usuário autenticado tentar executar uma função sem o nível de autoridade apropriado, um erro será exibido e a função não será executada.

No TSA, os níveis de autoridade são associados aos grupos de usuários. Os usuários recebem uma associação em um ou mais grupos de usuários e, por meio dessas associações, eles têm o nível de autoridade para executar funções específicas.

O TSA é fornecido com um grupo de usuários **administradores** e uma conta de usuário **administrador**. O grupo de usuários **administradores** tem acesso irrestrito a todas as funções do sistema. A conta de usuário **administrador** é designada ao grupo de usuários **administradores**.

Exibindo contas do usuário e grupos de usuários

É possível exibir as contas do usuário e os grupos de usuários existentes.

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.
   A página **Contas e grupos de usuários** é exibida.
2. Para exibir as contas do usuário existentes, clique na guia **Contas**.
   A tabela Contas do usuário exibe as contas do usuário

   Dica: Para visualizar detalhes de uma conta de usuário específica, clique no nome da conta do usuário. A área de janela **Geral** no lado direito exibe o nome do usuário, o nome completo e a descrição associados à conta de usuário selecionada. Clique na área de janela **Membro de** à direita para visualizar os grupos de usuários aos quais este usuário pertence.
3. Para exibir os grupos de usuários existentes, clique na guia **Grupos**.
   A tabela Grupos de usuários exibe os grupos de usuários.

   Dica: Para visualizar detalhes de um grupo de usuários específico, clique no nome do grupo de usuários. A área de janela **Geral** no lado direito exibe o nome e o nível de autoridade que estão associados ao grupo de usuários. Clique na área de janela **Restrições de escopo** à direita, para visualizar os conjuntos de escopos que o grupo de usuários selecionado pode descobrir. Clique na área de janela **Membros** para visualizar as contas de usuários associadas a este grupo de usuários.

Incluindo contas de usuário e grupos de usuários

É possível incluir contas e grupos de usuários para controlar o acesso às funções do TSA.
Conceitos relacionados
Escopos de descoberta e conjuntos de escopos

Os escopos de descoberta identificam os recursos que você deseja que o TSA descubra. Os escopos de descoberta são agrupados em conjuntos de escopos de descoberta.

Incluindo um grupo de usuários

É possível incluir grupos de usuários para controlar o acesso às funções do TSA.

Sobre Esta Tarefa

Para incluir um grupo de usuários, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.
   A página **Contas e grupos de usuários** é exibida.
2. Clique na guia **Grupos**.

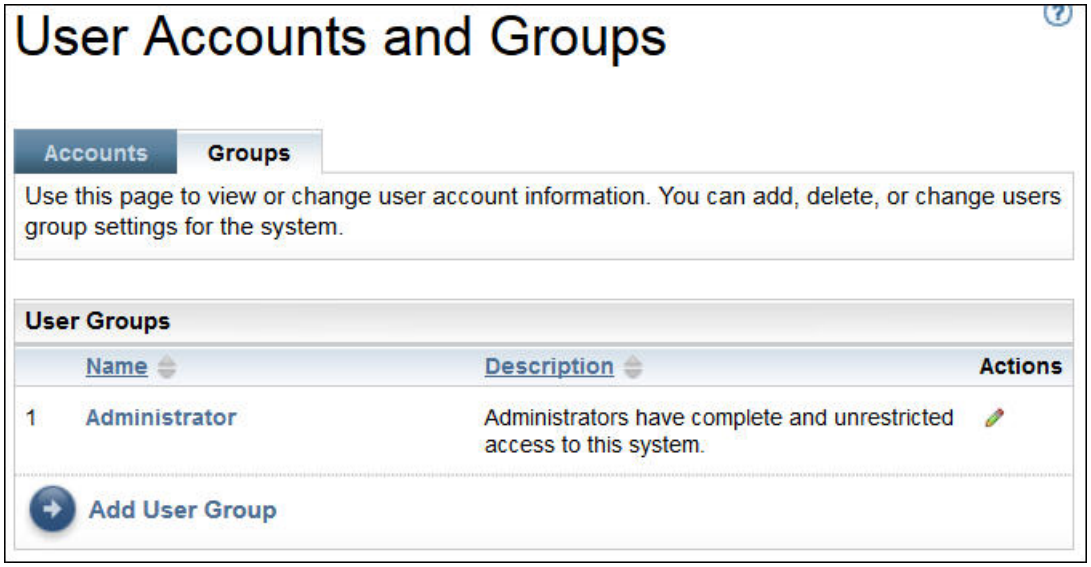

Figura 102. Grupos

3. Clique em **Incluir grupo de usuários**.
   A página **Grupo de usuários** é exibida.

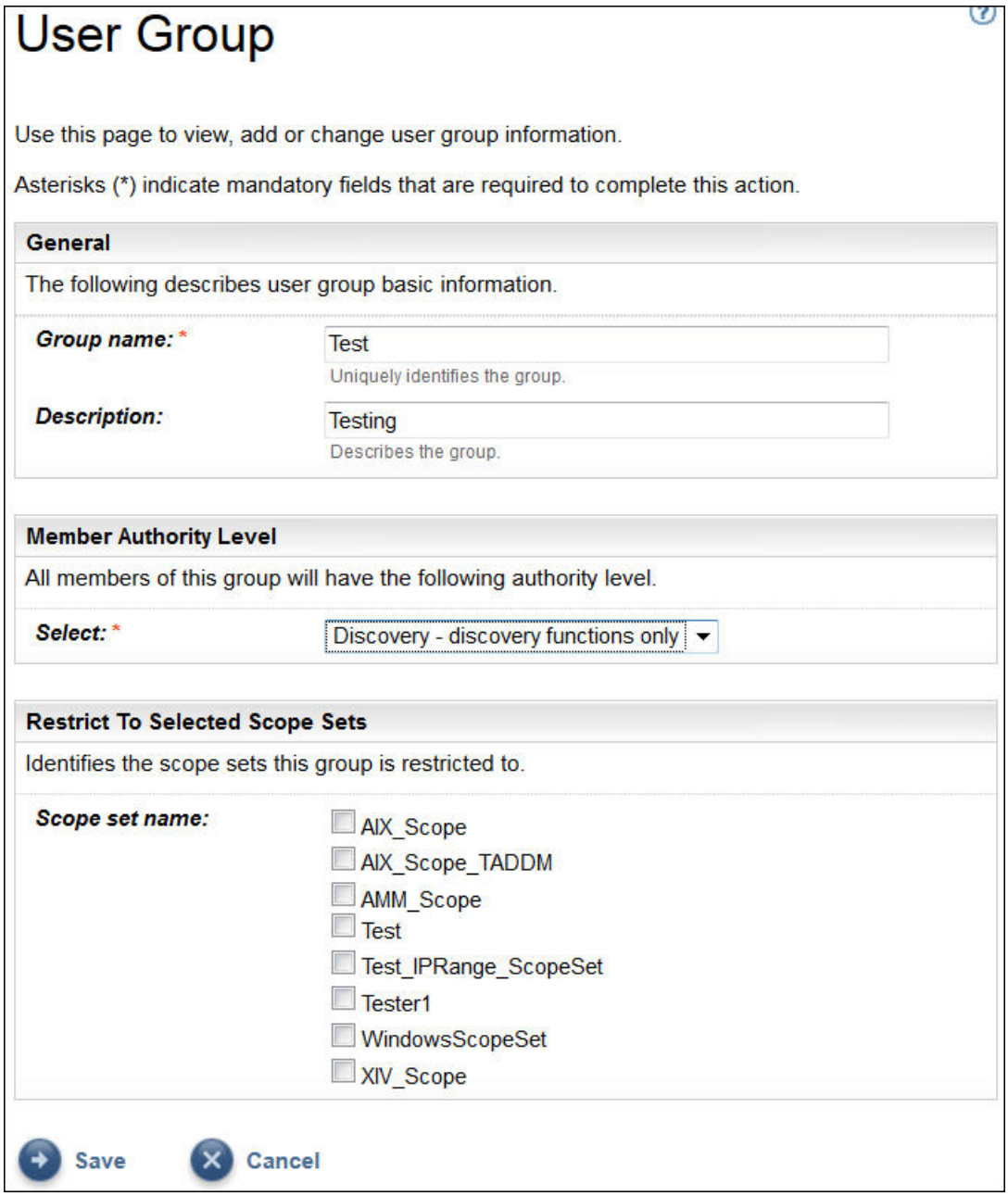

Figura 103. Incluir grupo de usuários

4. No campo **Nome do grupo**, insira um nome exclusivo para esse grupo de usuários.
5. Opcional: No campo **Descrição**, insira uma descrição para esse grupo de usuários.
6. Selecione o nível de autoridade que deseja que os membros desse grupo de usuários tenham.

   O TSA define os seguintes níveis de autoridade de grupo:

   - **Administrador** – sem restrições
   - **Descoberta** – somente funções de descoberta
   - **Visitante** – somente acesso de leitura
7. Se você especificar o nível de autoridade *Discovery* para esse grupo de usuários, deverá selecionar pelo menos um conjunto de escopos restrito a esse grupo de usuários.

   Para obter mais informações sobre os conjuntos de escopo, consulte "Escopos de descoberta e conjuntos de escopos" na página 2.
8. Clique em **Salvar** para salvar o grupo de usuários.

A página **Contas e grupos de usuários** é exibida com o novo grupo de usuários na lista.

Incluindo uma conta de usuário

É possível incluir contas de usuários para controlar o acesso às funções do TSA.

Sobre Esta Tarefa

Para incluir uma conta de usuário, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.
   A página **Contas e grupos de usuários** é exibida.

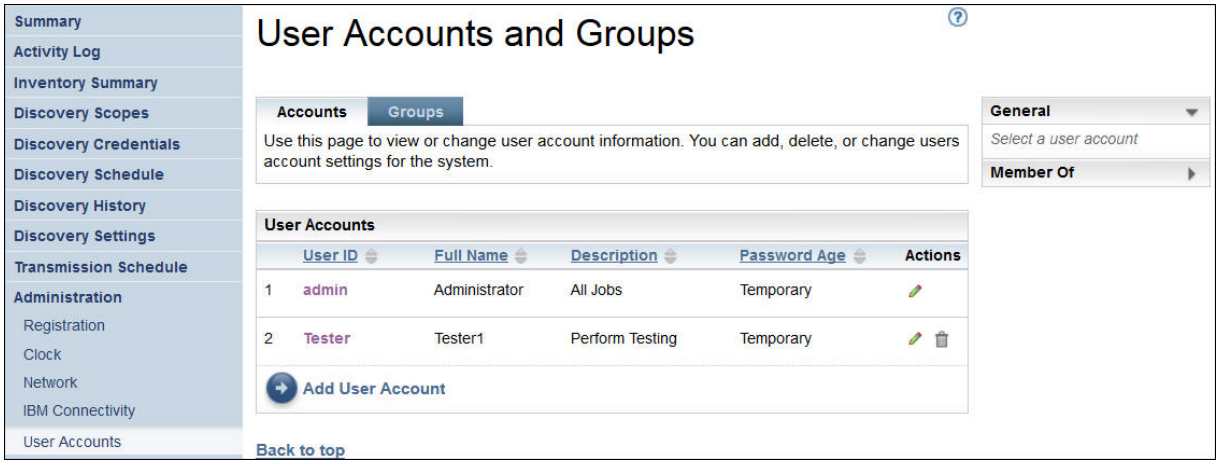

Figura 104. Contas e grupos de usuários

2. Para definir uma nova conta de usuário, clique em **Incluir conta de usuário**.
   A página **Conta do usuário** é exibida.

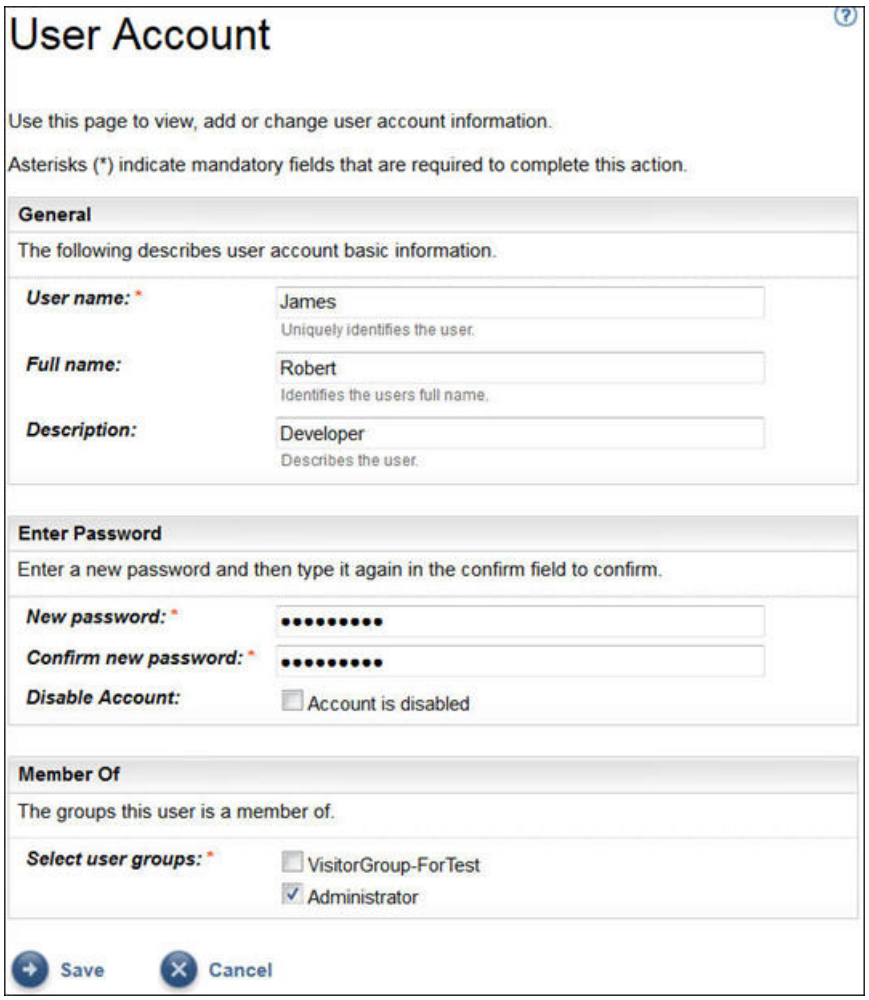

Figura 105. Incluir conta de usuário

3. No campo **Nome do usuário**, insira um nome para essa conta do usuário.
4. Opcional: No campo **Nome completo**, insira um nome completo para o usuário dessa conta.
5. Opcional: No campo **Descrição**, insira uma descrição para essa conta do usuário.
6. No campo **Nova senha**, insira novamente a senha para essa conta do usuário.

   A senha deve obedecer às seguintes regras:

   - Deve ter pelo menos oito caracteres
   - Deve conter pelo menos um caractere alfabético e um não alfabético
   - Não deve conter o nome do usuário
   - Não deve ser igual a nenhuma das oito últimas senhas
   - Deve ser mudado pelo menos uma vez a cada 30 dias (por padrão) ou conforme especificado na seção “Modificando a duração da senha” na página 104, mas não deve ser mudado mais de uma vez por dia.
7. No campo **Confirmar senha**, insira novamente a senha para essa conta do usuário.

   As duas senhas inseridas são comparadas para confirmar se são correspondentes antes que a senha seja salva.

   Nota: A senha deve ser alterada no primeiro login nessa conta do usuário.
8. Se você desejar desativar essa conta do usuário, marque a caixa de seleção **A conta está desativada**.

   A desativação da conta permite evitar que ela seja usada sem exclui-la.

Nota: Não é possível desativar a conta do **administrador** nem mudar o grupo da conta **administrativa**.

9. Selecione os grupos de usuário dessa conta do usuário. Pelo menos um grupo de usuários deve ser selecionado. O usuário terá o nível de autoridade definido para os grupos que você selecionar.
10. Clique em **Salvar** para salvar a conta do usuário.

    A página **Contas e grupos de usuários** é exibida com a nova conta do usuário na lista.

Modificando contas do usuário e grupos de usuários

É possível modificar as contas do usuário e os grupos de usuários existentes.

Modificando contas do usuário

É possível modificar contas do usuário existentes.

Sobre Esta Tarefa

Para modificar uma conta do usuário, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.

   A página **Contas e grupos de usuários** é exibida.
2. Clique na guia **Contas** e, em seguida, clique no ícone **Editar** ( ) ao lado da conta do usuário.

   A página **Conta do usuário** é exibida.
3. Na área de janela **Geral**, é possível mudar as informações básicas para essa conta do usuário.
4. Na área de janela **Inserir senha**, é possível mudar a senha e as informações de administração de senha. Também é possível desativar esta conta do usuário.

   A senha deve obedecer às seguintes regras:

   - Deve ter pelo menos oito caracteres
   - Deve conter pelo menos um caractere alfabético e um não alfabético
   - Não deve conter o nome do usuário
   - Não deve ser igual a nenhuma das oito últimas senhas
   - Deve ser mudada pelo menos a cada 90 dias, mas não deve ser mudada mais de uma vez por dia.

   Nota: A senha deve ser alterada no primeiro login nessa conta do usuário.
5. Se desejar desativar essa conta do usuário, selecione **A conta está desativada**.

   A desativação da conta permite evitar que ela seja usada sem exclui-la. Para obter informações sobre como excluir uma conta do usuário, consulte “Excluindo contas do usuário e grupos de usuários” na página 138.

   Nota: Não é possível desativar a conta do **administrador** nem mudar o grupo da conta **administrativa**.

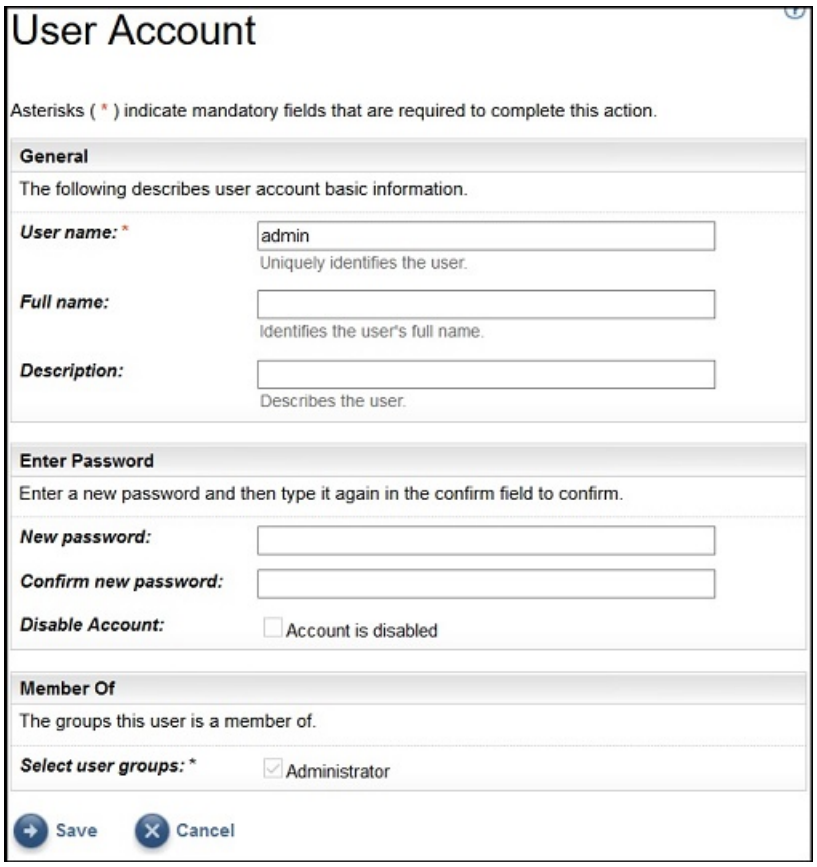

Figura 106. Modificar a conta do usuário administrativo

6. Na área de janela **Membro de**, é possível mudar os grupos de usuários aos quais essa conta do usuário pertence. A conta do usuário deve ser membro de pelo menos um grupo de usuários:
7. Clique em **Salvar** para salvar as mudanças.
   As informações mudadas são exibidas na página **Contas e grupos do usuário**.

Modificando grupos de usuários

É possível modificar os grupos de usuários existentes.

Antes de Iniciar

Nota: Não é possível mudar o grupo de **Administradores**.

Sobre Esta Tarefa

Para modificar um grupo de usuários, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.
   A página **Contas e grupos de usuários** é exibida.
2. Clique na guia **Grupos** e, em seguida, clique no ícone **Editar** ( ) ao lado do grupo de usuários.
   A página **Grupo de usuários** é exibida.
3. Na área de janela **Geral**, é possível mudar as informações básicas para esse grupo de usuários.
4. Na área de janela **Nível de autoridade do membro**, é possível mudar se esse grupo de usuários tem a autoridade *Administrator*, *Discovery* ou *Read*.

5. Se você especificou o nível de autoridade *Discovery* no **Nível de autoridade do membro**, será possível mudar os conjuntos de escopos sobre os quais esse grupo de usuários tem autoridade para descobrir na área de janela Restringir aos conjuntos de escopos selecionados.
6. Clique em **Salvar** para salvar as mudanças.

   As informações mudadas são exibidas na página **Contas e grupos do usuário**.

Excluindo contas do usuário e grupos de usuários

É possível excluir contas do usuário e grupos de usuários existentes.

Excluindo contas do usuário

É possível excluir contas do usuário existentes.

Sobre Esta Tarefa

Nota: Não é possível excluir a conta do usuário **administrativo**.

Para excluir uma conta do usuário, siga estas etapas:

Procedimento

1. Na área de janela de navegação, clique em **Administração** > **Contas de usuário**.

   A página **Contas e grupos de usuários** é exibida.
2. Clique na guia **Contas** e, em seguida, clique no ícone **Excluir** ( ) próximo à conta do usuário que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir a conta do usuário.

Excluindo grupos de usuários

É possível excluir grupos de usuários existentes.

Sobre Esta Tarefa

Nota: Não é possível excluir o grupo de usuários **administrativos**.

Para excluir um grupo de usuários, siga estas etapas:

Procedimento

1. Clique em **Administração** > **Contas do usuário**.

   A página **Contas e grupos de usuários** é exibida.
2. Clique na guia **Grupos** e, em seguida, clique no ícone **Excluir** ( ) próximo à conta do usuário que você deseja excluir.
3. Clique em **OK** para confirmar que você deseja excluir o grupo de usuários.

   Nota: Um grupo de usuários poderá ser excluído somente se não houver usuários designados a ele.

Acessibilidade

O Technical Support Appliance não interfere nos recursos de acessibilidade dos navegadores suportados. Para obter uma lista abrangente dos recursos de acessibilidade, visite a página de suporte à acessibilidade do navegador suportado que você está usando. Para obter uma lista dos navegadores suportados, consulte “Navegadores da web obrigatórios” na página 5.

As publicações deste produto estão em Adobe Portable Document Format (PDF) e devem estar em conformidade com os padrões de acessibilidade. Se você tiver dificuldades para usar os arquivos PDF e desejar solicitar um formato baseado na web para uma publicação, envie uma solicitação por e-mail para o seguinte endereço:

icfeedbk@us.ibm.com

Ou, você pode enviar uma solicitação para o seguinte endereço:

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

Na solicitação, certifique-se de incluir o título da publicação, "Guia de configuração do IBM Technical Support Appliance" no tópico do assunto da sua nota.

Quando o Cliente envia informações à IBM, o Cliente concede à IBM um direito não exclusivo de usar ou distribuir as informações da maneira que a IBM julgar apropriada, sem incorrer em nenhuma obrigação para com o Cliente.

Avisos

Essas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA.

A IBM pode não oferecer os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte o seu representante IBM local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um produto, programa ou serviço IBM não pretende declarar ou implicar que apenas esse produto, programa ou serviço IBM poderá ser usado. Será possível usar qualquer produto, programa ou serviço equivalente funcionalmente que não viole nenhum direito de propriedade intelectual da IBM. No entanto, é responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa ou serviço não IBM.

A IBM pode ter patentes ou aplicativos de patente pendentes que cobrem o assunto descrito neste documento. O fornecimento deste documento não concede nenhuma licença a essas patentes. Você pode enviar consultas sobre licença, por escrito, para:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EUA.

Para consultas sobre licença sobre informações de byte duplo (DBCS), contate o departamento de propriedade intelectual da IBM em seu país ou envie perguntas, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japão

O parágrafo a seguir não se aplica ao Reino Unido ou qualquer outro país onde essas disposições sejam inconsistentes com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE QUALQUER TIPO, EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, A COMERCIALIZAÇÃO OU A ADEQUAÇÃO A UMA PARTICULARIDADE. Alguns estados não permitem a isenção de garantias explícitas ou implícitas em determinadas transações; portanto, esta declaração pode não se aplicar a você.

Essas informações podem incluir imprecisões técnicas ou erros tipográficos. Periodicamente são feitas mudanças nas informações aqui contidas; essas mudanças serão incorporadas em novas edições da publicação. A IBM pode fazer melhorias e/ou mudanças no(s) produto(s) e/ou no(s) programa(s) descrito(s) nesta publicação a qualquer momento, sem aviso prévio.

Quaisquer referências nestas informações a sites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses sites. Os materiais contidos nesses sites não fazem parte dos materiais deste produto IBM e o uso desses sites é por conta e risco do Cliente.

A IBM pode usar ou distribuir qualquer informação fornecida de qualquer maneira considerada apropriada sem incorrer em qualquer obrigação para com o Cliente.

Quaisquer dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido feitas em sistemas de nível de desenvolvimento e não há garantia de que essas medidas serão as mesmas em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações sobre produtos não IBM foram obtidas dos fornecedores desses produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a precisão do desempenho, compatibilidade ou quaisquer outras reivindicações relacionadas a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas aos fornecedores desses produtos.

Todas as declarações relacionadas às direções ou intenções futuras da IBM estão sujeitas a mudanças ou retirada sem aviso prévio e representam apenas metas e objetivos.

Essas informações são apenas para fins de planejamento. As informações aqui contidas estão sujeitas a mudanças antes que os produtos descritos estejam disponíveis.

Marcas registradas

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corp., registradas em muitas jurisdições no mundo inteiro. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual das marcas registradas da IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Linux é a marca registrada da Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Hyper-V e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java™ e todas as marcas registradas e logotipos baseados em Java são marcas comerciais ou registradas da Oracle e/ou de suas afiliadas.

VMware, o logotipo VMware, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server e VMware vSphere são marcas registradas ou marcas comerciais da VMware, Inc. ou suas subsidiárias nos Estados Unidos e/ou em outras jurisdições.

Número da Peça:

(1P) P/N: