IBM® Technical Support Appliance Guia do Assistente de Configuração

Versão 2.8.0.0

Janeiro de 2021

Índice

Introdução

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

O objetivo deste documento é fornecer informações e orientações para ajudar na instalação, no planejamento e na configuração do TSA.

Considerações sobre pré-descoberta de rede

Antes de configurar o TSA para a descoberta e transmissão iniciais, verifique se os itens a seguir foram abordados. Supõe-se que o TSA já tenha sido instalado, a interface da Web esteja acessível e o TSA tenha sido atualizado para o nível mais atual. Caso contrário, consulte o Guia de Instalação do Dispositivo de Suporte Técnico (referido como Guia de configuração no restante deste documento).

Considerações sobre pré-descoberta de rede do TSA	
Rede	
	Abra o acesso ao firewall do TSA para a IBM. Veja a seção **Requisitos de configuração para conexões com o Suporte IBM** no Guia de configuração.
	Se um proxy SSL for usado para conectar de volta à IBM, assegure-se de que ele esteja configurado no TSA. Veja a seção **Configurando a conectividade IBM** no Guia de configuração. A Inspeção SSL não é suportada. Se utilizar a inspeção SSL no proxy, desative-a para esses fluxos.
	Se existir algum firewall entre o TSA e os dispositivos de destino, assegure-se de que as portas necessárias estejam abertas. Para obter mais informações, consulte a seção "Considerações sobre firewall" na página 42.

Documentação útil

O link abaixo o apontará diretamente para o website de informações do Technical Support Appliance. Aqui, você encontrará tudo o que é necessário para começar a usar o IBM Technical Support Appliance. É possível acessar guias de configuração e documentação de segurança, visualizar relatórios de amostra e fazer download do código de instalação do Technical Support Appliance em ibm.com.

Para saber mais sobre o Technical Support Appliance: https://ibm.biz/TSAdemo

Visão geral

O TSA coleta informações de descoberta sobre sua infraestrutura de TI, que inclui componentes de Sistema Operacional implementados, componentes de firmware, servidores físicos, dispositivos de rede, LAN virtual etc. Para otimizar a amplitude e a profundidade das informações coletadas, são necessárias tarefas de configuração dentro do TSA para identificar os dispositivos de descoberta.

O TSA tenta minimizar os impactos no ambiente de rede do cliente. Assim, o processo de descoberta usa uma abordagem iterativa e medida que pode fazer com que uma descoberta completa demore até 72 horas. O status da tarefa de descoberta pode ser monitorado visualizando a seção **Resumo do trabalho** do painel de **Resumo**.

Como parte do processo de descoberta, o TSA tenta inicialmente detectar dispositivos dentro do escopo definido sem usar credenciais. Isso envolve o uso do Nmap para descobrir e classificar dispositivos por meio de varredura IP intrusiva baixa, da impressão digital da pilha e do mapeamento de porta. Geralmente, essa atividade não deve ser significativa o bastante para acionar um sistema de detecção de intrusão (IDS), porém pode ocorrer se houver configurações locais rigorosas.

Para que o TSA colete informações sobre sua infraestrutura de TI, forneça o seguinte:

- Escopos
- Credenciais de acesso

Definindo conjunto de escopos

Um conjunto de escopos é um agrupamento lógico de escopos individuais. Os escopos usam endereços IP para informar ao TSA onde começar a descobrir o ambiente. Um conjunto de escopos é composto por um ou mais escopos. Há três tipos de entradas de escopos:

- Sub-rede - Definida por um endereço IP e uma máscara de sub-rede. As sub-redes são limitadas às sub-redes da classe C.
- Intervalo de IP - Inclui todos os endereços IP entre o início e o término.
- Endereço IP/Host - Um endereço IP individual ou nome do host.

> O nome do host é resolvido na hora da entrada e não na hora da descoberta. Consulte a seção "Fatores a serem considerados ao criar escopos," na página 6 para obter detalhes.

Se desejar, as exclusões de escopo poderão ser definidas para um escopo especificando uma definição de host, intervalo ou sub-rede. Os endereços IP resultantes não serão considerados parte do escopo e não serão digitalizados.

O TSA suporta três tipos de conjuntos de escopos:

1. **Conjuntos de escopos gerais**: permite descobrir elementos de rede de TI individuais. O conjunto de escopos contém um ou mais escopos que identificam o local desses elementos de rede usando um endereço IP, um intervalo de endereços IP ou uma rede ou subconjunto.
2. **Conjuntos de escopos dinâmicos do HMC**: permite especificar o endereço IP de um ou mais HMCs do IBM POWER Systems juntamente com as credenciais associadas. Além disso, as informações relativas a todas as LPARs que os HMCs gerenciam também podem ser coletadas sem a necessidade de identificar os endereços IP para as LPARs. O conjunto de escopos dinâmicos usa as informações de credencial que você fornece para acessar essas LPARs com sucesso.
3. **Conjuntos de escopos dinâmicos do VMware**: permite especificar o endereço IP de uma ou mais instâncias do VMware vCenter Server ou do ESXi juntamente com suas credenciais associadas. Além disso, as informações relativas a todas as máquinas virtuais que o VMware gerencia também podem ser coletadas sem a necessidade de identificar os endereços IP para as máquinas virtuais. O conjunto de escopo dinâmico usa as informações de credencial que você fornece para acessar essas máquinas virtuais com sucesso.

Para HMCs e VMware vCenter Servers/ESXi, é recomendado o uso de conjuntos de escopos dinâmicos. 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, para ambientes nos quais as LPARs ou máquinas virtuais são incluídas e excluídas ao longo do tempo, os conjuntos de escopos dinâmicos podem manipular isso sem a necessidade de modificar nenhum conjunto de escopos.

Para obter instruções detalhadas sobre como definir escopos de descoberta no TSA, consulte a seção **Configurando escopos de descoberta** no Guia de configuração.

Fatores a serem considerados ao criar escopos

Embora não haja nenhum padrão definido para configurar escopos, há algumas considerações práticas que podem economizar tempo e esforço:

- Sempre que possível, use conjuntos de escopos dinâmicos para definir descobertas de HMCs e suas LPARs gerenciadas, ou VMware vCenter Server/ESXi e suas máquinas virtuais gerenciadas. Quando conjuntos de escopos dinâmicos são usados, não há nenhuma necessidade de definir escopos para as LPARs ou máquinas virtuais.
- Os Conjuntos de escopos dinâmicos do HMC permitem a importação de um ou mais endereços IP/nomes de host para os HMCs que você deseja descobrir. Para obter mais informações, veja a seção **Conjuntos de escopos dinâmicos do HMC** no Guia de configuração.
- Os Conjuntos de escopos dinâmicos do VMware permitem a importação de um ou mais endereços IP/nomes de host para as instâncias do VMware vCenter Servers e

ESXi que você deseja descobrir. Para obter mais informações, veja a seção **Escopos dinâmicos do VMware** no Guia de configuração.

- Use escopos de intervalo de IP ou sub-rede para descobrir vários dispositivos, em vez de endereços IP individuais ou nomes de host. Isso limitará o número de definições de escopo e facilitará a administração.
- Se estiver usando definições de escopo de sub-rede, inclua apenas uma por conjunto de escopo. Verifique se a definição do escopo da sub-rede oferece uma resolução para uma rede Classe C (256 endereços IP) ou menos.
- Use o recurso **Importar conjunto de escopos gerais** para criar um novo conjunto de escopos baseado no nome especificado e na lista dos endereços IP de um arquivo de texto de entrada. Para obter mais informações, veja a seção **Escopos de descoberta → Importar conjunto de escopos gerais** no Guia de configuração para obter instruções.
- O TSA resolve os nomes de host uma vez na hora de entrada. Se o endereço IP de um sistema mudar, mantendo o mesmo nome de host, o escopo desse sistema deverá ser excluído e recriado para resolver para o novo endereço IP.
- Quanto mais endereços IP estiverem no conjunto de escopos, mais longa será a descoberta. Para minimizar o tempo que uma descoberta leva, configure os escopos para focar apenas nos elementos que você deseja descobrir.

Ao usar os Conjuntos de Escopos Gerais, limite o número acumulativo de endereços IP que um conjunto de escopos resolve (após expandir quaisquer definições de escopo de intervalo ou sub-rede) a 400 ou menos. Problemas de desempenho, servidor ou rede poderão ser encontrados durante o processo de descoberta se mais de 400 endereços IP forem varridos para um único conjunto de escopos. Exibir o conjunto de escopos mostrará quantos endereços IP um determinado conjunto de escopos tentará descobrir.

- O TSA não impede que os endereços IP sejam definidos em vários conjuntos de escopos. Em geral, essa prática deve ser evitada, pois aumenta o tempo de descoberta sem coletar informações adicionais.
- Agrupar escopos em conjuntos de escopos que formam um agrupamento lógico de dispositivos:
  - Agrupar o mesmo tipo de dispositivo em um conjunto de escopos. Por exemplo, crie um conjunto de escopos para subsistemas de armazenamento IBM FlashSystem.
  - Agrupar dispositivos que estão na mesma geografia.

- Agrupar dispositivos com base em aplicativos de trabalho ou serviços.

Credenciais de descoberta

Com algumas exceções, as descobertas requerem algum nível de acesso para adquirir as informações detalhadas necessárias para um entendimento completo de seu ambiente.

Normalmente, as contas de serviço devem ser criadas nos dispositivos de descoberta para serem usadas pelo TSA. Consulte as seções a seguir para obter os direitos de acesso específicos requeridos por cada tipo de plataforma. Para simplificar a administração dessas contas de serviço, use o mesmo nome de usuário para todos os dispositivos de uma determinada família de produtos.

A tarefa de manter as contas de serviço que o TSA usa para conectar-se aos dispositivos pode ser simplificada usando uma das seguintes estratégias:

- Criar contas de serviço com senhas que não expiram
- Usar chaves SSH para famílias de produtos de dispositivos que suportam seu uso

Para obter instruções detalhadas sobre como definir as credenciais de acesso no dispositivo, veja a seção **Configurando credenciais de descoberta** no Guia de configuração.

Fatores a serem considerados ao configurar Credenciais de Descoberta

O dispositivo tenta usar credenciais na ordem em que aparecem na lista de acesso. Para acelerar a descoberta, verifique se você tem as credenciais na ordem que melhor se adéqua ao seu ambiente. Algumas considerações são as seguintes:

- Restringir as credenciais para especificar os conjuntos de escopos onde for apropriado. Isso limitará as tentativas de login desnecessárias e melhorará o desempenho de descoberta.
- As chaves SSH podem ser usadas para essas descobertas de dispositivos:
  - AIX
  - Ponto de verificação
  - Cisco
  - Dell iDRAC
  - F5 Big IP
  - Fortinet
  - HMC
  - HP-UX
  - IBM FlashSystem

- IBM i
- IVM
- Linux
- Sun SPARC (Solaris)
- SVC / V7000
- VIOS

Apenas uma credencial de chave SSH pode ser vinculada a um conjunto de escopos.

- É a melhor prática para criar contas de serviços separadas que são usadas exclusivamente pelo TSA com o menor nível de autoridade necessário.

Introdução

Esta seção abrange algumas melhores práticas e recomendações para configurar o TSA.

Instalação e configuração inicial do TSA

Acesse as instruções especificadas nas seções a seguir do Guia de configuração:

- Instalando o Technical Support Appliance
- Efetuando login no Technical Support Appliance
- Aceitando o Contrato de Licença
- Configurando o Technical Support Appliance usando o assistente de configuração

Preparando para descobertas

Um processo interativo é recomendado, pelo qual uma pequena parte da rede é inicialmente configurada para descoberta e mais seções da rede são incluídas em cada iteração até que toda a rede desejada seja coberta.

É uma melhor prática salvar um backup de sua configuração do TSA após inclusões/modificações significativas feitas nos escopos e/ou nas credenciais. Para obter mais informações, consulte a seção "Backup e restauração" no Guia de Configuração do IBM Technical Support Appliance.

Etapas de descoberta

Para cada iteração de descoberta execute as seguintes etapas:

1. Prepare os dispositivos para descoberta. Para qualquer dispositivo e requisitos de configuração de credencial necessários, consulte a seção "Configuração de Descoberta de Dispositivo" na página 12.
2. Para Conjuntos de Escopos Dinâmicos do HMC, execute as seguintes etapas:
   a. Inclua os endereços IP dos HMCs na página **Conjuntos de escopos dinâmicos do HMC**.
   b. Inclua as credenciais para os HMCs na página **Conjuntos de escopos dinâmicos do HMC**.
   c. Selecione quais tipos de LPAR você deseja descobrir. Forneça as credenciais para cada tipo.

      Você pode selecionar os tipos de LPAR para descobrir quando o conjunto de escopos dinâmicos foi criado ou pode incluir os tipos de LPAR em uma iteração posterior editando o conjunto de escopos dinâmicos.

d. (Opcional) Use a função Testar na página **Conjunto de escopos dinâmicos do HMC** para verificar se as credenciais estão definidas corretamente e podem ser usadas para estabelecer uma conexão com os HMCs ou suas LPARs.

3. Para Conjuntos de Escopos Dinâmicos do HMC, execute as seguintes etapas:

   a. Inclua os endereços IP dos VMware vCenter Servers.

   b. Inclua os endereços IP de quaisquer hosts VMware ESXi que não sejam gerenciados por um VMware vCenter Server.

   c. Inclua as credenciais para as instâncias de VMware vCenter Servers e ESXi na página **Conjunto de escopos dinâmicos do VMware**.

   d. Selecione quais tipos de máquina virtual você deseja descobrir. Forneça as credenciais para cada tipo.

   > Você pode selecionar os tipos de máquina virtual a serem descobertos quando o conjunto de escopos dinâmicos é criado ou pode incluir os tipos de máquina virtual em uma iteração posterior editando o conjunto de escopos dinâmicos.

   e. (Opcional) Use a função Testar na página **Conjunto de escopos dinâmicos do VMware** para verificar se as credenciais estão definidas corretamente e podem ser usadas para estabelecer uma conexão com as instâncias de VMware vCenter Servers e ESXi, bem como suas máquinas virtuais.

4. Para Escopos Gerais de Descoberta, execute as seguintes etapas:

   a. Inclua os endereços IP desejados nos escopos/conjuntos de escopos adequados. Se existirem firewalls entre a instância do TSA e os dispositivos de descoberta, verifique se as portas adequadas estão abertas no firewall para permitir que a descoberta seja bem-sucedida Para obter informações sobre quais portas devem estar acessíveis para cada tipo de plataforma, consulte a seção "Considerações de firewall" na página 42.

   b. Crie as credenciais necessárias.

   c. (Opcional) Use a função Teste no painel **Novo Descoberta Credenciais** para verificar se a credencial está definida corretamente e se pode ser usada para estabelecer uma conexão com um dispositivo de destino.

5. Execute uma descoberta completa para varrer os endereços IP incluídos para essa iteração.

6. Execute uma transmissão para fazer upload dos dados para a IBM.

Configuração de descoberta do dispositivo

Além de fornecer credenciais, pode haver pré-requisitos específicos de configuração do dispositivo de descoberta necessários para que o TSA descubra e colete efetivamente informações úteis sobre o componente. Esta seção permite identificar dispositivos de descoberta em seu ambiente que exigirão configurações específicas. Recomenda-se a criação de contas de serviço com as autoridades mínimas necessárias. Consulte também a seção "Considerações sobre firewall" para obter informações de porta e protocolo.

- Para dispositivos para os quais ambas as portas SSH e Telnet estão abertas, o TSA primeiro tentará uma conexão usando SSH (por motivos de segurança). Se essa conexão do SSH falhar, o TSA tentará a conexão usando Telnet.

Sistemas operacionais e hosts

Plataforma
IBM Power Systems • Hardware Management Console (HMC) • Integrated Virtualization Manager (IVM) • Partições do Servidor de E/S Virtual (VIOS) • AIX • Linux on Power
IBM i
UNIX Systems • Solaris • Solaris via iLOM • Linux • HP-UX
VMware vCenter Server e VMware ESXi
Windows
Dispositivos ATM

Módulo de gerenciamento
• Flex System Manager (FSM) • Chassis Management Module (CMM) • Advanced Management Module (AMM) • HP ProLiant Blade Server via HP OnBoard Administrator • Integrated Management Module (IMM e IMM2) • HP Integrity & HP9000 Servers via iLO • Dell Server via Integrated Dell Remote Access Controller (iDRAC)
Clique em cada um dos links acima para obter informações detalhadas.

IBM Power Systems

Para sistemas IBM Power, em que a configuração de LPARs é gerenciada por um HMC ou IVM, use Conjuntos de Escopos Dinâmicos do HMC. Com os Conjuntos de Escopos Dinâmicos do HMC, você cria uma definição de escopo para os HMCs e fornece as credenciais do HMC e LPAR associadas, porém não precisa criar escopos para cada LPAR gerenciada. Quando o HMC é descoberto, o TSA determina quais LPARs existem naquele momento e varre automaticamente cada LPAR.

Para IBM Power Systems em que a configuração de LPARs geralmente é estática, um método alternativo para Conjuntos de Escopos Dinâmicos do HMC é iterar incluindo escopos e credenciais para entidades na seguinte ordem:

1. **As instâncias do HMC ou do IVM**: o HMC retorna informações de alto nível sobre todos os Power Systems que ele gerencia e as partições lógicas ali contidas. O IVM retorna informações semelhantes para o sistema único que ele gerencia.
2. **As partições VIOS**: isso retorna informações sobre os adaptadores físicos e os recursos que pertencem a essas partições.
3. **Partições individuais**: em alguns casos, uma partição não VIOS possui adaptadores físicos.

Hardware Management Console (HMC)

Para descobrir instâncias do HMC, conclua as etapas a seguir:

Preparando o ambiente:

- Para que o TSA reúna informações sobre o gerenciamento de LPARs por meio do HMC, o HMC deve ser capaz de se comunicar com os LPARs usando as ferramentas de RMC. Assegure-se de que o HMC e os LPARs estejam configurados para permitir essa comunicação. Para obter mais informações sobre as ferramentas RMC para Linux, consulte https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html
- Para ativar a coleta de dados segura, a execução de comando remoto deve ser ativada no HMC. Para obter informações, consulte "Ativando e desativando comandos remotos do HMC" no seguinte endereço: https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

Credenciais para lista de acesso:

- Para Conjuntos de Escopos Dinâmicos do HMC - Nome do usuário/senha ou Nome do usuário/autenticação de chave SSH para a conta de serviço do HMC.
- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta de serviço do HMC.
- O usuário do HMC deve ter as seguintes funções:
  - Função do recurso: AllSystemResources
  - Função da tarefa (com base no **hmcoperator** com tarefas da linha de comandos):
    - ManagedSystem (lshwres, lssyscfg)
    - Partição lógica (lshwres, lssyscfg, viosvrcmd)
    - Configuração HMC (lshmc)
- Um usuário (conta de serviço) com autoridade **hmcviewer** pode ser usado, se necessário, no entanto, isso resultará na coleta de dados parcial.

> Ao executar com autoridade **hmcviewer**, não será possível obter informações sobre os adaptadores pertencentes às partições VIOS. Para obter essas informações, assegure-se de que a conta do serviço tenha no mínimo a autoridade **hmcoperator**. Se isso não for possível, inclua escopos e credenciais para descobrir partições VIOS diretamente, além do HMC.

Integrated Virtualization Manager (IVM)

Para descobrir instâncias do IVM, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço IVM.
- A conta do serviço deve ter permissão somente para visualização.

Partições do Servidor de E/S Virtual (VIOS)

Para descobrir instâncias do VIOS, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Para Conjuntos de Escopos Dinâmicos do HMC - Nome do usuário/senha ou Nome do usuário/autenticação de chave SSH para a conta de serviço de partição do VIOS.
- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta de serviço de partição do VIOS.
- A conta de serviço deve ser uma conta de administrador (como **padmin**).
- A conta de serviço deve ter um atributo de usuário de **rlogin=true**. É possível configurar esse atributo usando SMIT ou editando o arquivo **/etc/security/user**.
- O parâmetro **PermitUserEnvironment** no arquivo **/etc/ssh/sshd_config** deve ser configurado como **yes**.

AIX

Para descobrir instâncias do AIX, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que os pacotes bos.perf.tools e openSSH/openSSL estejam instalados.
- Desative a falha de tentativa de login inválido para a conta do serviço.

Credenciais para lista de acesso:

- Para Conjuntos de Escopos Dinâmicos do HMC - Nome do usuário/senha ou Nome do usuário/autenticação de chave SSH para a conta de serviço de partição do AIX.

- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta de serviço do AIX.
- A conta do serviço pode ser raiz ou uma conta com autoridade sudo.
- A conta de serviço deve ter um atributo de usuário de **rlogin=true**. É possível configurar esse atributo usando SMIT ou editando o arquivo **/etc/security/user**.
- Para ativar uma conta do serviço não raiz para autoridade sudo para AIX:
  - Instale o RPM sudo (sudo-1.6.9p15-2noldap) e os conjuntos de arquivos ssh (openssh.base.server, openssh.base.client na instância do AIX).
  - Crie um ID do usuário não raiz na instância do AIX de destino que possa ser usado pelo TSA para acessar o sistema.
  - Modifique **/etc/sudoers** em cada instância do AIX para permitir que o TSA execute os comandos especificados usando a autoridade sudo.

    # Especificação do alias Cmnd

    ```
    Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no,
    /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo,
    /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo,
    /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
    /usr/bin/sissasraidmgr, /usr/sbin/lswpar,
    /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso,
    /usr/sbin/bosdebug, /usr/sbin/chedition,
    /usr/esa/bin/esacli, /usr/sbin/bootinfo,
    /usr/bin/mpio_get_config, /usr/bin/cat
    /etc/objrepos/CuData,
    /usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat
    /var/adm/ras/bootlog, /usr/bin/cat
    /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
    /usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr
    view, /usr/sbin/powermt version, /usr/sbin/powermt display,
    /usr/bin/pcmpath query, /usr/sbin/datapath query
    ```

    # Especificação de privilégio de usuário

    ```
    <Nome do usuário> ALL = NOPASSWD: TSA_CMDS
    ```

    - <Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do AIX. Esse <Nome do usuário> é um usuário em cada instância do AIX. O arquivo **/etc/sudoers** em cada instância do AIX deve ser atualizado com a especificação acima.

    Ou

    Uma alternativa para a modificação acima para **/etc/sudoers** é usar a especificação de privilégio de usuário a seguir:

    ```
    <Nome do usuário> ALL = NOPASSWD: ALL
    ```

> <Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do AIX. Essa especificação do usuário permite que a conta do serviço use a autoridade sudo em um comando do AIX.

Linux on Power

Para descobrir instâncias do Linux on Power, conclua as seguintes etapas:

Preparando o ambiente:

- Desative a falha de tentativa de login inválido para a conta do serviço

Credenciais para lista de acesso:

- Para Conjuntos de Escopos Dinâmicos do HMC - Nome do usuário/senha ou Nome do usuário/autenticação de chave SSH para a conta de serviço de partição do Linux.
- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta de serviço do Linux.
- Para ativar uma conta do serviço não raiz para autoridade sudo para Linux:
  - Crie um ID do usuário não raiz na instância do Linux de destino real que possa ser usado pelo TSA para acessar o sistema.
  - Modifique **/etc/sudoers** em cada instância do Linux para permitir que o TSA execute os comandos especificados usando a autoridade sudo.

    # Especificação do alias Cmnd

    ```
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,
    /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,
    /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,
    /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
    /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*,
    /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,
    /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-
    bound, /bin/cat /proc/sys/kernel/random/entropy_avail
    ```

    # Especificação de privilégio de usuário

    ```
    <Nome do usuário> ALL = NOPASSWD: TSA_CMDS
    ```

    > <Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do Linux. Esse <Nome do usuário> é um usuário em cada instância do Linux. O arquivo **/etc/sudoers** em cada instância do Linux deve ser atualizado com a especificação acima.

    Ou

Uma alternativa para a modificação acima para **/etc/sudoers** é usar a especificação de privilégio de usuário a seguir:

```
<Nome do usuário> ALL = NOPASSWD: ALL
```

> <Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do Linux. Essa especificação do usuário permite que a conta do serviço use a autoridade sudo em um comando do Linux.

- Se você usar o portal IBM Proweb para AIX como parte de sua oferta de suporte da IBM, é recomendável que você configure o TSA usando Conjuntos de Escopos Dinâmicos do HMC. Como alternativa, é possível configurar o TSA para descobrir os HMCs e as partições lógicas (incluindo VIOS) nos Power Systems.
- Ao varrer usando Conjuntos de Escopos Dinâmicos do HMC, você obtém informações de configuração do SO mais detalhadas para cada LPAR que podem ser recuperadas e analisadas pelo ProWeb.

> Para obter informações sobre como incluir escopos e credenciais para ambientes do HMC, consulte a seção **Escopos Dinâmicos do HMC** no Guia de Configuração do IBM Technical Support Appliance.

- Nível de dados coletados para o relatório por meio da varredura de várias entidades do Power Systems:
  - Ao varrer somente HMCs, você obterá todas as informações essenciais sobre a guia Identificado e as guias Topologia do HMC, Firmware dos Power Systems, Recomendações do IBM i, Recomendações do Linux, HMC/VIOS/AIX e Contrato, além de algumas informações do Adaptador.
  - Ao varrer partições do VIOS diretamente, você obterá informações adicionais sobre o firmware do adaptador e o armazenamento conectado.
  - Ao varrer LPARs diretamente, você obterá mais informações sobre a LPAR, incluindo detalhes e instâncias do SO de software específico como PowerHA, GPFS e PowerSC.

IBM i

Instâncias do IBM i são descobertas usando uma conexão SSH. Se a instância do IBM i não tiver o SSH instalado e configurado, conclua as seguintes etapas:

Preparando o ambiente:

Assegure-se de que os produtos/opções a seguir estejam instalados e configurados para o IBM i 7.2:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opção 30
- Portable App Solutions Environment, 5770-SS1, opção 33
- IBM Developer Kit for Java, 5770-JV1

Assegure-se de que os produtos/opções a seguir estejam instalados e configurados para o IBM i 7.3:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opção 30
- Portable App Solutions Environment, 5770-SS1, opção 33
- IBM Developer Kit for Java, 5770-JV1 opção 16
- Java SE 8 32 bit

Assegure-se de que os seguintes produtos/opções estejam instalados e configurados para o IBM i 7.4:

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, opção 30
- Portable App Solutions Environment, 5770-SS1, opção 33
- IBM Developer Kit for Java, 5770-JV1 opção 16
- Java SE 8 32 bit

Para iniciar o daemon SSH, execute o seguinte comando:

```
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))
```

Para iniciar o serviço SSHD no IBM i, execute o seguinte comando:

```
STRTCPSVR SERVER(*SSHD)
```

Para obter informações adicionais sobre como configurar o SSH no IBM i, consulte os capítulos 21-23 neste Redbook - http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode ter qualquer classe de usuário que inclua ***USER**; portanto, são necessários requisitos adicionais de autoridade de objeto para coleta de informações de PTF (que pode ser feita usando o comando **DSPPTF**).

- **DSPPTF** é enviado com as seguintes restrições de autoridade de objeto:
  - O comando é enviado com a autoridade pública ***EXCLUDE**
  - **Os perfis de usuário QPGMR**, **QSYSOPR**, **QSRV** e **QSRVBAS** são enviados com autoridades privadas para usar este comando
  - Como sempre, o perfil do usuário **QSECOFR** ou qualquer perfil do usuário com uma classe de usuário ***SECOFR** pode executar esse comando
- O objeto **QSYS/DSPPTF** do tipo de objeto ***CMD** pode ter suas autoridades editadas para permitir que qualquer outro usuário execute esse comando.
- Se uma nova conta do serviço for criada para o TSA, as seguintes recomendações serão aplicadas:
  - Crie o perfil do usuário com a classe de usuário ***USER**
  - Use o comando **GRTOBJAUT** para permitir que esse perfil do usuário execute o comando **DSPPTF**; o objeto é **QSYS/DSPPTF** do tipo de objeto ***CMD**.

Sistemas UNIX

Solaris

Para descobrir dispositivos Solaris, conclua as seguintes etapas:

Preparando o ambiente:

- Em sistemas Solaris, assegure-se de que o pacote SUNWscpu (Compatibilidade com a origem) esteja instalado.
- Em alguns sistemas Solaris, o SNEEP precisa ser instalado e configurado para obter números de série.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- A conta do serviço pode ser não raiz.

Solaris via Oracle iLOM

Para descobrir dispositivos Solaris via Oracle iLOM, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço pode ter privilégios de **Operador** ou **Administrador**.

Linux

Se a instância do Linux estiver em execução em um IBM Power System, consulte a seção Linux on Power na página 17, sob IBM Power Systems para obter instruções.

Para descobrir dispositivos Linux on x86, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que o pacote pciutils esteja instalado. O comando `lspci` ali contido é usado para coletar informações sobre adaptadores e conexões com dispositivos de armazenamento externo.

Credenciais para lista de acesso:

- Para Conjuntos de Escopos Dinâmicos do VMware - Nome do usuário/senha ou Nome do usuário/autenticação de chave SSH para a conta de serviço de máquina virtual Linux.
- Para Conjuntos de Escopos Gerais de Descoberta – Sistema computacional: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta de serviço do Linux.
- Configure `/bin/sh` como o shell para essa conta.
- Para Linux (x86), a conta de serviço pode ser raiz ou uma conta com `autoridade` sudo.
- Para descobrir como usar uma conta de serviço não raiz, inclua o seguinte no arquivo **/etc/sudoers** no sistema Linux.

```
# Especificação do alias Cmnd
    Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode

# Especificação de privilégio de usuário
    <Nome do usuário> ALL = NOPASSWD: TSA_CMDS
```

> <Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do Linux. Esse <Nome do usuário> é um usuário em cada instância do Linux. O arquivo **/etc/sudoers** em cada instância do Linux deve ser atualizado com a especificação acima.

Ou

Uma alternativa para a modificação acima para **/etc/sudoers** é usar a especificação de privilégio de usuário a seguir:

```
<Nome do usuário> ALL = NOPASSWD: ALL
```

<Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do Linux. Essa especificação do usuário permite que a conta do serviço use a autoridade sudo em um comando do Linux.

HP-UX

Para descobrir dispositivos HP-UX, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- Para ativar uma conta do serviço não raiz para autoridade sudo para HP-UX:
  - Modifique **/usr/local/etc/sudoers** em cada dispositivo HP-UX para permitir que o TSA execute os comandos especificados usando autoridade sudo.

```
# Especificação do alias Cmnd
Cmnd_Alias TSA_CMDS
=/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus

        # Especificação de privilégio de usuário
<Nome do usuário> ALL=(ALL) NOPASSWD:TSA_CMDS
```

<Nome do usuário> é a conta do serviço não raiz que o TSA usa para coletar informações do HP-UX.

VMware vCenter Server e VMware ESXi

Para ambientes do VMware, use Conjuntos de Escopos Dinâmicos do VMware. Com os Conjuntos de Escopos Dinâmicos do VMware, você cria uma definição de escopo para um VMware vCenter Server/ESXi e fornece as credenciais do VMware e da máquina virtual associadas, porém não é necessário criar escopos para cada máquina virtual gerenciada. Quando o VMware vCenter Server/ESXi é descoberto, o TSA determina quais máquinas virtuais existem naquele momento e varre automaticamente cada máquina virtual.

Para ambientes do VMware em que a configuração de máquinas virtuais geralmente é estática, um método alternativo para Conjuntos de Escopos Dinâmicos do VMware é iterar incluindo escopos e credenciais para entidades na seguinte ordem:

1. **As instâncias do vCenter Server**: isso retorna informações de alto nível sobre os hosts ESXi que elas gerenciam e os guests de máquina virtual ali contidos.
2. **Hosts ESXi**: inclua hosts ESXi que não são gerenciados por um vCenter Server.
3. **Guests de máquina virtual individual**: isso permite a coleta de informações mais detalhadas sobre o sistema operacional.

Ao configurar o TSA para ambientes do VMware, as seguintes ações são recomendadas:

1. Configure o TSA para descobrir os VMware vCenter Servers, quando disponíveis. A descoberta de um VMware vCenter Server faz com que o TSA colete automaticamente informações sobre todos os hosts do VMware ESXi que o vCenter Server gerencia. Não é necessária nenhuma informação de configuração sobre os hosts ESXi.
2. Configure o TSA para descobrir hosts do VMware ESXi apenas quando o host ESXi não é gerenciado por um VMware vCenter Server.
3. Instale as Ferramentas do VMware em cada máquina virtual que está hospedada nos hosts ESXi. Se as Ferramentas do VMware não estiverem instaladas, alguns dados de inventário como endereço IP ou Sistema Operacional instalado não estarão acessíveis.
4. Configure cada host ESXi do VMware para ter a interface do CIM ativa. A interface do CIM permite que o TSA colete informações detalhadas sobre os adaptadores dentro do host ESXi. Para obter mais informações sobre o provedor CIM, consulte o "Apêndice C" na página 44.

Para descobrir instâncias do servidor vCenter, bem como informações sobre os servidores ESXi que eles gerenciam, execute as seguintes etapas:

Preparando o ambiente

- Instale as Ferramentas do VMware em cada máquina virtual que está hospedada nos hosts ESXi.
- Configure cada host ESXi do VMware para ter a interface do CIM ativa.
- A porta do CIM (5989) deve estar acessível a partir do TSA (desbloqueada por firewalls etc.) para a descoberta completa.

Credenciais para lista de acesso

- Para Conjuntos de Escopos Dinâmicos do VMware - Nome do usuário/senha para a conta de serviço do VMware vCenter Server.
- Para Conjuntos de Escopos Gerais de Descoberta - Nome do usuário/senha para a conta de serviço do VMware vCenter Server.
- A conta de serviço deve ter permissões de função de **Administrador** ou pelo menos permissões para uma função Somente leitura customizada com os seguintes privilégios adicionais:
  - Global → Licenças
  - Global → Configurações
  - Host → CIM
  - Host → Configuração → Mudar configurações

- Host → CIM→ Interação do CIM

Para descobrir dispositivos ESXi diretamente, conclua as seguintes etapas:

Preparando o ambiente

- Instale as Ferramentas do VMware em cada máquina virtual que está hospedada nos hosts ESXi.
- Configure cada host ESXi do VMware para ter a interface do CIM ativa.

Credenciais para lista de acesso

- Para Conjuntos de Escopos Dinâmicos do VMware - Nome do usuário/senha para a conta de serviço ESXi do VMware.
- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional: nome do usuário/senha para a conta de serviço do VMware ESXi.
- A conta de serviço deve ter permissões de função de **Administrador**.

Windows

O TSA suporta a descoberta de instâncias do Windows com os seguintes métodos:

- WINRM
- SMB1


O Windows via WINRM é preferível, pois ele é a interface mais segura.

Windows via WINRM

Para descobrir dispositivos Windows via WINRM, conclua as seguintes etapas:

Preparando o ambiente:

A maneira mais comum de preparar o ambiente é usar um certificado de servidor gerado por uma autoridade de certificação instalada no servidor Windows de destino. O certificado deve atender às seguintes condições:

- Os certificados raiz e intermediário da autoridade de certificação estão nos certificados de Autoridades de Certificação Raiz Confiáveis.
- O certificado do servidor é instalado nos certificados pessoais.
- O certificado do servidor deve mostrar que foi emitido para o nome do host completo do servidor.
- O certificado do servidor deve incluir a chave privada para esse servidor.

O comando a seguir configura o WINRM para conexões HTTPS remotas:

```
winrm quickconfig -transport:https
```

Esse comando executa o seguinte:

- Ativa o WINRM se não estiver ativo no momento
- Modifica o serviço WINRM para que o WINRM seja iniciado automaticamente na reinicialização
- Configura o listener WINRM HTTPS
- Modifica as regras de firewall do Windows para permitir conexões HTTPS remotas

O comando produz a saída a seguir. Insira **y** para confirmar as mudanças.

```
O serviço WinRM já está em execução nesta máquina.
O WinRM não está configurado para permitir o acesso remoto a esta
máquina para gerenciamento.
As seguintes mudanças devem ser feitas:

Criar um listener do WinRM no HTTPS://* para aceitar solicitações
WS-Man para qualquer IP nessa máquina.
Definir a configuração CertificateThumbprint para o serviço, a
ser usada para autenticação do CredSSP.
Configurar LocalAccountTokenFilterPolicy para conceder direitos
administrativos remotamente para os usuários locais.

Efetuar essas mudanças [s/n]? s

O WinRM foi atualizado para gerenciamento remoto.

Criado um listener WinRM no HTTPS://* para aceitar solicitações
WS-Man para qualquer IP nessa máquina.
Definidas as configurações necessárias para o serviço.
Configurada a LocalAccountTokenFilterPolicy para conceder
direitos administrativos remotamente para usuários locais.
```

Finalmente, para permitir a autenticação de ID do usuário/senha, execute o seguinte comando:

```
winrm set winrm/config/service/auth @{Basic="true"}
```

Uma alternativa é usar um certificado autoassinado. As instruções para essa configuração estão no Apêndice D: Windows usando WINRM na página 52.

Credenciais para lista de acesso:

- Para Conjuntos de escopos dinâmicos do VMware: nome do usuário/senha para a conta de serviço.
- Para Conjuntos de escopos gerais de descoberta: sistema computacional (Windows): nome do usuário/senha para a conta de serviço.
- A conta do serviço deve ser um membro de um dos seguintes grupos:
  - Administradores
  - WinRMRemoteWMIUsers__

Para incluir um usuário no grupo WinRMRemoteWMIUsers__, use o seguinte comando:

```
net localgroup WinRMRemoteWMIUsers__ [user_id] /add
```

Windows via SMB1

Para descobrir dispositivos Windows, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que o Windows Scripting Host (WSH) ou o serviço Management Instrumentation (WMI) e o VBScript estejam ativados no dispositivo de destino.
- Assegure-se de que a porta 445 não esteja bloqueada pelo firewall ou pelas políticas de segurança de IP, pois o TSA requer o protocolo Server Message Block (SMBv1) via TCP/IP.
- Para aplicar as políticas de segurança, acesse **Iniciar → Painel de controle → Ferramentas administrativas** e, em seguida, escolha a navegação a seguir, dependendo se suas políticas estão armazenadas localmente ou em um Active Directory:
  - Política armazenada localmente: Ferramentas administrativas → Política de segurança local → Políticas de segurança de IP no computador local
  - Políticas armazenadas no Active Directory: Ferramentas administrativas → Configurações de segurança de domínio padrão → Políticas d segurança de IP no Active Directory ou Ferramentas administrativas → Configurações de segurança do controlador de domínio padrão → Políticas de segurança de IP no Active Directory
- O TSA requer acesso ao compartilhamento de disco oculto de administração remota oculto para acessar o sistema %TEMP% e outros diretórios. O acesso ao compartilhamento de comunicações interprocessos (IPC$) também é necessário para o TSA acessar registros remotos. Assegure-se de que o serviço do Servidor de compartilhamento da Comunicação Inteprocessos foi iniciado. Para iniciar o serviço do Servidor, acesse → **Painel de controle → Ferramentas administrativas → Serviços → Servidor**.
- Assegure-se de que o Serviço de registro remoto esteja ativo. Isso é necessário para o TSA estabelecer uma sessão com o dispositivo Windows.

Credenciais para lista de acesso:

Windows release 2012 R2 e mais recente:

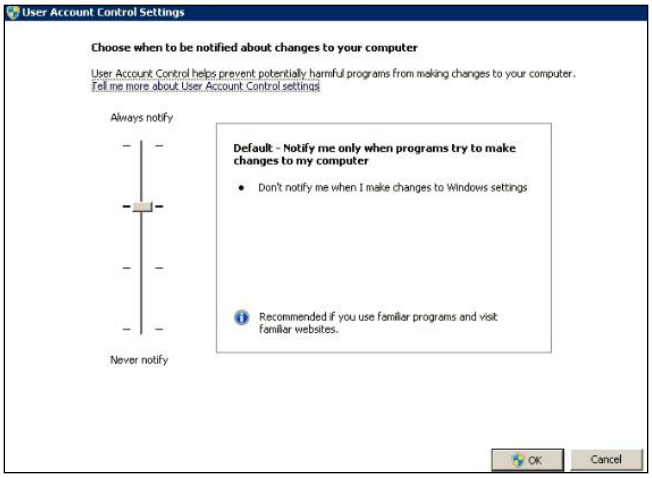
- Para Conjuntos de Escopos Dinâmicos do VMware - Conta/senha de administrador base. Essa conta funcionará independentemente das configurações do Controle de conta do usuário (UAC).
- Para Conjuntos de Escopos Gerais de Descoberta - Sistema computacional (Windows): Conta/senha de administrador base. Essa conta funcionará independentemente das configurações do Controle de conta do usuário (UAC).

Será possível usar uma conta que não seja a conta do Administrador base se determinadas condições forem atendidas. A conta deve ser uma conta de administrador local ou de domínio e as configurações do Controle de conta do usuário (UAC) devem atender a determinados requisitos. Consulte a tabela a seguir para obter as combinações de tipo de conta e configuração de UAC que são suportadas. Consulte a documentação do Microsoft Windows para obter detalhes adicionais sobre o UAC.

	Configurações do Controle de conta do usuário			
	Sempre notificar	**Notificar-me somente quando os programas tentarem fazer mudanças em meu computador (configuração padrão)**	**Notificar-me somente quando os programas tentarem fazer mudanças em meu computador (não em minha área de trabalho)**	**Nunca notificar**
Administrador base	**Sim**	**Sim**	**Sim**	**Sim**
Usuário no Grupo de administradores de domínio	**Não**	**Sim**	**Sim**	**Sim**
Usuário no Grupo de administradores locais	**Não**	**Sim**	**Sim**	**Sim**
Conta não administrador (domínio ou local)	**Não**	**Não**	**Não**	**Não**

Para acessar configurações do UAC, clique em **Iniciar**, em seguida, clique em **Painel de Controle**. Digite **uac** na caixa de procura e depois clique em **Mudar configurações do Controle de conta do usuário**.

A seguinte é a configuração padrão:



Dispositivos ATM

Alguns modelos de dispositivos ATM podem ser descobertos. Para descobrir os dispositivos ATM, incluindo informações básicas sobre seus componentes, conclua as etapas a seguir:

Preparando o ambiente:

- Modelos Wincor Nixdorf - siga as instruções para Windows via SMB.

Módulo de gerenciamento

Para IBM Flex Systems o ideal é iterar incluindo escopos e credenciais para entidades na seguinte ordem:

1. **O Flex System Manager (FSM):** isso retorna informações de alto nível sobre os Flex System Managers e o chassi que eles gerenciam, juntamente com seus nós de computação associados.

   > Se os FSMs não estiverem presentes, recomenda-se varrer os CMMs e todos os HMCs que gerenciam os nós de computação POWER nos Flex Systems.

2. **O Chassis Management Module (CMM):** para chassis que não são gerenciados por um FSM, aponte para cada CMM para recuperar informações de alto nível para cada chassi e seus nós associados.
3. **Os nós de computação:** isso retorna informações detalhadas sobre o sistema operacional.

Dispositivos Flex System Manager (FSM)

Para descobrir dispositivos FSM, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter autoridade **SMAdmin**.

Dispositivos Chassis Management Module (CMM)

Para descobrir dispositivos CMM, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter pelo menos a autoridade de **operador**.

Dispositivos Advanced Management Module (AMM)

Para descobrir dispositivos AMM, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter pelo menos a autoridade de **operador**.

HP Proliant Blade Server via HP OnBoard Administrator

Para os Hewlett Packard (HP) ProLiant Servers, recomenda-se incluir escopos e credenciais para entidades do HP OnBoard Administrator (HP OBA). O HP OBA retornará informações de alto nível sobre o HP OnBoard Administrator, o gabinete que ele gerencia e os nós de computação contidos no gabinete.

Para descobrir um servidor HP Proliant Blade via HP OnBoard Administrator (OBA), conclua as seguintes etapas:

Preparando o ambiente:

- O HP OBA deve estar no modo ativo.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade de **administrador de OA**, **Operador de OA** ou **Usuário de OA** no HP Onboard Administrator. Recomenda-se a função de autoridade de **Usuário de OA**.

O TSA coleta informações dos HP OnBoard Administrators que estão no estado ativo somente. Nenhuma informação é coletada dos HP OnBoard Administrators que estão no estado standby.

Dispositivos Integrated Management Module (IMM) & Integrated Management Module II (IMM2)

Para descobrir dispositivos IMM e IMM2, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode ter qualquer autoridade válida.

HP Integrity e HP9000 Servers via iLO

O iLO é uma placa do processador distinta dentro do HP Integrity e HP9000 Server que fornece informações básicas de hardware sobre o servidor. O iLO fica ativo assim que o servidor é conectado, mesmo que o servidor ainda não esteja ligado.

Para descobrir as informações de nível de Resumo via iLO para servidores HP Integrity e HP9000, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode usar qualquer nível de autoridade válido. Recomenda-se autoridade de usuário.

Dell Server via Integrated Dell Remote Access Controller (iDRAC)

iDRAC é uma placa do processador distinta dentro do Dell Server que fornece informações básicas de hardware sobre o servidor. O iDRAC é desabilitado por padrão e precisa ser habilitado e configurado para ser usado.

Os pré-requisitos a seguir são necessários:

- O iDRAC precisa ser ativado e configurado para ser usado.
- Um módulo de serviço iDRAC precisa ser instalado no sistema operacional para que as informações do sistema operacional sejam detectáveis.

Para descobrir as informações de inventário de nível resumido por meio do iDRAC para servidores Dell, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter pelo menos nível de autoridade de administrador.
- A credencial deve ter acesso SSH para executar comandos da CLI.

Dispositivos de rede

Esta seção fornece informações detalhadas sobre os seguintes tipos de dispositivos de rede:

Plataforma
Switches BNT
Switches Brocade
Ponto de verificação
Switches Cisco
F5 Big-IP (TMOS)
Fortinet (FortiOS)
Switches IBM b-type Storage Area Network (SAN)
Switches Juniper
Palo Alto Networks (PAN-OS)
Switches QLogic
Clique em cada um dos links acima para obter informações detalhadas.

Switches BNT

Para descobrir switches BNT, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter autoridade de **administrador**.

Brocade

Para descobrir dispositivos Brocade, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- Modo Virtual Fabric desativado: a conta do serviço pode usar qualquer autoridade válida. A autoridade de **usuário** é recomendada.
- Modo Virtual Fabric ativado: a conta de serviço requer autoridade de **Administrador** no Fabric OS.

Ponto de verificação

Para descobrir sistemas de Ponto de verificação, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- A conta de serviço deve ter autoridade de administrador (**adminRole**).
- A conta do serviço deve ter acesso SSH para executar os comandos da CLI.

Cisco

Para descobrir dispositivos Cisco, é possível usar as seguintes credenciais do sistema de computador ou as credenciais do SNMP.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- Outro (dispositivo Cisco): Nome de usuário/senha e autenticação de senha para ativação opcional para a conta de serviço.
- Outro (Cisco Works): autenticação de nome de usuário/senha para a conta de serviço.
- A conta de serviço requer privilégios da função de **administrador de rede**.
- SNMP: insira a sequência de comunidades (para SNMPv1 e SNMPv2).
- SNMP (SNMPv3):
  - Insira:
    - nome do usuário
    - senha
    - senha privada (opcional)
  - Selecionar protocolo de autenticação: nenhum, MD5, SHA

É importante que uma única sequência de comunidades seja disponibilizada ao TSA, que tenha acesso somente leitura a TODOS nos dispositivos de rede do escopo.

F5 Big-IP (TMOS)

Para descobrir sistemas F5 Big-IP que estão executando TMOS, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador F5.
- A conta do serviço deve ter acesso SSH para executar os comandos da CLI de TMSH.

Fortinet (FortiOS)

Para descobrir os dispositivos Fortinet que estão executando FortiOS, conclua as seguintes etapas:

Preparando o ambiente

- Assegure-se de que o console do sistema esteja configurado para exibir a saída de comando completa:

```
config system console
set output standard
end
```

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- A conta do serviço deve ter pelo menos as permissões Somente leitura.

Switches IBM b-type Storage Area Network (SAN)

Para descobrir dispositivos IBM b-type SAN, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- Modo Virtual Fabric desativado: a conta do serviço pode usar qualquer autoridade válida. A autoridade de **usuário** é recomendada.
- Modo Virtual Fabric ativado: a conta de serviço requer autoridade de **Administrador** no Fabric OS.

Juniper

Para descobrir dispositivos Juniper, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

Nota: a descoberta de informações de tamanho da memória requer que o Junos® versão 12.1 ou posterior esteja instalado no dispositivo.

Palo Alto Networks (PAN-OS)

Para descobrir sistemas Palo Alto Network que estão executando PAN-OS, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ser Superusuário ou Superusuário (somente leitura)
- A conta do serviço deve ter acesso de API de REST (porta 443).

Switches QLogic

Para descobrir switches QLogic, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

Dispositivos de Armazenamento

Esta seção fornece informações detalhadas sobre os tipos de dispositivos de Armazenamento e Fita a seguir:

Plataforma
EMC Corporation Storage
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx, DS4xxx ou DS5xxx
IBM DS6xxx or DS8xxx
IBM FlashSystem, v9000
IBM ProtecTier
IBM SVC ou V7000/V3700
Biblioteca de fitas IBM TS3100
Biblioteca de fitas IBM TS3200
IBM TS3310 Tape Library
IBM TS3494, TS3953 Tape Libraries
IBM TS3500, TS3584 Tape Libraries
Biblioteca de fitas IBM TS4300

Plataforma
IBM TS4500 Tape Library
IBM TS7700 Tape Library
IBM V7000 Unified
IBM XIV
nSeries ou NetApp

Clique em cada um dos links acima para obter informações detalhadas.

EMC Corporation Storage

EMC CLARiiON / VNX / VMAX

Para descobrir dispositivos EMC CLARiiON/VNX/VMAX, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que uma instância do produto EMC SMI-S esteja instalada em um sistema Windows ou Linux. Por padrão, o TSA segue a recomendação de EMC SMI-S para descobrir o local do provedor usando SLP. Se sua política de segurança de rede bloquear o tráfego de rede SLP, o TSA poderá ser configurado para acessar diretamente o Provedor EMC SMI-S sem o uso do SLP
- Se sua segurança de rede não permitir tráfego de rede SLP, use a página **Configurações de descoberta→ Configurações de conexão** para fornecer informações sobre em quais portas os Provedores EMC SMI-S atendem solicitações de consulta.
- Assegure-se de que pelo menos um dos endereços IP que o Provedor SMI-S está usando esteja definido em um conjunto de escopos. O TSA se conectará ao Provedor SMI-S para recuperar informações sobre os dispositivos EMC que ele gerencia. Os endereços IP dos dispositivos EMC individuais não precisam ser colocados em um conjunto de escopos. O TSA tenta se conectar ao provedor SMI-S usando HTTPS se disponível, caso contrário, o HTTP será usado.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.

- A conta do serviço pode usar qualquer função válida. A função de **monitor** é recomendada.

> Somente as credenciais para o provedor SMI-S precisam ser inseridas no TSA. Nenhuma credencial para os dispositivos EMC precisa ser inserida.

EMC Data Domain

Para descobrir dispositivos EMC Data Domain, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode ter qualquer nível de autoridade. Recomenda-se usar o níveis mais baixo de autoridade.

HP StorageWorks P2000 Modular Smart Array

Para descobrir sistemas HP Storage, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço pode ter qualquer nível de autoridade. Recomenda-se usar o níveis mais baixo de autoridade.

Armazenamento IBM DS3xxx, DS4xxx ou DS5xxx

Para descobrir dispositivos IBM DS3xxx, DS4xxx ou DS5xxx, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que o gerenciador de armazenamento permita o uso de comandos **smcli** remotos.

Credenciais para lista de acesso:

- Para dispositivos de armazenamento não seguros, nenhuma credencial é necessária.
- Para dispositivos de armazenamento protegidos, conclua as seguintes etapas:
  - Sistema de computador: nome do usuário/senha para a conta do serviço.
  - A conta de serviço pode ter a função de **administrador** ou de **monitor**. A função de **monitor** é recomendada.

Armazenamento IBM DS6xxx/DS8xxx

Para descobrir dispositivos IBM DS6xxx/DS8xxx, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que o gerenciador de armazenamento permita o uso de comandos **dscli** remotos.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter a função de **monitor**.

IBM FlashSystem, v9000

Para descobrir IBM FlashSystems, conclua as seguintes etapas:

Preparando o ambiente:

- Para modelos antigos, a MCP (Porta de Controle de Gerenciamento) deve estar em um estado ativo para descobrir o sistema com êxito.
  - Para verificar se um sistema está no estado ativo, execute o comando - `system status`.
  - Dos dois endereços IP, se um IP ficar inativo, o sistema ficará no estado passivo. Para ativar a outra porta Ethernet, execute o comando - `sync activate`.
  - O sistema descoberto deve ser o endereço IP de gerenciamento e/ou o nó de configuração.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/autenticação de chave SSH para a conta do serviço.
- A conta do serviço pode usar qualquer função válida. A função de **monitor** é recomendada.

IBM ProtecTIER

Para descobrir dispositivos ProtecTIER, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter privilégios de administrador.

Armazenamento IBM SVC, V7000/V3700

Para descobrir dispositivos SVC e V7000/V3700, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha ou nome do usuário/chave SSH para autenticação.
- A conta do serviço pode usar qualquer função válida. A função de **monitor** é recomendada.

Biblioteca de fitas IBM TS3100

Para descobrir dispositivos de Biblioteca de Fitas TS3100, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

Biblioteca de fitas IBM TS3200

Para descobrir dispositivos de Biblioteca de Fitas TS3200, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

IBM TS3310 Tape Library

Para descobrir dispositivos de Biblioteca de Fitas TS3310, conclua as seguintes etapas:

Preparando o ambiente:

- O serviço da web é configurado no modo seguro sempre.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

Bibliotecas de fitas IBM TS3494, TS3953

Para descobrir dispositivos de Biblioteca de Fitas TS3494, TS3953, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode ter a autoridade mínima necessária.

Bibliotecas de Fitas IBM TS3500, TS3584

Os pré-requisitos a seguir são necessários:

- A Biblioteca de Fitas TS3500 deve estar no nível de firmware 8xxx (ou superior).
- O Advanced Library Management System (ALMS) deve estar instalado e ativado.

> Ambas as conexões SSL e não SSL são suportadas.

Para descobrir dispositivos TS35xx Tape Library, conclua as seguintes etapas:

Preparando o ambiente:

- A interface da web do TS3500 pode ser configurada para **Nenhuma proteção de senha** ou **Proteção de senha**

- Se **Proteção de senha** estiver ativada, crie uma credencial conforme descrito em **Credenciais para lista de acesso** abaixo.
- Se **Proteção de senha** estiver desativada, nenhuma credencial será necessária.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço deve ter autoridade do administrador.

Biblioteca de fitas IBM TS4300

Os pré-requisitos a seguir são necessários:

- A Biblioteca de fitas TS4300 deve ter a API de REST ativada na porta 3031 via HTTPS.

Para descobrir dispositivos de Biblioteca de Fitas TS4300, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter pelo menos o nível de autoridade de **Serviço**.
- A credencial deve ter acesso à API de Rest na porta 3031 via HTTPS.

IBM TS4500 Tape Library

Os pré-requisitos a seguir são necessários:

- A Biblioteca de Fitas TS4500 deve estar no nível de firmware 1.4.1.2 ou superior (até 1.7.0.0).
- O Advanced Library Management System (ALMS) deve estar instalado e ativado.

Ambas as conexões SSL e não SSL são suportadas.

Para descobrir dispositivos TS4500 Tape Library, conclua as seguintes etapas:

Preparando o ambiente:

- A interface da web do TS4500 pode ser configurada para exigir nome de usuário/senha ou pode ser configurada para que nome de usuário/senha não sejam necessários.

Credenciais para lista de acesso:

- Sistema de computador: o nome de usuário/senha para a conta de serviço é necessário apenas se o TS4500 estiver configurado para requerer credenciais de login.
- A conta de serviço deve ser mapeada para a função de **Serviço**.

Biblioteca de fitas IBM TS7700

Para descobrir dispositivos TS7700 Tape Library, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço precisa apenas de autoridade **Somente leitura**.

Armazenamento IBM V7000 Unified

Para descobrir dispositivos V7000 Unified, conclua as seguintes etapas:

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode usar qualquer função válida. A função de **monitor** é recomendada.

Armazenamento IBM XIV

Para descobrir dispositivos XIV, conclua as seguintes etapas:

Preparando o ambiente:

- Assegure-se de que o gerenciador de armazenamento permita o uso de comandos **xcli** remotos.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta de serviço deve ter a função de usuário **somente leitura**.
- Lembre-se que os sistemas XIV podem ter um limite baixo para tentativas de conexão inválidas antes de gerar alertas. Se você estiver usando um grande conjunto de credenciais, poderá exceder esse limite e fazer com que problemas desnecessários sejam relatados. Tente agrupar os dispositivos XIV em um único conjunto de escopos e restringir suas credenciais de conta do serviço a esse conjunto de escopos.

Armazenamento nSeries ou NetApp

Para descobrir dispositivos nSeries ou NetApp, conclua as seguintes etapas:

Preparando o ambiente:

- A coleta de dados é suportada para sistemas configurados com Dados ONTAP CLI, RLM CLI e SP CLI. No entanto, o BMC CLI não é suportado.
- A opção **telnet.distinct.enable** deve estar ligada.

Credenciais para lista de acesso:

- Sistema de computador: nome do usuário/senha para a conta do serviço.
- A conta do serviço pode ter qualquer nível de autoridade. Recomenda-se usar o níveis mais baixo de autoridade.

Considerações sobre Firewall

O(s) firewall(s) entre o dispositivo e os dispositivos de descoberta podem impedir que uma descoberta completa e bem-sucedida ocorra.

Nos casos em que é necessário atravessar um firewall, talvez seja necessário abrir portas no firewall, dependendo do tipo de dispositivo que o usuário deseja descobrir. Geralmente, as portas 22 (SSH) e 161 (SNMP) devem ser abertas, seguidas por aquelas apropriadas na tabela abaixo com base nos dispositivos suportados.

Endpoint de descoberta	**Portas**	**Interface/Protocolo**
Diversas	161	SNMP
Dispositivo de Armazenamento		
DS6000 / DS8000	1750 (HTTP) ou 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries ou NetApp	22 / 23	SSH ou Telnet
SVC ou V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3100 / TS3200	80	HTTP
IBM TS3310	80	HTTP
IBM TS3500	443 / 80	HTTPS ou HTTP
IBM TS4300	3031	HTTPS (na porta 3031)
IBM TS4500	443 / 80	HTTPS ou HTTP
IBM TS7700	443 / 80	HTTPS ou HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22 / 23	SSH ou Telnet
IBM Flash System, v9000	22	SSH

Endpoint de descoberta	Portas	Interface/Protocolo
EMC Corporation Storage - CLARiion/VNX/VMAX	427 - (padrão) quando a descoberta SLP é permitida, além disso, se a descoberta SLP estiver desativada, essa porta não será usada. Portas HTTPS / HTTP configuradas pelo provedor EMC SMI-S; os valores padrão são 5989 / 5988	SLP, HTTPS / HTTP
	É possível ativar ou desativar a opção de descoberta SLP para descobrir os dispositivos de armazenamento EMC por meio dos Provedores EMC SMI-S.	
EMC Corporation Storage – EMC Data Domain	22	SSH*
Sistemas operacionais e Hosts		
FSM	22 / 23	SSH ou Telnet
CMM	22 / 23	SSH ou Telnet
AMM	22 / 23	SSH ou Telnet
HP Proliant Blade Server via HP OnBoard Administrator	22 / 23	SSH ou Telnet
IMM e IMM2	22 / 23	SSH ou Telnet
HP iLO para os servidores HP Integrity / HP 9000	22 / 23	SSH* ou Telnet
Dell iDRAC	22 / 23	SSH ou Telnet
Dispositivos de rede		
Brocade	161 / 22 /23	SNMP, SSH, Telnet
Switches IBM b-type Storage Area Network (SAN)	22 /23	SSH, Telnet
Cisco	161 / 22 / 23	SNMP, SSH, Telnet
BNT	22 / 23	SSH ou Telnet

Endpoint de descoberta	Portas	Interface/Protocolo
Juniper	22 / 23	SSH ou Telnet
QLogic	22 / 23	SSH* ou Telnet
Fortinet (FortiOS)	22 / 23	SSH ou Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH ou Telnet
Ponto de verificação	22 / 23	SSH ou Telnet
Sistemas operacionais/Plataformas do servidor		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443, 5989	HTTPS
IVM	22 / 23	SSH ou Telnet
IBM i	22	SSH
SUN	22	SSH

- O TSA suporta apenas o SSH v1 para os dispositivos que são marcados por SSH*.

Problemas de descoberta

A maioria dos problemas de descoberta deve-se a questões de acesso ou autorização.

Os problemas de acesso mais comuns acontecem devido a firewalls que bloqueiam o acesso às portas necessárias no dispositivo. As portas que precisam ser abertas e alcançadas variam de acordo com o tipo de dispositivo. Consulte a seção "Considerações de firewall" na página 42 para determinar quais portas são aplicáveis.

Os problemas de autorização mais comuns incluem o seguinte:

- **Nenhuma credencial definida**. Assegure-se de que as credenciais para os dispositivos estejam definidas no TSA e que as contas de serviço apropriadas sejam criadas nos dispositivos.
- **Nome do usuário ou senha da credencial incorretos**. Use a função **Testar** ao criar ou editar uma credencial para verificar se a credencial é válida.
- **Senha da credencial expirada**.
- **A credencial não tem as autoridades necessárias no dispositivo**. Para determinar os requisitos de credencial para um dispositivo de destino, consulte a seção Configuração de descoberta de dispositivo na página 12.
- **Use um tipo de credencial válido**. Para dispositivos Windows, crie uma credencial 'Computer System (Windows)' e não uma credencial 'Computer System'.

Verifique a página **Status de autenticação (Ferramentas → Status de autenticação)** para ver se quaisquer credenciais da conta de serviço possuem senhas expiradas ou pararam de funcionar.

Considerações contínuas

Depois que as partes desejadas da rede forem definidas no TSA e varridas com sucesso, o TSA poderá ser deixado para executar descobertas e transmissões periódicas nas programações desejadas.

Veja a seguir algumas atividades contínuas esperadas:

- Revise periodicamente os relatórios gerados pelo TSA com seu representante IBM.
- Faça backup periodicamente por meio da interface com o usuário do TSA para salvar uma cópia da configuração do TSA.

Essa operação não salva os dados coletados pelo TSA. Ela apenas salva as informações de configuração.

- Verifique periodicamente a **página** Status de autenticação **(Ferramentas → Status de autenticação)** para ver se quaisquer credenciais de conta de serviço possuem senhas expiradas ou pararam de funcionar.
- Quando as senhas forem atualizadas para as contas do serviço nos dispositivos, assegure-se de atualizar também as senhas no TSA, para manter a definição de credencial no TSA em sincronização com a credencial no dispositivo de destino.
- Se a sua política de segurança permitir, considere configurar as contas do serviço com senhas que não expiram ou usar chaves SSH. Isso elimina a necessidade de atualizar periodicamente as senhas na interface com o usuário do TSA e nos dispositivos.

Resolução de problemas

Sessão ativa para Descoberta de AMM

Os dispositivos AMM têm uma configuração que limita o número de sessões ativas simultâneas (máximo de 20). Se essa configuração não for alta o suficiente para permitir que o TSA crie uma sessão, não será possível descobrir o dispositivo AMM.

Para mudar o limite das sessões ativas de um dispositivo AMM, siga estas etapas:

1. Efetue login na interface da web do AMM digitando o endereço IP do dispositivo AMM em um navegador da web.
2. Acesse **Controle MM → Perfis de login**.
3. Clique no ID de login que o TSA está usando para descobrir o dispositivo.
4. Aumente o valor da configuração **Máximo de sessões ativas simultâneas**.
5. Clique em **Salvar** na parte inferior direita da página.

Apêndice A: Termos e definições

Presume-se que o leitor tenha um entendimento profundo de redes e protocolos Internet Protocol (IP).

Termo	**Definição**
Dispositivo de descoberta	Consulte os componentes de implementação da infraestrutura de TI que podem ser descobertos pelo TSA. Os dispositivos típicos incluem: Servidores, Sistemas de computador (por exemplo, IBM, Dell e HP), Elementos de armazenamento e Elementos de rede (por exemplo, switches, pontes, roteadores).

Apêndice B: Itens diversos

Funções de download da interface com o usuário

Em alguns casos, ao usar um navegador da web, Fazer download de todos os logs (na página **Log de atividades**) ou Downloads de arquivo (na página **Histórico de descoberta**) não são concluídos com sucesso. Para resolver esse problema, tente alternar para outro navegador da web suportado, conforme documentado no Guia de Configuração do IBM Technical Support Appliance. Se isso não for uma opção, tente reconfigurar as propriedades do seu navegador para as configurações padrão.

Apêndice C: CIM Provider for VMware ESXi

Um provedor CIM é um conjunto de plug-ins do VMware ESXi que podem coletar informações adicionais de hardware e firmware sobre o servidor em que o VMware ESXi está executando.O TSA e o VMware vCenter podem se beneficiar dessas informações adicionais.

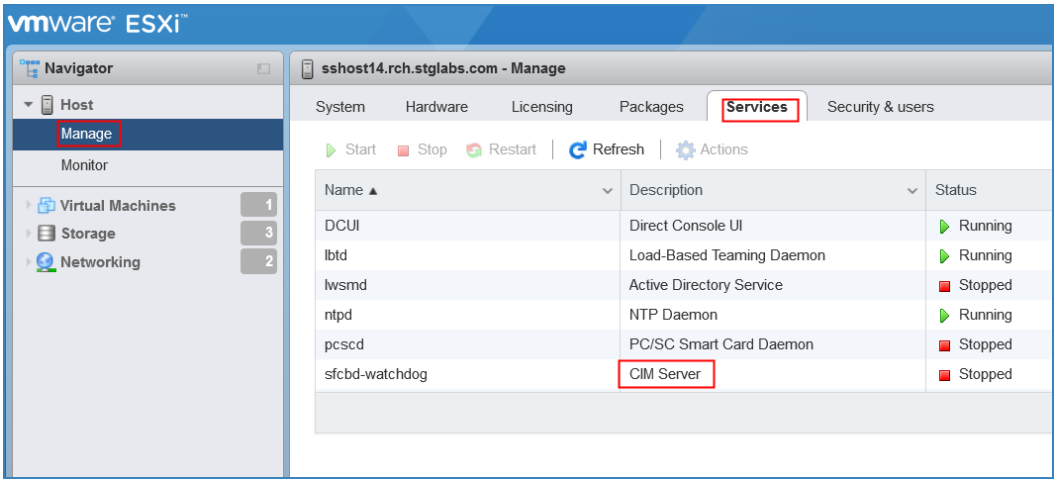
Os plug-ins do provedor CIM são desenvolvidos pelos fabricantes de servidores e componentes. Para garantir que os plug-ins do provedor CIM sejam incluídos no ESXi, use uma imagem de instalação customizada em que os plug-ins do provedor CIM estão incluídos. Para instâncias existentes do VMware ESXi que não têm o provedor CIM instalado, obtenha os plug-ins necessários dos fabricantes do servidor e do componente e instale no ESXi. O VMware fornece uma lista dos vários plug-ins fornecidos pelos fabricantes.

Para obter mais informações, consulte https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

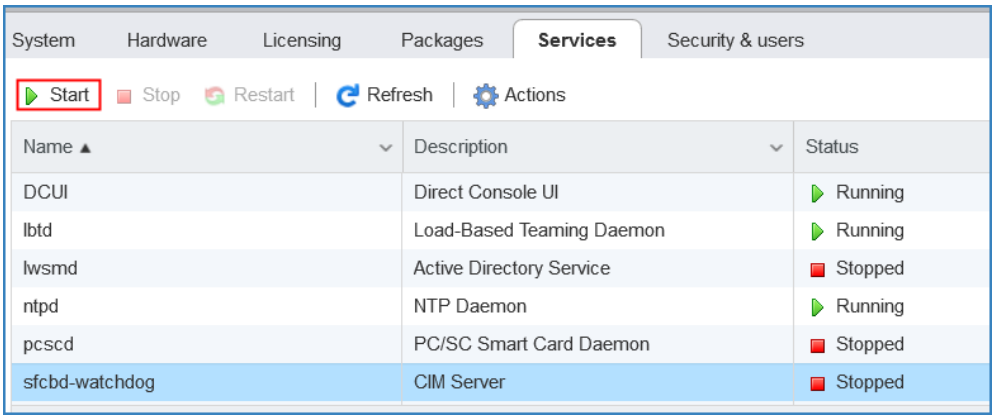
Para determinar se o provedor CIM está ativo, e para ativá-lo se não estiver ativo, siga as etapas abaixo.

No VMware vSphere Web Client

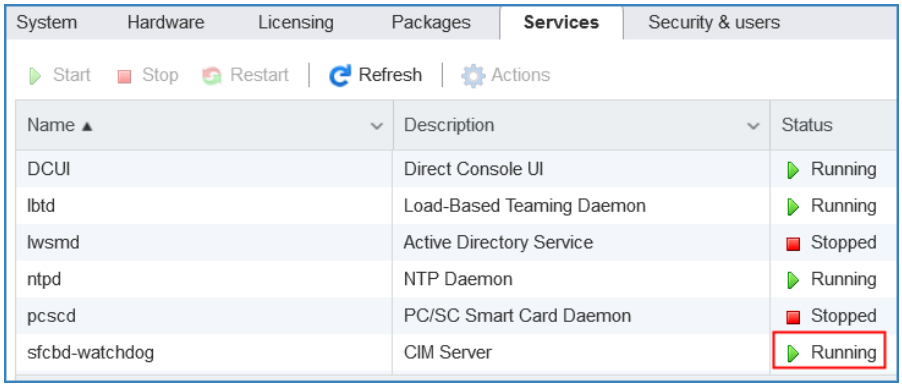
- Efetue login no VMware vSphere Web Client.
- Clique em **Host → Gerenciar** na janela de navegação esquerda e selecione a guia **Serviços** no painel direito.
- Um conjunto de serviços, incluindo o **Servidor CIM** é exibido.



- Se o **Servidor CIM** estiver no estado **Parado**, selecione-o e clique em **Iniciar**.



- O serviço do Servidor CIM é iniciado e o status estará no estado **Em execução**.



Apêndice D: Windows usando WINRM

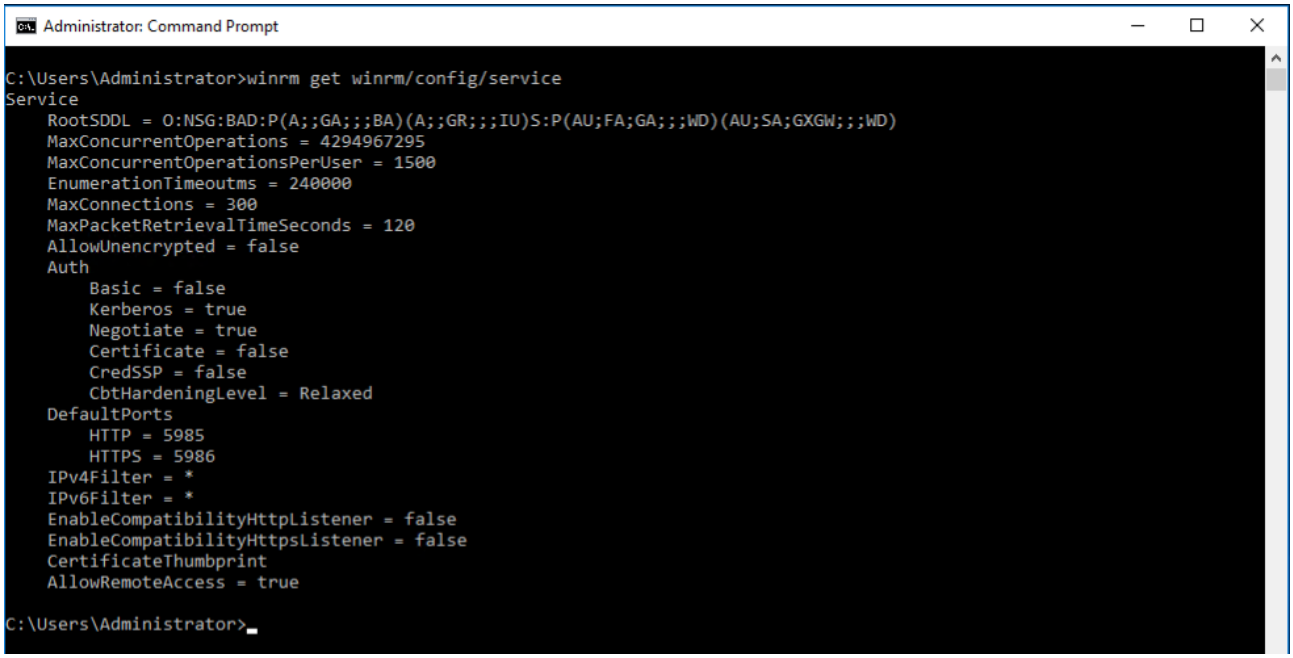
Para o Windows 2012 Server, o 2016 Server e o 2019 Server, o serviço WINRM é iniciado automaticamente. Entretanto, o gerenciamento remoto não é ativado por padrão. Aqui está um breve resumo do que é necessário para permitir que o WINRM permita conexões remotas usando um certificado autoassinado:

- Ative o WINRM para aceitar conexões HTTPS autenticadas com ID do usuário/senha
- Associe um certificado autoassinado ao listener HTTPS para o WINRM que foi ativado
- Modifique o firewall do Windows para permitir a conexão de entrada via porta 5986 (a porta padrão do WINRM HTTPS)

Os comandos a seguir preparam o WINRM para permitir conexões remotas via HTTPS:

- Determine o estado atual do serviço WINRM usando este comando:

  winrm get winrm/config/service



- O valor para **AllowUnencrypted** deve ser *false*. Se *true*, use o comando a seguir para mudar para *false*:

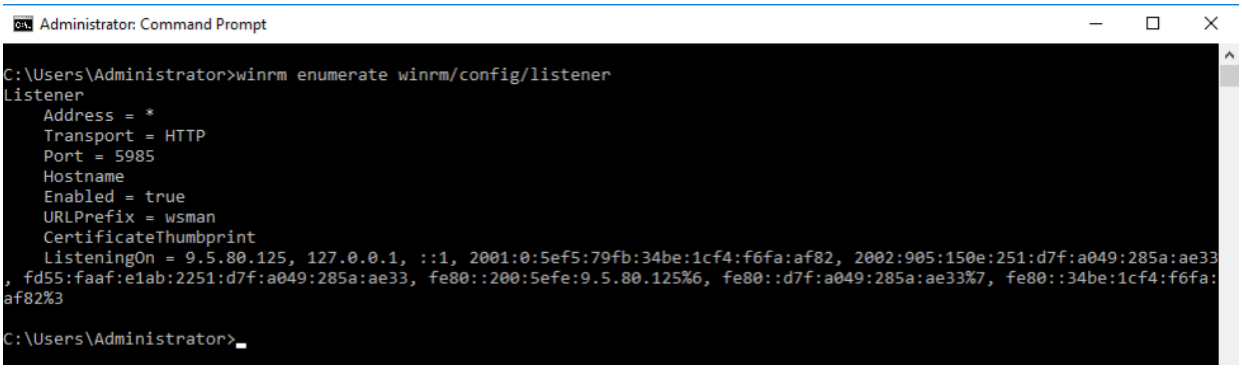
  winrm set winrm/config/service @{AllowUnencrypted="false"}

- O valor para **Basic** deve ser *true*. Se *false*, use o comando a seguir para mudar para *true*:

  winrm set winrm/config/service/auth @{Basic="true"}

- Determine se WINRM tem um listener HTTPS usando este comando:

  winrm enumerate winrm/config/listener

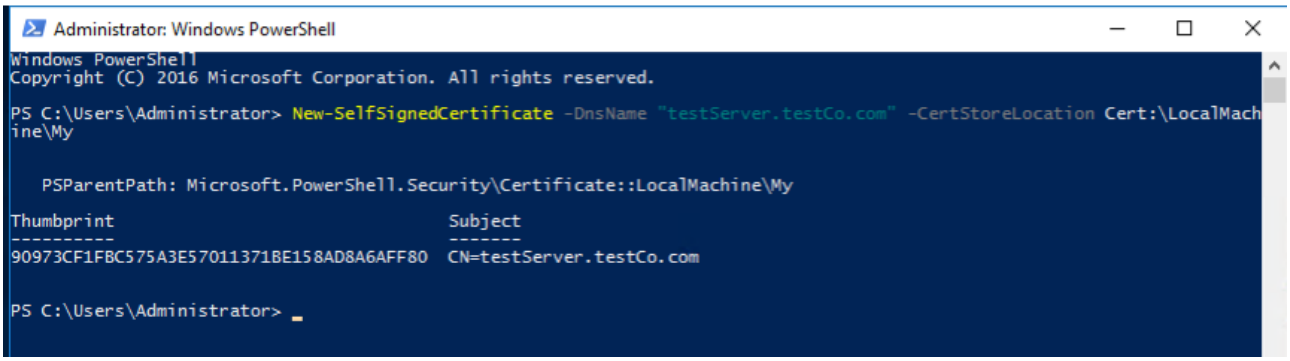


- No exemplo de comando acima, existe apenas um listener HTTP; portanto, um listener HTTPS precisa ser configurado. Para ativar o listener HTTPS, se ele não estiver configurado:
  - Usando o PowerShell, crie um certificado autoassinado:

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > Substitua o DnsName **(myHost@myBusiness.com)** no exemplo acima com o nome completo do domínio do Windows para o servidor Windows.

  - Salve a impressão digital do certificado para a próxima etapa



- Crie o listener HTTPS:

  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}

- Verifique para assegurar-se de que o HTTPS agora está configurado:

  winrm enumerate winrm/config/listener

- Modifique o firewall do Windows para permitir conexões remotas de entrada para o WINRM:

- Acesse o Painel de Controle → Sistema Firewall de Segurança →do Windows
- Clique em Configurações avançadas. A janela Windows Firewall with Advanced Security é exibida.
- Clique em Regras de entrada.
- Selecione o menu Ações e clique na Nova regra. O novo Assistente de regra de entrada é exibido.
- Selecione **Porta** e clique em **Avançar**.
- Selecione **TCP → Especificar portas locais** e especifique 5986. Clique em **Avançar.**
- Selecione a opção **Permitir a conexão** e clique em **Avançar**.
- Selecione as caixa de seleção **Domínio**, **Privado** e **Público** se ainda não selecionadas e clique em **Avançar.**
- Dê um nome à nova regra (como Gerenciamento Remoto do Windows (HTTPS-In) e clique em **Concluir**.

Avisos

IBM Corporation
Comunicações de marketing
Systems and Technology Group
Route 100
Somers, Nova Iorque, 10589
Produzido nos Estados Unidos da América
Janeiro de 2021.

Este documento foi desenvolvido para produtos e/ou serviços oferecidos nos Estados Unidos. É possível que a IBM não ofereça os produtos, recursos ou serviços discutidos nesta publicação em outros países.

As informações podem estar sujeitas a alterações sem aviso prévio. Consulte o contato comercial local da IBM para obter informações sobre os produtos, recursos e serviços disponíveis em sua área.

Todas as declarações relacionadas aos objetivos e as intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam apenas metas e objetivos.

IBM, o logotipo IBM, POWER, System I, System p, i5/OS são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Uma lista completa das marcas comerciais pertencentes à IBM nos Estados Unidos pode ser encontrada em http://www.ibm.com/legal/copytrade.shtml.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou de serviço de terceiros.

Os produtos de hardware IBM são fabricados a partir de peças novas ou de peças novas e usadas. Independentemente do caso, nossos termos de garantia se aplicam.

Este equipamento está sujeito às regras da FCC. Ele estará em conformidade com as regras adequadas da FCC antes da entrega final para o comprador.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores desses produtos.

Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

A página inicial da IBM na Internet pode ser encontrada em http://www.ibm.com.

A página inicial do IBM System p na Internet pode ser encontrada em http://www.ibm.com/systems/p.

A página inicial do IBM System I na Internet pode ser encontrada em http://www.ibm.com/systems/i.

PSW03007-USEN-00