CONTENTS

RELATED

Como Instalar o Servidor Web Apache no Ubuntu 18.04 [Quickstart]

View

Como Criar uma Imagem do Seu Ambiente Linux e Lançá-la na DigitalOcean

View

// Tutorial //

Como instalar e configurar um daemon e cliente SNMP no Ubuntu 18.04

Published on April 10, 2020

Ubuntu 18.04 Networking System Tools

By Vadym Kalsin and Justin Ellingwood

Português

O autor selecionou Internet Archive para receber uma doação como parte do programa Write for DOnations.

Introdução

Grande parte de ser um administrador de sistemas é coletar informações precisas de seus servidores e infraestrutura. Existe um grande número de ferramentas e opções para a reunião e processamento deste tipo de informação. Muitas delas são construídas em uma tecnologia chamada *SNMP*.

SNMP significa protocolo simples de gerência de rede. É uma maneira que os servidores podem compartilhar informações sobre o estado atual deles, e também um canal através do qual um administrador pode modificar valores pré-definidos. Embora o protocolo em si seja leve, a estrutura de programas que implementam o SNMP pode ser bastante complexa. Para obter mais informações sobre o básico do protocolo SNMP, consulte nosso artigo de Introdução ao SNMP.

Neste guia, você configurará as ferramentas para se comunicar usando o SNMP. Você usará dois servidores Ubuntu 18.04. para uma demonstração. Um deles terá o *SNMP manager*, que dirá ao agente para implementar dispositivos de rede. Este servidor será chamado de **manager server**. O outro servidor terá o *SNMP agent*, que agirá conforme as ordens do servidor gerente. Este servidor será chamado de **agent server**. Você pode escolher instalar o agente na máquina do gerente também. Porém, mantê-los separados torna mais fácil demonstrar qual funcionalidade é fornecida por cada componente.

Pré-requisitos

Para seguir este tutorial, você vai precisar do seguinte:

- Dois servidores Ubuntu 18.04 configurados seguindo o Guia de configuração inicial de servidor para o Ubuntu 18.04, incluindo um usuário não raiz com privilégios sudo e um firewall configurado com o `ufw`.

Passo 1 – Instalando o daemon e utilitários SNMP

Comece a explorar como o SNMP pode ser implementado em um sistema instalando o daemon e as ferramentas em seus servidores Ubuntu.

A partir de sua máquina local, faça login no **manager server** como seu usuário não raiz:

```
$ ssh your_username@manager_server_ip_address
```

Copy

Atualize o índice do pacote para o gerenciador de pacotes do APT:

```
$ sudo apt update
```

Copy

Em seguida, instale o software SNMP:

```
$ sudo apt install snmp snmp-mibs-downloader
```
Copy

O pacote `snmp` fornece uma coleção de ferramentas de linha de comando para a emissão de solicitações SNMP a agentes. O pacote `snmp-mibs-downloader` ajudará a instalar e gerenciar os arquivos da Base de informações de gerenciamento (MIB), que monitora os objetos de rede.

Então, abra um novo terminal em sua máquina local e faça login no **agent server**:

```
$ ssh your_username@agent_server_ip_address
```
Copy

Em **agent server**, atualize o índice do pacote:

```
$ sudo apt update
```
Copy

Em seguida, instale o daemon SNMP.

```
$ sudo apt install snmpd
```
Copy

Note que você não precisa do pacote `snmp-mibs-downloader` , pois o **agent server** não gerenciará os arquivos MIB.

Agora que instalou esses componentes, você configurará seu **manager server**.

Passo 2 – Configurando o servidor gerente do SNMP

Como mencionado anteriormente, a maioria dos trabalhos acontece no **agent server**. Por este motivo, sua configuração no **manager server** será mais simples. Você precisa modificar um arquivo para garantir que as ferramentas do SNMP possam usar os dados extras do MIB instalados.

Em seu **manager server**, abra o arquivo `/etc/snmp/snmp.conf` em seu editor de texto com privilégios sudo. Este tutorial usará o `nano` .

```
$ sudo nano /etc/snmp/snmp.conf
```
Copy

Neste arquivo, há alguns comentários e uma única linha descomentada. Para permitir que o gerente importe os arquivos do MIB, deixe a linha `mibs :` como comentário:

/etc/snmp/snmp.conf

```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :
```

Salve e feche o `snmp.conf` pressionando `CTRL+X` , seguido de `Y` e, em seguida, `ENTER` se estiver usando o `nano` .

Você acabou de configurar o **manager server**, mas ainda assim precisará usar este servidor para ajudar a configurar seu **agent server**, o que você fará no próximo passo.

Passo 3 – Configurando o servidor agente do SNMP

Como um verdadeiro sistema de cliente-servidor, o **agent server** não possui nenhuma das ferramentas externas necessárias para configurar sua própria configuração do SNMP. Você pode modificar alguns arquivos de configuração para fazer algumas alterações, mas a maioria das alterações que precisa fazer serão feitas ao se conectar ao seu **agent server**, a partir do servidor de gerenciamento.

Neste tutorial, você usará a versão 3 do protocolo do SNMP. Ao contrário do SNMPv1 e do v2, no SNMPv3, cada mensagem contém parâmetros de segurança que são codificados. Neste passo, você configurará a autenticação e as regras de controle de acesso do SNMPv3.

Para começar, em seu **agent server**, abra o arquivo de configuração do daemon com privilégios do sudo:

```
$ sudo nano /etc/snmp/snmpd.conf
```

Copy

Dentro dele, você terá que fazer algumas alterações. Esses arquivos serão usados principalmente para a inicialização de sua configuração, para que possa gerenciá-la de seu outro servidor.

Primeiro, altere a diretiva do `agentAddress`. Atualmente, ela está definida para permitir apenas conexões originárias do computador local. Será necessário comentar a linha atual e descomentar a linha abaixo dela, que permite todas as conexões.

/etc/snmp/snmpd.conf

```
#  Listen for connections from the local system only
#agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161
```

Nota: como permitir todas as conexões não é uma boa prática de segurança, é melhor se certificar de reverter isso logo após a conclusão da inicialização.

Em seguida, insira temporariamente uma linha `createUser`. Essas diretrizes normalmente não são mantidas neste arquivo; você irá removê-las em instantes.

O usuário que você está criando será chamado de **bootstrap** e será usado como modelo para criar seu primeiro usuário real. Os pacotes do SNMP fazem isso através de um processo de clonagem das propriedades do usuário.

Ao definir um novo usuário, você deve especificar o tipo de autenticação (MD5 ou SHA), assim como fornecer uma senha que deve ter pelo menos oito caracteres. Caso esteja planejando usar criptografia para fazer a transferência, como fará neste tutorial, especifique também o protocolo de privacidade (DES ou AES) e, como opção, uma senha do protocolo de privacidade. Caso nenhuma senha de protocolo de privacidade seja fornecida, será usada a senha de autenticação para o protocolo de privacidade.

Adicione essa linha `createUser` ao final do arquivo:

/etc/snmp/snmpd.conf

```
...
createUser bootstrap MD5 temp_password DES
```

Agora que tem um novo usuário especificado, configure o nível de acesso que este usuário terá. Neste tutorial, você configurará este nível de acesso para seu usuário **bootstrap** e para o novo usuário que criará, chamado de **demo**. Você permitirá o acesso de leitura e a gravação deles usando a diretiva `rwuser` (outra alternativa é usar o `rouser` para acesso de somente leitura).

Você também aplicará o uso da criptografia, especificando `priv` após seu usuário. Caso quisesse restringir o usuário a uma parte específica do MIB, você poderia especificar o identificador de objeto (IDO) de mais alto nível ao qual o usuário deve ter de acesso ao final da linha.

Para fins deste tutorial, ambas as linhas serão como se segue:

/etc/snmp/snmpd.conf

```
...
rwuser bootstrap priv
rwuser demo priv
```

Quando terminar de fazer essas alterações, salve e feche o arquivo.

Para implementar essas alterações, reinicie o serviço `snmpd` em seu **agent server**:

```
$ sudo systemctl restart snmpd
```

Copy

O daemon do SNMP escutará conexões na porta `:161`. Configure o UFW para permitir conexões do **manager server** para essa porta:

```
$ sudo ufw allow from manager_server_ip_address to any port 161
```

Copy

Aprenda mais sobre o UFW em Como configurar um firewall com o UFW no Ubuntu 18.04.

Agora que o **agent server** está configurado, conecte-se ao seu **agent server** a partir do **manager server** para verificar a conexão.

Passo 4 – Verificando a autenticação para o servidor agente

Neste passo, você fará um teste para garantir que é possível se conectar com sua conta **bootstrap** ao **agent server**. No entanto, antes disso, este tutorial falará um pouco a respeito da estrutura geral de se enviar um comando do SNMP.

Ao usar o conjunto de ferramentas incluídas no pacote `snmp` (o conjunto de software `net-snmp`), existem alguns padrões na maneira como se deve chamar os comandos. A primeira coisa a fazer é autenticar-se ao daemon do SNMP que você deseja se comunicar. Normalmente, isso envolve fornecer algumas informações. As mais comuns são as seguintes:

- `-v`: este sinalizador é utilizado para especificar a versão do protocolo SNMP que você gostaria de usar. Este tutorial utilizará a v3.
- `-c`: este sinalizador é usado caso esteja utilizando a cadeia da comunidade no estilo SNMP v1 ou v2 para a autenticação. Como você está usando a autenticação baseada no usuário no estilo v3, não será necessário fazer isso.
- `-u`: este parâmetro é usado para especificar o nome de usuário que você deseja usar para se autenticar. Para ler ou modificar qualquer coisa usando o SNMP, você deve autenticar-se com um nome de usuário conhecido.
- `-l`: é usado para especificar o nível de segurança ao qual você está se conectando. Os valores possíveis são `noAuthNoPriv` para não ter autenticação e nem criptografia, `authNoPriv` para ter a autenticação, mas não ter criptografia e a `authPriv` para ter a autenticação e a criptografia. O nome de usuário que está usando deve ser configurado para operar no nível de segurança especificado, ou então a autenticação não será bem sucedida.
- `-a`: este parâmetro é usado para especificar o *authentication protocol* utilizado. Os valores possíveis são o `MD5` ou o `SHA`. Essa informação deve corresponder às informações especificadas quando o usuário foi criado.
- `-x`: este parâmetro é usado para especificar o *encryption protocol* utilizado. Os valores possíveis são `DES` ou `AES`. Essa informação deve corresponder às informações especificadas quando o usuário foi criado. Isso é necessário sempre que a especificação de privilégios do usuário tiver um `priv` depois dela, tornando a criptografia obrigatória.
- `-A`: é usado para fornecer a senha de autenticação especificada quando o usuário foi criado.
- `-X`: esta é a senha da criptografia especificada quando o usuário foi criado. Caso nenhuma senha tenha sido especificada, mas um algoritmo de criptografia tenha sido dado, será utilizada a senha de autenticação. Isso é necessário quando o parâmetro `-x` é dado ou sempre que a especificação de privilégios de um usuário tiver um `priv` depois dela, exigindo uma criptografia.

Ao usar essas informações, é possível construir seus comandos. Dado que você configurou seu usuário **bootstrap**, os comandos que você usará com essa conta se parecerão a este:

```
snmp_command -u bootstrap -l authPriv -a MD5 -x DES -A temp_password -X temp_password remote_
```

A partir de seu **manager server**, faça um teste para garantir que a conta **bootstrap** está disponível. Digite o seguinte para exibir as informações de sistema para o **agent server**:

```
$ snmpget -u bootstrap -l authPriv -a MD5 -x DES -A temp_password -X temp_password a
```

Copy e

A string `1.3.6.1.2.1.1.1.0` é a IDO responsável pela exibição das informações do sistema. Ela retornará o resultado do `uname -a` no sistema remoto.

Isso dará o seguinte resultado:

```
Output
SNMPv2-MIB::sysDescr.0 = STRING: Linux agent 4.15.0-66-generic #75-Ubuntu SMP Tue Oct 1 05:24
```

Agora que você verificou que é possível autenticar-se ao servidor executando o daemon do SNMP, continue para criar sua conta de usuário normal.

Passo 5 – Configurando a conta de usuário normal

Embora tenha especificado os privilégios para a conta de usuário **demo** no arquivo `snmpd.conf`, você ainda não criou este usuário. Neste passo, você utilizará o usuário **bootstrap** como modelo para seu novo usuário. Você fará isso usando a ferramenta `snmpusm`, usada para a gestão de usuários.

No **manager server**, é possível criar o usuário a partir do modelo, utilizando a ferramenta `snmpusm` e a seguinte sintaxe geral:

```
snmpusm authentication_info agent_server_ip_address create new_user existing_user
```

Usando o que sabe sobre os sinalizadores de autenticação que você precisa passar e aproveitando a conta de usuário que já tem (**bootstrap**), crie um usuário que corresponda aos privilégios do usuário que já definiu (**demo**).

O comando ficará parecido com este:

```
$ snmpusm -u bootstrap -l authPriv -a MD5 -x DES -A temp_password -X temp_password ag
```
Copy r

Você receberá a seguinte mensagem:

```
Output
User successfully created.
```

Agora, você tem um usuário totalmente funcional chamado **demo** em seu **agent server**. No entanto, ele ainda está usando as mesmas informações de autenticação da conta **bootstrap**. Para aumentar a segurança, modifique a senha para uma outra. Desta vez, você utilizará a conta **demo** para se autenticar. Lembre-se: senhas devem ter pelo menos oito caracteres:

```
$ snmpusm -u demo -l authPriv -a MD5 -x DES -A temp_password -X temp_password agent_s
```
Copy i

Você receberá a seguinte mensagem:

```
Output
SNMPv3 Key(s) successfully changed.
```

Teste suas novas credenciais e senha perguntando ao **agent server** quanto tempo o serviço do SNMP está funcionando. Será utilizado o comando `snmpget` para obter um valor único do **agent server**.

Desta vez,aproveite das definições extras do MIB baixadas para pedir o valor pelo nome, em vez da ID numérica IDO.

```
$ snmpget -u demo -l authPriv -a MD5 -x DES -A new_password -X new_password agent_se
```
Copy p

Você receberá um valor que representa a última vez que o daemon remoto do SNMP foi reiniciado:

```
Output
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53309) 0:08:53.09
```

Agora, você tem uma conta de usuário funcional chamada **demo**. No próximo passo, você simplificará o trabalho com os comandos do SNMP ao configurar o cliente.

Passo 6 – Criando um arquivo de configuração de Cliente

Neste ponto, você provavelmente notou que os detalhes de autenticação para todos os seus comandos do SNMP serão bastante estáticos em cada pedido. Em vez de digitá-los toda vez, é possível criar u

arquivo de configuração do lado do cliente que terá as credenciais às quais você está se conectando.

O arquivo de configuração de cliente pode ser colocado em dois locais diferentes, dependendo de como deseja compartilhá-lo.

Caso queira compartilhar suas credenciais de login com qualquer usuário válido em sua máquina de gerenciamento, você pode colocar seus detalhes de configuração no arquivo global `snmp.conf` no **manager server**. Será necessário abrir esse arquivo com privilégios do sudo:

```
$ sudo nano /etc/snmp/snmp.conf
```
Copy

No entanto, caso queira definir as credenciais de autenticação para apenas seu usuário, crie um diretório `.snmp` escondido dentro do diretório home do seu usuário no **manager server** e crie o arquivo lá:

```
$ mkdir ~/.snmp
$ nano ~/.snmp/snmp.conf
```
Copy

Independentemente de sua decisão sobre onde colocar sua configuração, o conteúdo será o mesmo.

Os comandos que você usará para autenticar estão na tabela a seguir. Na coluna da direita, é possível ver os nomes da diretiva usados para definir esses detalhes de configuração dentro do arquivo `snmp.conf`:

Sinalizador de comando	Descrição	Diretiva `snmp.conf` traduzida
`-u username`	O nome de usuário do SNMPv3 para se autenticar.	`defSecurityName username`
`-l authPriv`	O nível de segurança para se autenticar.	`defSecurityLevel authPriv`
`-a MD5`	O protocolo de autenticação que deve ser usado.	`defAuthType MD5`
`-x DES`	O protocolo de privacidade (criptografia) que deve ser usado.	`defPrivType DES`
`-A passphrase`	A senha de autenticação para o nome de usuário fornecido.	`defAuthPassphrase passphrase`
`-X passphrase`	A senha de privacidade do nome de usuário fornecido.	`defPrivPassphrase passphrase`

Ao usar essas informações, é possível construir um arquivo `snmp.conf` adequado. Para este guia, ele ficará parecido com isto:

snmp.conf

```
defSecurityName demo
defSecurityLevel authPriv
defAuthType MD5
defPrivType DES
defAuthPassphrase new_password
defPrivPassphrase new_password
```

Quando você terminar, salve e feche o arquivo.

Agora, é possível emitir comandos sem fornecer os detalhes de autenticação. Será necessário apenas o comando SNMP, o host e os argumentos do comando.

Em vez de digitar:

```
$ snmpget -u demo -l authPriv -a MD5 -x DES -A new_password -X new_password agent_se
```
Copy

Digite:

```
$ snmpget agent_server_ip_address sysUpTime.0
```
Copy

Como pode ver, isso reduz significativamente a quantidade de informações necessárias para se fornecer em cada pedido. A seguir, você removerá a conta **bootstrap** para reforçar a segurança da rede.

Passo 7 – Removendo a conta Bootstrap

Agora que sua conta normal está configurada corretamente, você pode remover a conta **bootstrap** não segura.

Em seu **agent server**, abra novamente o arquivo `/etc/snmp/snmpd.conf` com privilégios sudo.

```
$ sudo nano /etc/snmp/snmpd.conf
```
Copy

Encontre e deixe como comentário (ou remova) ambas as linhas adicionadas anteriormente que faziam referência ao usuário **bootstrap**:

/etc/snmp/snmpd.conf

```
...
#createUser bootstrap MD5 temp_password DES
#rwuser bootstrap priv
...
```

Salve e feche o arquivo.

Agora, reinicie o daemon do SNMP:

```
$ sudo systemctl restart snmpd
```
Copy

Isso cumprirá a recomendação de não ter diretivas do tipo `createUser` no arquivo `snmpd.conf` normal. Isso também removerá os privilégios desse usuário temporário.

Caso queira remover completamente o usuário **bootstrap** do `usmUserTable`, envie este comando pelo **manager server**:

```
$ snmpusm agent_server_ip_address delete bootstrap
```
Copy

Você receberá a seguinte resposta:

```
Output
User successfully deleted.
```

Conclusão

Neste ponto, você tem uma instalação de cliente-servidor totalmente configurada que consegue se comunicar com segurança usando o protocolo do SNMP. Agora, é possível adicionar daemons adicionais em outros hosts e configurar o acesso de conta em toda sua infraestrutura.

Para estudar mais a respeito das ferramentas do SNMP e como utilizá-las para recuperar valores um a um ou em massa, e como modificar dados, utilize nosso tutorial sobre Como utilizar o conjunto de ferramentas Net-SNMP para gerenciar e monitorar servidores.