AAA

HUAWEI TECHNOLOGIES CO., LTD.

Prefácio

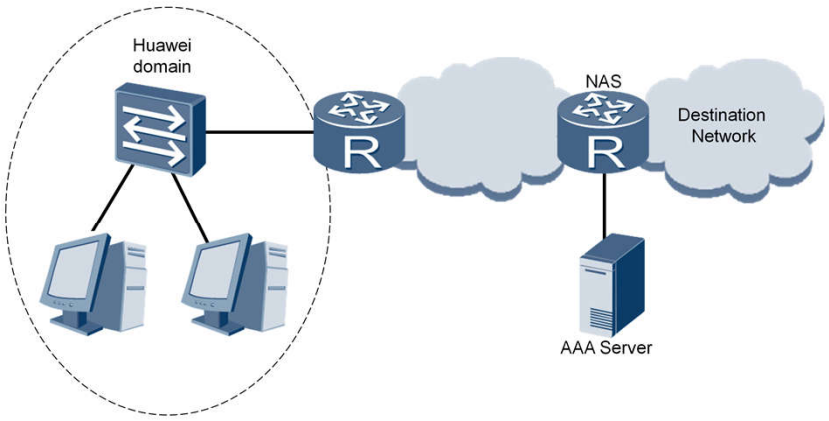
O AAA define uma arquitetura de segurança composta por três funções, denominadas Autenticação, Autorização e Contabilidade. Cada uma dessas funções representa um componente modular que pode ser aplicado como componente da estrutura de segurança implementada por uma empresa, e geralmente gerenciado através do uso de protocolos baseados em cliente / servidor, como RADIUS e HWTACACS. A implementação da arquitetura AAA como uma solução para funcionalidade aprimorada é introduzida para reforçar a estrutura geral de segurança da rede corporativa.

Objetivos

Após a conclusão desta seção, os estagiários serão capazes de:

- Descreva os esquemas da arquitetura de segurança AAA.
- Configure com êxito os esquemas de autenticação e autorização.

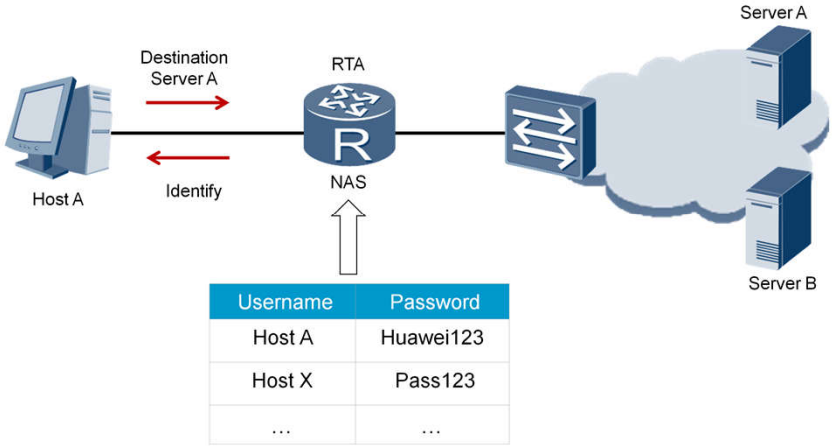
Aplicação AAA



- O AAA permite a autenticação, autorização e contabilidade de usuários que tentam acessar os recursos da rede de destino.

Autenticação, Autorização e Contabilidade (Authentication, Authorization, Accouting - AAA) é uma tecnologia usada para verificar se um usuário tem permissão para acessar uma rede, autorizando exatamente o que um usuário tem permissão para acessar e registrando os recursos de rede usados por um usuário. O VRP é capaz de suportar os serviços de autenticação e autorização AAA localmente dentro da série de roteadores ARG3, que é comumente referido como Servidor de Acesso à Rede ou NAS (Network Access Server); no entanto, os serviços de contabilidade geralmente são suportados por um servidor de contabilidade AAA externo. O exemplo aqui demonstra como os usuários considerados parte do domínio Huawei podem obter acesso aos recursos localizados na rede de destino exibida. O Network Access Server (NAS) opera como o dispositivo de gateway que pode executar autenticação e autorização de usuários ou oferecer suporte à autenticação e autorização de usuários do servidor AAA. No caso do servidor AAA, os usuários autenticados e autorizados a acessar a rede de destino também podem iniciar a contabilidade no servidor AAA pelo período de uma sessão ativa do usuário.

Autenticação



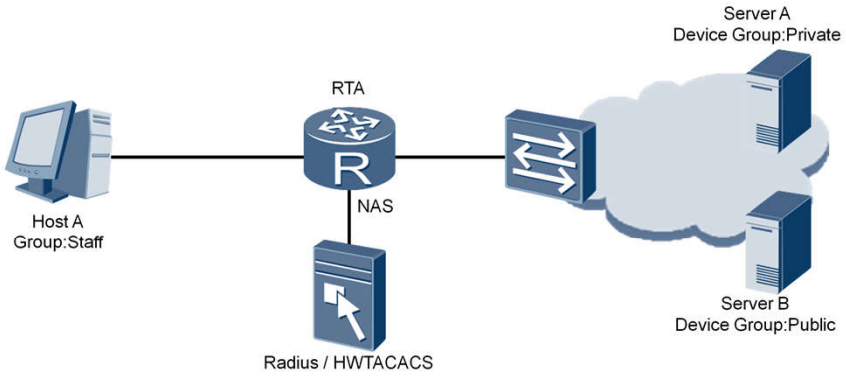
Username	Password
Host A	Huawei123
Host X	Pass123
…	…

- O acesso do usuário é gerenciado com base em um esquema de autenticação.

AAA suporta três modos de autenticação. A não-autenticação confia completamente nos usuários e não verifica sua validade. Isso raramente é usado por razões óbvias de segurança. A autenticação local configura as informações do usuário, incluindo o nome do usuário, a senha e os atributos dos usuários locais, em um servidor de acesso à rede (NAS). A autenticação local tem vantagens como processamento rápido e baixos custos operacionais. A desvantagem da autenticação local é o armazenamento limitado de informações devido ao hardware. A autenticação remota configura as informações do usuário, incluindo o nome do usuário, a senha e os atributos no servidor de autenticação. O AAA pode autenticar usuários remotamente usando o protocolo RADIUS (Remote Authentication Dial In User Service) ou o protocolo Huawei Terminal Access Controller System (HWTACACS). Como cliente, o NAS se comunica com o servidor RADIUS ou HWTACACS.

Se vários modos de autenticação forem usados em um esquema de autenticação, esses modos de autenticação entrarão em vigor na sequência com a qual os modos de configuração foram configurados. Se a autenticação remota foi configurada antes da autenticação local e se uma conta de logon existe no dispositivo local, mas não está disponível no servidor remoto, o AR2200 considera o usuário que está usando essa conta como tendo falhado em ser autenticado pela autenticação remota e, portanto, a autenticação local não é realizada. A autenticação local seria usada apenas quando o servidor de autenticação remota não respondesse. Se a não-autenticação estiver configurada, ela deverá ser configurada como o último modo para entrar em vigor.

Autorização

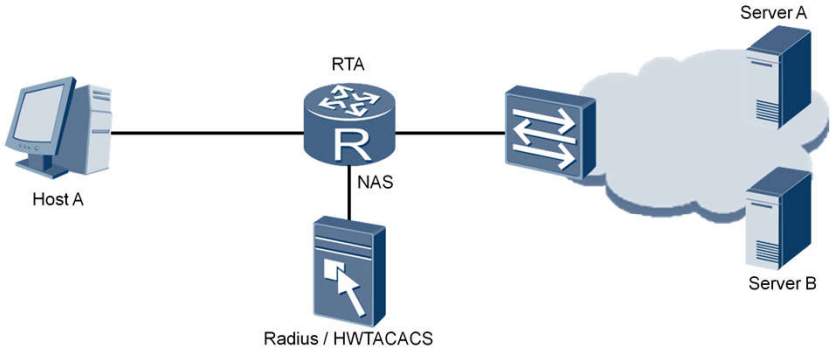


Device Group	User Group	Time	Privilege
Private	Admin	09:00-12:00	15
Public	Admin	09:00-18:00	15
Public	Staff	09:00-18:00	2

A função de autorização AAA é usada para determinar a permissão para os usuários obterem acesso a redes ou dispositivos específicos, pois o AAA suporta vários modos de autorização. No modo sem autorização, os usuários não estão autorizados. A autorização local, no entanto, autoriza os usuários de acordo com os atributos relacionados das contas de usuários locais configuradas no NAS. Como alternativa, o HWTACACS pode ser usado para autorizar usuários através de um servidor TACACS.

Um modo de autorização se autenticado pode ser usado onde os usuários são considerados autorizados no caso em que esses usuários podem ser autenticados no modo de autenticação local ou remota. A autorização RADIUS autoriza os usuários depois que eles são autenticados usando um servidor de autenticação RADIUS. A autenticação e a autorização do protocolo RADIUS são unidas, portanto, o RADIUS não pode ser usado para executar apenas autorização. Se vários modos de autorização estiverem configurados em um esquema de autorização, a autorização será executada na sequência em que os modos de configuração foram configurados. Se configurado, a não autorização deve ser o último modo a entrar em vigor.

Contabilidade

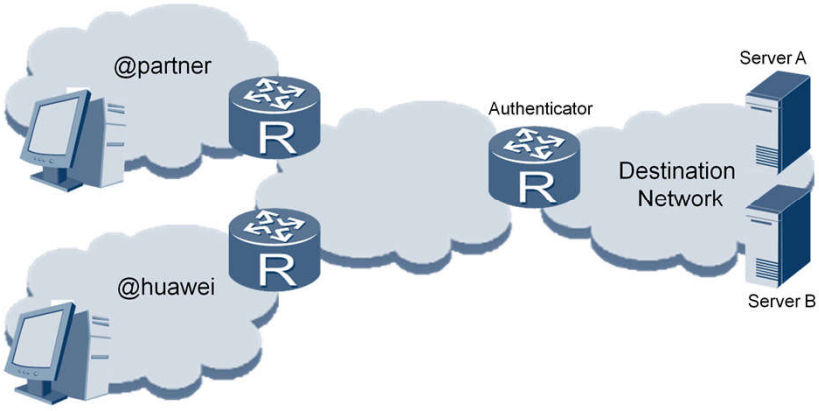


Login Time	Username	Uptime	Bandwidth Up/Down
May/01/2013 03:20:55	Host A	01:22:15	496.2KB / 21MB
Apr/16/2013 12:40:51	Host X	00:30:12	123KB / 1MB

O processo contábil pode ser usado para monitorar a atividade e o uso de usuários autorizados que obtiveram acesso aos recursos da rede. A contabilidade AAA suporta dois modos de contabilidade específicos. Não contábil pode ser usado e fornece serviços gratuitos para usuários sem nenhum registro de usuários ou logs de atividades.

A contabilidade remota, por outro lado, suporta a contabilidade usando o servidor RADIUS ou o servidor HWTACACS. Esses servidores devem ser usados para oferecer suporte à contabilidade devido ao requisito de capacidade de armazenamento adicional necessária para armazenar informações sobre logs de acesso e atividades de cada usuário autorizado. O exemplo demonstra uma representação muito geral de algumas das informações típicas normalmente registradas nos logs de contabilidade do usuário.

Domínios



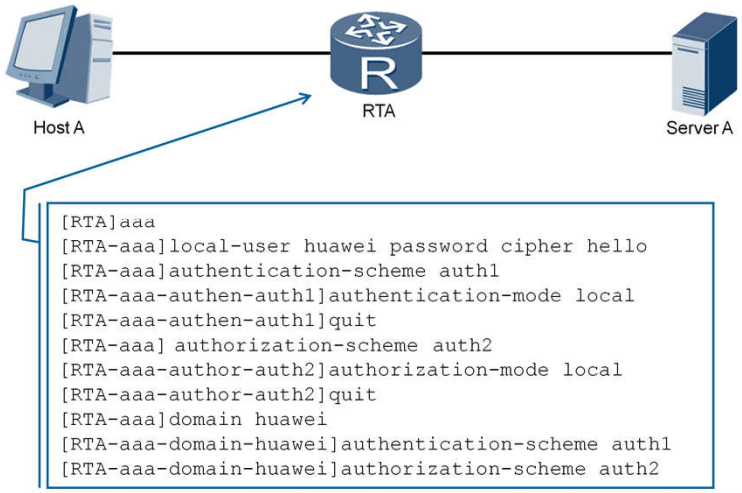
- Esquemas diferentes podem ser aplicados a usuários em domínios diferentes.

O dispositivo usa domínios para gerenciar usuários. Os esquemas de autenticação, autorização e contabilidade podem ser aplicados a um domínio para que o dispositivo possa autenticar, autorizar ou cobrar usuários no domínio usando os esquemas. Cada usuário do dispositivo pertence a um domínio. O domínio ao qual um usuário pertence é determinado pela cadeia de caracteres com o sufixo do delimitador de nome de domínio que pode ser @, | ou%.

Por exemplo, se o nome de usuário for user @ huawei, ele pertencerá ao domínio huawei. Se o nome do usuário não contiver um @, o usuário pertencerá ao domínio padrão denominado default no sistema. O dispositivo possui dois domínios padrão: padrão (domínio padrão global para usuários de acesso comum) e default_admin (domínio padrão global para administradores). Os dois domínios podem ser modificados, mas não podem ser excluídos.

Se o domínio de um usuário de acesso não puder ser obtido, o domínio padrão será usado. O domínio padrão é usado para usuários de acesso, como usuários de acesso NAC. A autenticação local é executada por padrão para usuários neste domínio. O domínio default_admin é usado para administradores como os que efetuam login usando HTTP, SSH, Telnet, FTP e terminais. A autenticação local é executada por padrão para usuários neste domínio. O dispositivo suporta no máximo 32 domínios, incluindo os dois domínios padrão.

Configuração de AAA Local



- Autenticação e autorização podem ser aplicadas no AR2200

HUAWEI

O roteador AR2200 pode ser usado como um servidor de acesso à rede (NAS) para implementar esquemas de autenticação e autorização. O exemplo demonstra o processo típico necessário para implementar com êxito o AAA local. Os usuários para autenticação devem ser criados usando o comando local-user <user-name> password [cipher \ simple] <password> nível de privilégio <level> comando. Este comando especifica um nome de usuário. Se o nome de usuário contiver um delimitador de nome de domínio como @, o caractere anterior a @ será o nome de usuário e o caractere depois de @ será o nome de domínio. Se o valor não contiver @, a cadeia de caracteres inteira será o nome de usuário e o nome de domínio será o domínio padrão.

Um esquema de autenticação é criado para autenticar usuários e deve ser criado antes que uma configuração adicional relevante à autenticação possa ser executada. O esquema de autenticação deve ser definido como local, radius, hwtacacs ou nenhum. Com exceção do parâmetro none, os outros modos de autenticação podem ser listados na ordem em que a autenticação deve ser tentada; por exemplo, o comando hwtacacs local no modo de autenticação deve ser usado e, se a autenticação HWTACACS falhar, o roteador AR2200 será usa a autenticação local. O esquema de autorização também deve ser criado para autorizar usuários (exceto no caso do suporte ao servidor Radius), criando um esquema de autorização que define o modo de autorização. O comando modo de autorização suporta modos para autorização hwtacacs, local, if-authenticated e none.

O comando domínio <nome de domínio> é usado para criar um novo domínio, e a implementação do esquema de autenticação <esquema de autenticação> e do esquema de autorização <esquema de autorização> na exibição de domínio aplicará os esquemas de autenticação e autorização para esse domínio.

Verificação da Configuração de AAA Local

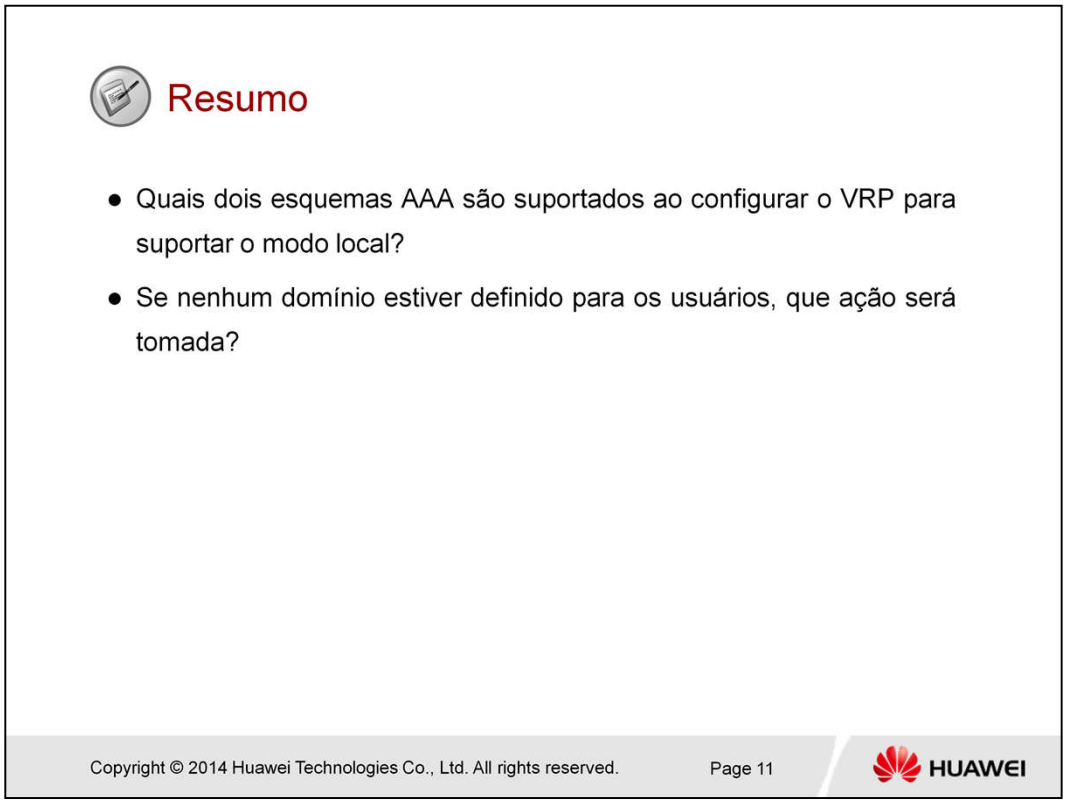
```
[Huawei]display domain name huawei
  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : auth1
  Accounting-scheme-name          : default
  Authorization-scheme-name       : auth2
  Service-scheme-name             : -
  RADIUS-server-template          : -
  HWTACACS-server-template        : -
  User-group                      : -
```

- Os esquemas AAA locais estão associados a domínios individuais.

A configuração do domínio AAA local e os esquemas para autenticação e autorização podem ser verificados por meio dos comandos domínio de exibição ou nome de domínio <nome de domínio>. O uso do comando display domain fornece informações breves sobre todos os domínios que foram criados, incluindo o nome do domínio e um índice de domínio usado para fazer referência a cada domínio criado.

O comando display domain name <domain-name> fornece detalhes de configuração específicos em referência ao domínio definido no parâmetro domain-name. Juntamente com o nome do domínio, está o estado do domínio que se apresenta como Ativo ou Bloco, em que o bloco se refere a um domínio que está no estado de bloqueio e impede que os usuários desse domínio possam efetuar login. Isso é implementado através de uma opção estado [ativo | bloco] implementado sob a visualização de domínio AAA. Um domínio está em um estado ativo após ser criado por padrão.

O nome do esquema de autenticação associa o esquema de autenticação criado ao domínio; o mesmo se aplica ao regime de autorização. O esquema contábil não está configurado localmente e, portanto, um esquema contábil não foi associado ao domínio criado e, como tal, o esquema contábil padrão é listado para o domínio por padrão. Caso a configuração não local (ou seja, RADIUS ou HWTACACS) seja implementada para oferecer suporte a serviços AAA, eles serão associados ao domínio nos campos de modelo de servidor.



1) A configuração do VRP no modo local suporta esquemas de autenticação e autorização; o esquema contábil requer o suporte do gerenciamento remoto através de um servidor HWTACACS ou RADIUS.

2) Se um usuário for criado sem definir o domínio ao qual ele pertence, ele será automaticamente associado ao domínio padrão, denominado padrão.

Thank you

www.huawei.com