Métodos de autenticação

As definições de autenticação de usuário controlam o processo de verificação de uma identidade reivindicada por um usuário para acessar o Archer.

Uma nova instalação do Archer é protegida por padrão (protocolo HTTPS ativado) com autenticação anônima. A autenticação anônima é suficiente para a maioria dos ambientes. Para os ambientes em que isso não é suficiente, são necessários métodos de autenticação mais sofisticados. A configuração de métodos de autenticação requer alterações em vários componentes do servidor, alguns dos quais estão fora do escopo do Archer.

um método de autenticação configurado incorretamente pode impedir que todo o Archer fique acessível.

Importante: Antes de fazer qualquer uma das alterações de configuração de autenticação abaixo, faça backup do arquivo web.config do Archer, do banco de dados de configuração e das configurações do IIS.

Nesta página

- Protocolo HTTPS/SSL
  - Configurar IIS para o protocolo HTTPS/SSL
  - Configurar o arquivo web.config da plataforma para o protocolo HTTPS/SSL
  - Configurar o arquivo web.config da API REST para o protocolo HTTPS/SSL
  - Configurar o Painel de controle do Archer para HTTPS/SSL
- Autenticação do Windows
  - Configurar o IIS para Autenticação do Windows
  - Configurar o arquivo web.config da plataforma para a Autenticação do Windows – HTTP
  - Configurar o arquivo web.config da plataforma para a Autenticação do Windows – HTTPS
- Ativando a autenticação do Kerberos
  - Configurar a autenticação do Windows para um único host

- Configurar a autenticação do Windows para vários hosts da Web no ambiente de balanceamento de carga
- Habilitando SSL para armazenamento em cache Redis

Protocolo HTTPS/SSL

O certificado para SSL deve estar disponível no componente Certificados do servidor (Nome da máquina > Certificados de servidor) no IIS. Quando o certificado estiver disponível, uma vinculação https que usa o certificado SSL deve ser adicionada ao site da Tecnologias da Archer.

Use as tarefas a seguir para configurar o IIS, os arquivos web.config e o Painel de controle do Archer para HTTPS/SSL.

se você precisar restaurar o HTTP após a configuração para o protocolo HTTPS/SSL, implemente o processo desfazendo todas as etapas de HTTPS/SSL.

Configurar IIS para o protocolo HTTPS/SSL

1. Selecione o site da plataforma no painel Conexões.
2. No painel Ações, clique em Vinculações.
3. Clique em Adicionar.
4. Na lista Tipo, selecione a opção https.
5. Na lista de certificação SSL, selecione o certificado aplicável.
6. Clique em OK.
7. Execute um destes procedimentos:
    - Para continuar sem remover a vinculação de site HTTP, vá para a próxima etapa.
    - Para remover a vinculação de site HTTP, faça o seguinte:
        a. Selecione a vinculação de site HTTP.
        b. Clique em Remover.
        c. Clique em Sim.
8. Clique em Fechar.
9. Execute uma redefinição do IIS.

Configurar o arquivo web.config da plataforma para o protocolo HTTPS/SSL

O Archer deve ser configurado para ser executado em HTTP ou HTTPS, não ambos. Edite o web.config do Archer no diretório base do site do Archer.

1. Localize a expressão **<!-- for HTTPS** e realize cada uma destas ações:
    - Substitua **httpGetEnabled** por **httpsGetEnabled="false"**.

    - Remova o comentário da linha **<security mode="Transport" />**.
    - Substitua o atributo **httpTransport** por **httpsTransport**.
4. Localize a expressão **<customHeaders>** e adicione cada uma das seguintes configurações em uma nova linha separada na seção de cabeçalhos personalizados:
    - <add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains" />
    - <add name="X-Content-Security-Policy" value="default-src 'self';" />
3. Clique em Salvar.
4. Execute uma redefinição do IIS.

Configurar o arquivo web.config da API REST para o protocolo HTTPS/SSL

O aplicativo IIS da API filho da API REST herda as propriedades do aplicativo Archer pai. Semelhante ao web.config da plataforma, o Archer deve ser configurado para ser executado em HTTP ou HTTPS, não ambos. Edite web.config da API REST no diretório API no diretório base do site do Archer.

1. Localize a expressão **<!-- for HTTPS**.
2. Substitua **httpGetEnabled** por **httpsGetEnabled="false"**.
3. Remova o comentário da linha **<security mode="Transport" />**.
4. Substitua o atributo **httpTransport** por **httpsTransport**.
5. Clique em Salvar.
6. Execute uma redefinição do IIS.

Configurar o Painel de controle do Archer para HTTPS/SSL

Todas as URLs no Painel de controle do Archer devem incluir HTTPS.

1. Abra o Archer Control Panel.
2. Em Gerenciamento de instâncias, clique duas vezes na instância que deseja configurar.
3. Clique na guia Web.
4. Altere todas as URLs de sites da Web da plataforma aplicáveis para incluir HTTPS.
5. Repita as etapas 2 a 4 para todas as outras instâncias.
6. Clique em Salvar todos.

Autenticação do Windows

O modo de autenticação deve ser definido como Autenticação do Windows no IIS; se a Autenticação do Windows não estiver disponível para seleção,

ela deverá ser instalada. Todos os outros modos de autenticação devem ser desativados.

Importante: A API REST não dá suporte à Autenticação do Windows. A Autenticação do Windows deve estar desativada para o aplicativo IIS da API filho e a Autenticação anônima deve ser habilitada novamente.

Importante: A pasta Web Service deve sempre ser definida como Autenticação Anônima.

Use as tarefas a seguir a fim de configurar o IIS e o arquivo web.config para os protocolos HTTP ou HTTPS do Windows.

Configurar o IIS para Autenticação do Windows

1. Selecione o site da plataforma no painel Conexões.
2. Selecione o recurso Autenticação.
3. Defina a Autenticação do Windows como Habilitada.
4. Desative todos os outros modos de autenticação, por exemplo, anônimo.
5. Execute uma redefinição do IIS.

Configurar o arquivo web.config da plataforma para a Autenticação do Windows – HTTP

Edite o arquivo web.config do Archer no diretório base do site do Archer.

1. Localize a expressão <!-- For Windows Authentication, change mode to 'Windows'.
2. Substitua <authentication mode="None" /> por <authentication mode="Windows" />.
3. Localize a expressão <!-- For Windows Authentication, and uncomment the lines.
4. Remova comentários das linhas relacionadas a <authorization><allow users="*" /></authorization>.
5. Localize a expressão <!-- For Basic Authentication (without SSL), and uncomment the lines.
6. Remova comentários das linhas relacionadas ao modo de segurança.
7. Localize a expressão <!-- for Windows Integrated Authentication, and add authenticationScheme="Negotiate".
8. Conforme for instruído, adicione authenticationScheme="Negotiate" /> a httpTransport ou httpsTransport.
9. Clique em Salvar.
10. Execute uma redefinição do IIS.

Configurar o arquivo web.config da plataforma para a Autenticação do Windows – HTTPS

Edite o web.config do Archer no diretório base do site do Archer.

1. Abra o arquivo web.config em um editor de texto.
2. Localize a tag <authentication mode> e altere o modo de autenticação de Nenhum para Windows.
3. Localize as tags <authorization> e <allow users> e remova os comentários.
4. Localize a tag <serviceMetaData> e altere o identificador de HTTP para HTTPS.
5. Localize a seção <webHttpBinding>.
6. Remova os comentários das tags <security mode> and <transport> identificadas para Autenticação do Windows e altere o modo de segurança da seguinte maneira:

   <security mode="Transport">

   <transport clientCredentialType="Windows" />

   </security>

7. Localize a marca <httpTransport> para binaryHttpBinding.
8. Adicione o atributo authenticationScheme="Negotiate" à tag e ao identificador HTTPS.

   <httpTransport maxReceivedMessageSize="1024000000" maxBufferSize="1024000000" authenticationScheme="Negotiate" />

9. Localize a tag <httpTransport> para a vinculação binaryHttpBindingStreaming binding.
10. Adicione o atributo authenticationScheme="Negotiate" à tag e ao identificador HTTPS.

    <httpsTransport transferMode="StreamedRequest" maxReceivedMessageSize="1024000000" maxbufferSize="1024000000" authenticationScheme="Negotiate" />

11. Localize a tag <location> e remova os comentários.
12. Salve o arquivo web.config
13. Execute uma redefinição do IIS.

Ativando a autenticação do Kerberos

Use as tarefas a seguir para configurar a autenticação do Windows para um ou vários hosts da Web.

Configurar a autenticação do Windows para um único host

Se ele ainda não existir, um SPN (Service Principal Name, nome principal do serviço) de HTTP deverá ser registrado primeiro com o domínio por um administrador de domínio. Use o comando a seguir para fazer isso:

Setspn -S HTTP/{URL do Archer} {identidade do pool de aplicativos}

Por exemplo, Setspn -S HTTP/all.archer.local archer.local\Administrator é o comando para injetar uma adição de SPN no domínio se ocorrer o seguinte:

- Archer é instalado no site padrão.
- A URL do Archer é https://all.archer.local.
- A identidade do Archer Application Pool é: archer.local\Administrator.

Se o Archer estiver instalado no site do RSAArcher — localizado dentro do site padrão — o comando para injetar será Setspn -S HTTP/all.archer.local archer.local\Administrator.

1. Abra o Microsoft IIS.
2. Selecione o site do Archer (padrão ou não).
3. Selecione a autenticação.
4. Habilite a autenticação do Windows.
5. Selecione Configurações avançadas.
6. Desmarque Habilitar autenticação do modo kernel e clique em OK.
7. Selecione Provedores.
8. Selecione Negociar: Kerberos no menu drop-down Provedores disponíveis.
9. Clique em Adicionar.
10. Mova Negociar Kerberos para a ordem desejada em Provedores habilitados e clique em OK.

    Certifique-se de que essas etapas tenham sido concluídas pelo menos no local do Archer. Essas etapas também podem precisar ser realizadas para os componentes padrão de nível de servidor e site no IIS, dependendo de suas necessidades.

11. Execute uma redefinição do IIS.

Configurar a autenticação do Windows para vários hosts da Web no ambiente de balanceamento de carga

Quando o IIS é executado em ambientes de carga balanceada ou em cluster, os aplicativos são acessados usando o nome de cluster em vez de um nome de nó. Esse cenário inclui o balanceamento de carga de rede.

Na tecnologia de cluster, um nó se refere a 1 computador que seja membro do cluster.

Para usar o Kerberos como protocolo de autenticação, a identidade do pool de aplicativos em cada nó de IIS deve ser configurada para usar a mesma conta de usuário do domínio. Para configurar cada nó de IIS para usar a mesma conta de usuário do domínio, use o seguinte comando:

Setspn –A HTTP/CLUSTER_NAME domain\username

Por exemplo, o comando pode exibe o seguinte resultado:

Setspn –A HTTP/www.myIISCluster.com mydomain\appPool1

1. Abra o Microsoft IIS.
2. Selecione o site do Archer (padrão ou não).
3. Selecione a autenticação.
4. Habilite a autenticação do Windows.
5. Selecione Configurações avançadas.
6. Desmarque Habilitar autenticação do modo kernel e clique em OK.
7. Selecione Provedores.
8. Selecione Negociar: Kerberos no menu drop-down Provedores disponíveis.
9. Clique em Adicionar.
10. Mova Negociar Kerberos para a ordem desejada em Provedores habilitados e clique em OK.

    Certifique-se de que essas etapas tenham sido concluídas pelo menos no local do Archer. Essas etapas também podem precisar ser realizadas para os componentes padrão de nível de servidor e site no IIS, dependendo de suas necessidades.

11. Execute uma redefinição do IIS.

Habilitando SSL para armazenamento em cache Redis

A versão Redis Enterprise oferece suporte a SSL. A versão de código aberto do Redis não oferece suporte à criptografia sem um manipulador.