21 de outubro de 2013

Perguntas Frequentes sobre o Serviço de Dados de Zona Centralizado

Durante o ICANN 47, em Durban, a equipe fez uma apresentação sobre o Serviço de Dados de Zona Centralizado (na época conhecido como CZDAP), a solução da ICANN para o escalonamento da provisão de dados de zona enquanto centenas de novos gTLDs são adicionados à Internet. Durante a sessão, recebemos algumas respostas que não pudemos avaliar devido à falta de tempo. Seguem abaixo as respostas para essas perguntas e várias outras recebidas sobre o CZDS. Perguntas e respostas adicionais podem ser acessadas pelas páginas de ajuda: https://czds.icann.org/en/help

Usuário final

P: O usuário poderá alterar o endereço IP que ele usa para o acesso?

R: Sim, na seção do perfil do usuário você pode identificar um ou mais endereços IP com os quais pretende acessar os servidores SFTP.

P: Se um usuário final tiver acesso a vários TLDs (por exemplo, 1.400), ele/ela precisa fazer o download de cada arquivo de dados individualmente?

R: Não, criamos a CZDS API que é um sistema baseado em token que permite o download em lote de credenciais de SFTP. O token garante que o acesso seja automatizado, permitindo que as pessoas obtenham novos dados de zona sem fazer login manualmente. Caso seja detectada a presença de abuso, a expiração do token (feita pelo admin do CZDS ou pelos próprios usuários do Operador de Registro) impedirá que qualquer script conclua outros downloads até que o novo token de usuário válido seja incluído no script.

As ferramentas para o download em lote de credenciais de SFTP já existem. Todas as informações sobre as ferramentas podem ser encontradas no repositório open source em:

https://github.com/fourkitchens/CZDS-tools

P: Pode ser interessante haver uma página de downloads que mostre todos os arquivos aos quais tenho acesso, em vez de que seja necessário acessar cada página individualmente. Deveria haver uma página com uma lista de todos os TLDs aos quais tenho acesso e alguns metadados anexados a ela. Por exemplo, quando foi feita a última atualização pelo Registro e outras informações que veríamos no FTP. Deveria haver uma conta de FTP onde eu pudesse ver todas as informações.

R: Esse recurso não está disponível no momento.

P: Há a possibilidade de ser disponibilizado algum tipo de dados históricos? Por exemplo, da última semana, das últimas quatro semanas.

R: Esse recurso não é oferecido pelo sistema.

P: Há alguma maneira de contestar a negação de um Registro?

R: O Contrato de Registro exige que um registro de gTLD ofereça os dados de zona sem custos para o consumidor dos dados. Se um usuário final acreditar que o registro está negando acesso de maneira indevida ou não recebe uma resposta do registro, ele poderá registrar uma reclamação com o departamento de Conformidade da ICANN, que entrará em contato com o registro e fará uma investigação.

P: Quando os Registros de novos gTLDs serão obrigados a começar a fornecer os dados de zona? Após a assinatura do contrato, a delegação técnica ou isso ainda não foi decidido?

R: Os Registros de novos gTLDs são obrigados a começar a fornecer os dados de zona após a delegação.

P: Como o Registros colocam seus dados de zona no sistema CZDS? Upload por FTP ou transferência de zona?

R: Existem duas opções: o Operador do Registro pode controlar os dados simplesmente aprovando o acesso e fornecendo aos usuários as credenciais de acesso (via CZDS) ao servidor SFTP deles ou permitir que a ICANN faça transferências periódicas de zona (AXFR) e configure os dados em nome do Operador de Registro, que seriam depois disponibilizados aos usuários para download diretamente por meio do sistema CZDS.

P: Se um Operador de Registro optar por fornecer acesso a zonas por meio de sistemas próprios, em vez de por meio do método de download direto pelo sistema do Serviço de Dados de Zona Centralizado, como seria esse processo?

R: O Operador do Registro deverá escolher “credenciais de SFTP” como seu método de download. Quando um usuário final fizer uma solicitação, o Operador do Registro aprovará a solicitação e fornecerá ao usuário final as credenciais de login e o nome do servidor SFTP. O usuário final pegará os dados no host especificado informando no CZDS o nome de usuário e a senha fornecidos a ele.

Antes de armazenar as credenciais, o site do CZDS as criptografará usando a chave pública de cada usuário individualmente.

P: Como os Operadores de Registro devem fornecer o arquivo de zona ao CZDS? Os arquivos devem ser enviados por uma API, descompactados?

R: O Operador de Registro fornecerá a chave TSIG e o endereço do servidor ao admin do CZDS e/ou autorizará transferências (AXFR) pela lista de endereços IP designados da ICANN. A ICANN realizará a transferência e entregará os dados no formato especificado para download direto via CZDS pelo usuário final.

P: Os registros de novos gTLDs são obrigados a fornecer dados de zona ao sistema?

R: Sim. Os registros de novos gTLDs são obrigados (de acordo com a Especificação 4, Seção 2 do Contrato de Registro de gTLDs) a fornecer os dados de zona aos usuários finais que os solicitarem. Os registros de novos gTLDs também são obrigados a usar o CZDS. Isso pode ser feito permitindo que a ICANN realize as transferências dos dados de zona ou fornecendo o nome do servidor SFTP com as credenciais para o usuário pegar os dados fora do sistema.

P: Enquanto um futuro Registro, posso aprovar todas as solicitações automaticamente?

R: Você poderá aprovar todas as solicitações de uma só vez. Para isso, basta selecionar todas as solicitações e clicar em aprovar. No entanto, no momento não é possível "pré-aprovar" todas as solicitações por padrão. A ICANN analisará a possibilidade de adicionar esse recurso de aprovação automática em versões futuras.

P: Como o Operador de Registro descobre que há uma solicitação pendente para ser aprovada ou negada?

R: O Operador de Registro pode ativar ou desativar o recurso de notificações por e-mail. Com esse recurso, ele poderá ser notificado sempre que houver uma nova solicitação. No entanto, se o volume de mensagens for muito grande, é possível desativar o recurso. Nesse caso, o Operador de Registro precisará fazer login periodicamente e verificar se há novas solicitações.

P: Já que os Operadores de Registro precisam liberar o arquivo de zona antes de assinar o Contrato de Registro, não seria melhor usar a opção "aprovar" por padrão?

R: Para ser exato, um novo Operador de Registro é obrigado a fornecer os dados de zona *após* a assinatura do Contrato de Registro, mediante a delegação, e não *antes* de assinar o Contrato de Registro. O recurso de pré-aprovação automática não está disponível no momento.

P: Não quero precisar fazer login todos os dias para aprovar solicitações. Seria bom se tivéssemos a opção de pré-aprovação ou aprovação automática de tudo.

R: Os Operadores de Registro não são obrigados a fazer login todos os dias para fazer aprovações, mas são responsáveis por validar as solicitações dos usuários finais. A regra de 24 horas significa que os Operadores de Registro devem fazer upload dos dados de zona a cada 24 horas, e esse processo pode ser automatizado.

P: Há alguma expectativa quanto à rapidez de resposta dos Registros às solicitações? O departamento de Conformidade da ICANN vai supervisionar isso?

R: Não é exigido um tempo de resposta específico, mas espera-se que os Registros respondam dentro de um prazo razoável. O departamento de Conformidade Contratual da ICANN exigirá o cumprimento do requisito de fornecer acesso aos dados de zona.

P: O Operador de Registro precisa aprovar todas as solicitações aos dados de zona? Por exemplo, é possível o .veryprivate, que não concorda com o conceito de compartilhar esses dados por padrão, negar todas as solicitações?

R: O Contrato de Registro de novos gTLDs básico exige que os Registros ofereçam acesso aos arquivos de zona. Existem certas condições com base nas quais eles podem negar solicitações. Consulte o Contrato de Registro para ver as condições em que os Operadores de Registro podem negar uma solicitação de acesso a arquivos de zona.

P: Se um usuário final fizer várias solicitações de dados, e o Operador de Registro revisar e aprovar pelo menos uma dessas solicitações, o Operador de Registro terá a opção de aprovar todas as outras solicitações desse usuário de uma só vez?

R: Os Operadores de Registro deverão aprovar cada solicitação de TLD dos usuários individualmente. Cada aprovação tem uma validade de 90 dias, ou mais, se o Registro preferir.

P: Há alguma punição por *não* aprovar o acesso a dados de zona?

R: Consulte o Contrato de Registro para ver essas informações.

P: Se um Operador de Registro gerenciar vários TLDs, quantas contas, com conjuntos diferentes de credenciais de login, serão necessárias para gerenciar as solicitações de acesso aos dados de zona de todos os TLDs dele?

R: Uma conta no CZDS deverá representar exatamente um indivíduo até que outra política seja especificada. Uma conta individual poderá administrar vários TLDs. O CZDS inclui recursos que permitem aos usuários e superusuários do Operador de Registro receberem autorização para negociar termos e condições em nome de todos os TLDs associados a um Registro atribuído. Os detalhes específicos para cada "superusuário" dependem das decisões corporativas de cada Registro. Por exemplo, os Operadores de Registro podem atribuir um ou muitos usuários de Operador de Registro para gerenciar o acesso aos dados de zona para vários TLDs sob seu controle, dependendo do volume.

P: É possível haver mais de um contato do Operador de Registro?

R: Sim, o recurso de superusuário permite a um Operador de Registro atribuir ou acrescentar outros usuários de Operador de Registro para gerenciar um TLD. O superusuário precisa confirmar se os Operadores de Registro indicados por ele têm a autoridade para negociar termos e condições em nome do Registro.

P: Enquanto um portfólio de Registros, um Operador de Registro poderá fazer login e ver todo o conteúdo anexado ou serão necessários vários logins?

R: Depois que um usuário de Operador de Registro estiver associado a um Registro, ele verá todas as solicitações para os TLDs gerenciados por ele com apenas um login.

P: Se eu indicar alguém como superusuário, como poderei supervisionar o trabalho dessa pessoa? Por exemplo, e se eu fizer login, ver que tenho cinco registros, indicar o meu admin para assumir essa função para os cinco registros, e ele "aprovar todos" e sair da empresa em seguida?

R: Se o usuário de Operador de Registro designado sair da empresa, o superusuário poderá atribuir esses registros a um usuário final, em vez de a um usuário de Operador de Registro. Ele não poderá aprovar mais solicitações, mas tudo que já foi aprovado será válido até o vencimento dos termos e das condições. Se todas as solicitações foram aprovadas por engano, é possível revogar uma ou mais ou todas as solicitações. Desse modo, os usuários finais teriam que fazer login e solicitar acesso novamente.

P: Há planos para implementar um sandbox, tanto para a versão SFTP quanto HTTP?

R: Não há planos para implementar um sandbox. Os Registros poderão trabalhar em parceria com o admin do CZDS para se ajustarem adequadamente no sistema e testar as transferências de arquivos de zona. A ICANN ajudará a garantir que tudo funcione perfeitamente antes que o Operador de Registro comece a aprovar solicitações de usuários finais.

P: Os termos e condições substituirão o acordo de acesso a arquivos de zona?

R: Sim. Na verdade, o texto dos termos e condições foi tirado diretamente dos atuais acordos de arquivos de zona.

P: Enquanto Registros, podemos criar nossos próprios Termos e Condições? Se isso for possível, poderemos criar versões diferentes para cada um de nossos TLDs?

R: A Seção 2.1.1 da Especificação 4 do Contrato de Registro de novos gTLDs determina que o acordo de acesso a arquivos de zona "será padronizado, simplificado e administrado por um Provedor de Acesso a Dados de Zona Centralizado".

P: Se um registro detectar abuso por parte de um usuário, qual é o processo para notificar a ICANN?

R: O Operador de Registro poderá revogar o acesso de um usuário por violação do acordo de acesso entre o usuário e o Operador de Registro. Dúvidas ou comentários sobre o sistema CZDS deverão ser encaminhados para CZDS@icann.org.

Segurança

P: “Como o CZDS utiliza a criptografia de chaves públicas?” O que faz a chave de download inicial? Os dados são ASCII e legíveis, por que esses dados precisam ser criptografados? Por que não usar HTTPS, por exemplo?

R: O HTTPS protege a confidencialidade das informações, nesse caso, as credenciais de acesso aos servidores de arquivos de zona, do servidor para o cliente, ou seja, entre duas partes. No entanto, o CZDS envolve três partes: o operador de registro, o usuário do arquivo de zona e o operador do CZDS, que atua como um intermediário. O uso de HTTPS protegeria apenas as informações de uma parte para a outra, mas não a cadeia inteira de comunicação entre duas partes por meio do intermediário. Ao usar a criptografia de chaves públicas, podemos garantir a privacidade do operador de registro com o usuário do arquivo de zona. O operador do CZDS (o intermediário) não terá acesso às credenciais.

O site do CZDS gera um par de chaves RSA de 2048 bits (não PGP). Tanto as chaves públicas quanto privadas são geradas no servidor da Web do CZDS. A chave privada é enviada via HTTPS para o usuário fazer o download dela. Depois, ela será destruída e nunca gravada no disco, na sessão do navegador ou em qualquer mecanismo que armazene dados. A chave pública é armazenada com os outros dados de perfil do usuário no site do CZDS. Esse par de chaves (a chave privada armazenada pelo usuário e a chave pública armazenada no CZDS) é necessário para descriptografar as credenciais de SFTP. O HTTPS não é usado para proteger as credenciais contra a exposição por terceiros.

O CZDS gera um par de chaves privada e pública. A chave *pública* permanece no servidor (assim como uma chave SSH pública permanece em um servidor) e, embora a intenção não seja revelá-la publicamente, se a chave fosse de alguma forma disponibilizada ao público, isso seria um evento de segurança menos crítico. Sendo assim, ela é armazenada no banco de dados. Enquanto isso, após a criação do par de chaves, a chave *privada* é enviada ao usuário em uma operação única (ela é transmitida juntamente com a página da Web que contém instruções para fazer o download da chave). O usuário deverá fazer o download dessa chave e guardá-la em um lugar seguro. Quando os usuários acessam a página que contém a chave, uma mensagem bastante enfática é exibida aconselhando-os a manter a chave em um lugar seguro.

Se o usuário sair da página que contém a chave privada sem fazer o download dela, ele não poderá mais fazer a descriptografia das credenciais e precisará gerar um novo par de chaves privada/pública, que é um procedimento fácil de ser realizado na interface do CZDS. Nos casos em que o usuário tentar gerar uma nova chave e já houver uma chave pública armazenada em sua conta, a interface exibirá uma mensagem antes de sobrescrever a chave pública existente (para que a chave válida não seja sobrescrita por acidente).

Para a descriptografia, o usuário fornecerá sua chave *privada* para a página da Web que contém as credenciais criptografadas, que serão descriptografadas por JavaScript, a linguagem de programação do cliente de todos os navegadores da Web. A chave privada NÃO é enviada ao servidor durante essa operação. A descriptografia é realizada no computador de cada usuário.

Há um token SEPARADO (para acesso à API) que é *totalmente dissociado* das chaves de criptografia/descriptografia. O token de API permite aos usuários fazerem o download das credenciais de SFTP, e não participa de nenhuma maneira no processo de descriptografia. O token de API é um recurso opcional do CZDS, e é possível que alguns usuários nem sequer criem um.

P: Se a chave privada RSA é usada para descriptografar as credenciais de SFTP e essa chave de API fornece acesso em lote a essas credenciais de SFTP, isso significa que o sistema de API ignora a criptografia de RSA das credenciais? Ou as credenciais precisarão ser descriptografadas "fora de banda"?

Não. A API não ignora a descriptografia. Nenhuma parte do sistema ignora a descriptografia porque as credenciais nunca são armazenadas em texto simples, e a chave privada necessária para a descriptografia nunca é armazenada no servidor.

Outros

P: Se houver uma alteração nos termos e condições, qual mecanismo será utilizado para notificar o usuário final? Haverá alguma consequência para o usuário final se ele não reconhecer a alteração nos termos, como negar o acesso aos dados, por exemplo?

R: Sempre que os termos e condições forem alterados ou atualizados, o Operador de Registro poderá revogar o acesso de todos os seus usuários, de modo que eles precisarão fazer novo login e solicitar novamente o acesso aos arquivos de zona de acordo com os novos termos. Caso contrário, o usuário final permanecerá vinculado às obrigações dos termos e condições acordados para cada TLD individualmente. É importante observar que a revogação do acesso no sistema CZDS não negará acesso automaticamente para um usuário final que estiver acessando os dados de zona via SFTP. O Operador de Registro terá o controle externo ao CZDS para alterar as credenciais dos usuários que foram revogadas ou estão expiradas no sistema.

P: Quais elementos de dados são fornecidos no CZDS?

R: Os arquivos de zona de TLDs contêm uma lista de nomes de domínio registrados e ativos para um determinado registro. Eles também contêm outras informações do DNS usadas pelos registros dependendo dos serviços oferecidos por eles. O formato de um arquivo de zona é definido na RFC 1035 e em RFCs posteriores. O formato exigido dos arquivos de zona distribuídos pelo CZDS é, na verdade, um subconjunto dessas RFCs, conforme definido pelo Grupo Consultivo sobre o Acesso a Arquivos de Zona na sua Proposta Estratégica, página 9, seção 5.1.7, e incluído na Especificação 4 do Contrato de Registro.

P: De quem são os endereços IP que vocês acessam e eles são obtidos por meio do sistema DNS? Como isso é exibido, como está sendo feito e como é feita a associação?

R: O endereço IP do usuário final é fornecido pelo usuário ao criar seu perfil do usuário e, em seguida, repassado ao Operador de Registro.

P: Se um usuário fizer o download de dados de um Registro, o Registro verá o histórico das pessoas que utilizam esses dados?

R: O Operador de Registro tem um histórico de solicitações por usuário, mas não um histórico de downloads feitos pelo usuário. É possível implementar downloads diretos no sistema CZDS, mas esse recurso não está disponível no momento.

P: A aprovação é concedida por solicitação de download ou por acesso para o TLD?

R: Por TLD. O acesso é concedido uma vez a fim de obter os dados de zona para o TLD no período estabelecido nos termos e condições (no mínimo 90 dias ou de acordo com a preferência do Registro). Após o vencimento dos termos e condições, o usuário deverá solicitar acesso novamente.

P: Precisamos de especialistas no assunto para conseguirmos automação total desse sistema e implementá-lo de acordo com a escala. E quanto aos jogos? Com que frequência posso fazer downloads? Seria ótimo se tivéssemos acesso por meio de um só botão.

R: Há um requisito nos termos e condições que limita o número de vezes que um usuário final pode acessar os arquivos de zona (uma vez a cada 24 horas). O upload dos arquivos é feito a cada 24 horas. Então, se um usuário final fizer mais de um download por dia, ele não verá informações novas. Além disso, os usuários não podem fazer downloads diretos no CZDS mais de três vezes a cada 24 horas por TLD. Se eles tentarem fazer isso, uma mensagem de erro será exibida.