Entender o gerenciamento centralizado de registros guarda-chuva com o serviço S3 da Amazon para clientes MSP, MSSP e de várias organizações

Contents

Introdução

Este documento descreve o gerenciamento centralizado de logs Umbrella com o serviço S3 da Amazon para clientes MSP, MSSP e multi-org.

Overview

Os consoles MSP, MSSP e Multi-org têm a capacidade de armazenar os logs de DNS, URL e IP de seus clientes off-line no armazenamento em nuvem. O armazenamento está no Amazon S3 e, após os logs serem carregados, eles podem ser baixados e mantidos por razões de conformidade ou análise de segurança.

Esta documentação ajuda você a entender esse recurso, configurá-lo no painel do Umbrella e no console Amazon S3, e executar através de várias opções de configuração, incluindo a duração de

tempo que você gostaria que os logs fossem mantidos no S3.

O Umbrella para MSP, MSSP e Multi-Org todos têm a capacidade de carregar os logs de atividade de tráfego das organizações filhas do console e armazenar esses logs na nuvem. O AWS S3 da Amazon (Simple Storage Service) é o serviço que arquiva logs e às vezes é chamado de armazenamento off-line ou de retenção de log.

O arquivamento de registros pode ser útil por vários motivos, dependendo da sua necessidade. Para algumas pessoas, os logs exportados e arquivados podem ser importados para ferramentas de análise de dados ou de segurança forense, como SIEMs. Para outros, um arquivo de registros de atividades pode ser útil para análise de dados em caso de um incidente de segurança ou registros de recursos humanos.

O AWS S3 armazena logs em um arquivo compactado (gzip) em formato CSV. Como os logs são carregados a cada dez minutos, há um atraso mínimo de dez minutos entre o tráfego de rede que vem de sua rede, registrado pelo Umbrella e disponibilizado para download do S3.

O número orgID do Console

Cada organização do cliente faz upload de seus logs individualmente, usando o número orgID da Console para mapear cada cliente para uma pasta. O recurso também pode ser ativado ou desativado por cliente/por organização.

Dois tipos de gerenciamento de registros de guarda-chuva

O gerenciamento de logs é realizado por meio do upload de logs para o que é chamado de it isbucketit (essencialmente uma pasta dentro do ambiente AWSit é S3). Há duas maneiras de hospedar um bucket para os logs do Umbrella:

- Administrado, gerenciado e pago por você, o administrador da empresa.
- Administrado, gerenciado e pago pelo Cisco Umbrella.

Há prós e contras em ter a Cisco gerenciando seu S3 bucket.

Os prós da Cisco no gerenciamento do seu bucket:

- Extremamente fácil de configurar. Leva apenas alguns minutos e depois é extremamente fácil de gerenciar.
- O gerenciamento de balde da Cisco está incluído no custo da licença com a Umbrella, tornando o serviço efetivamente gratuito. Embora seja barato ter seu próprio período, o custo indireto de gerenciar outra conta pode ser proibitivo.

Os prós do gerenciamento de uma instância do S3:

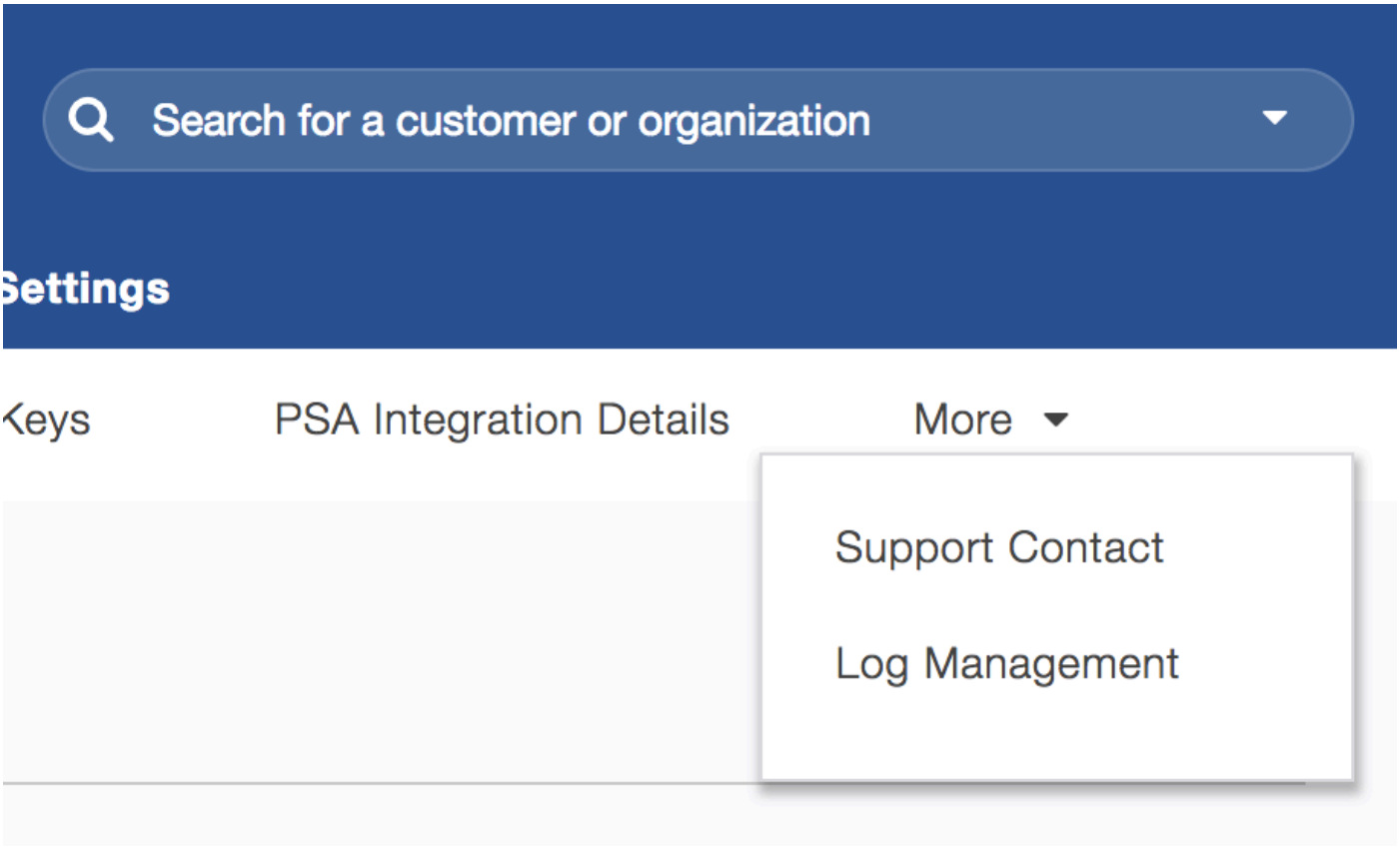
- Não há limitação quanto ao tempo em que os dados podem ser armazenados off-line. A Cisco limita o armazenamento off-line a no máximo 30 dias.
- Você pode adicionar qualquer coisa ao seu bucket, incluindo arquivos de log do Umbrella, para que o bucket possa ser usado por outros aplicativos também.
- Você pode obter suporte diretamente da Amazon para assistência de configuração

avançada, como automação ou ajuda com linha de comando.

Para a maioria dos clientes, o custo de manutenção de um balde é muito barato, mas pode ser um incômodo.

Getting Started

O recurso Gerenciamento de logs pode ser encontrado no Console em Configurações > Gerenciamento de logs (você pode pressionar a seta suspensa).



115012963103

Configuração de um compartimento de memória S3 autogerenciado

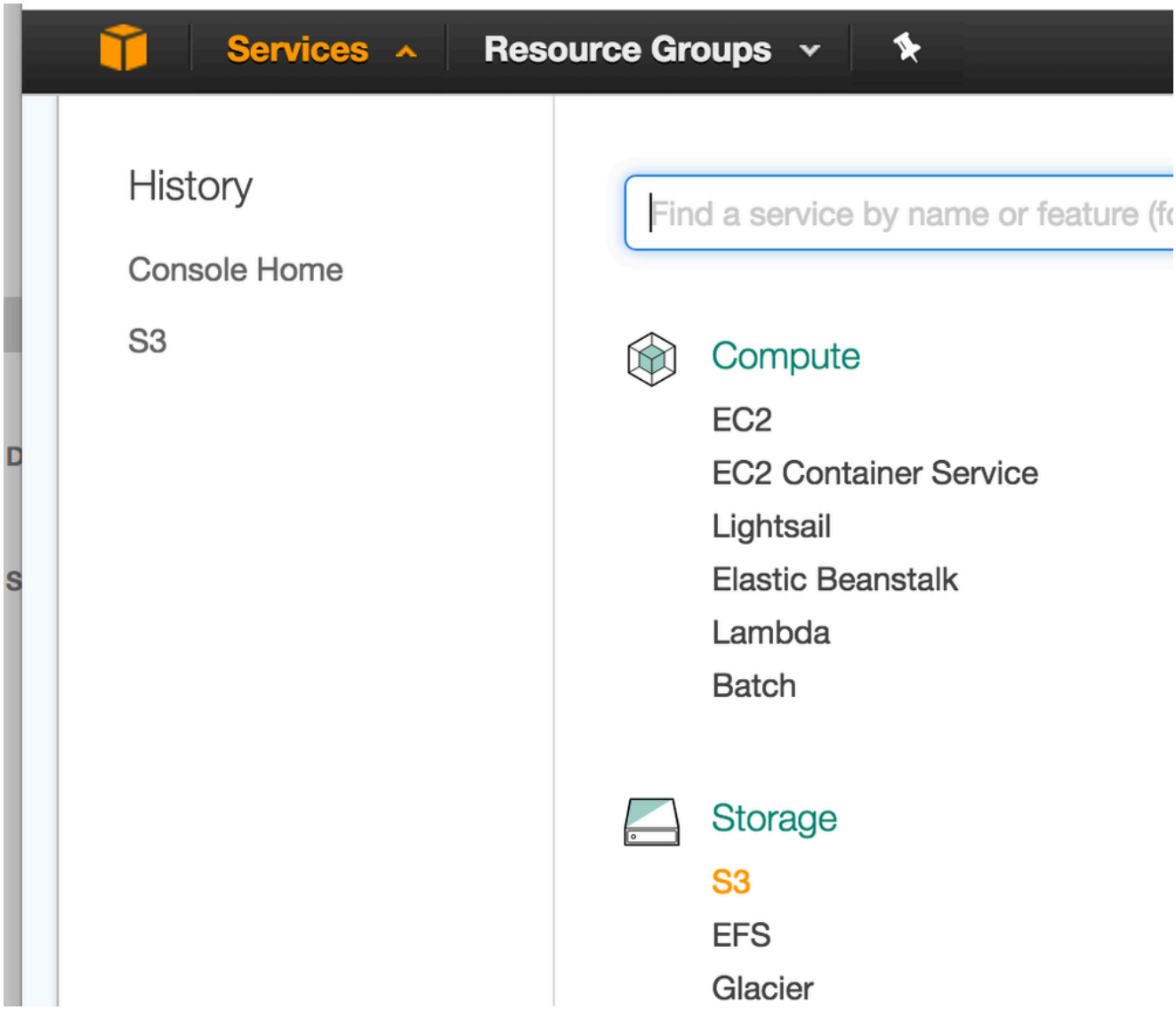
Pré-requisitos

Para arquivar logs, você deve atender a estes requisitos:

- Acesso administrativo completo ao Cisco Umbrella MSP, MSSP ou Console Multi-org.
- Um logon no serviço do Amazon AWS (https://aws.amazon.com/console/). Se você não tiver uma conta, o Amazon fornecerá inscrição gratuita para o S3. No entanto, eles exigem um cartão de crédito caso seu uso exceda o uso do plano gratuito.
- Um bucket configurado no Amazon S3 para armazenamento de log. Consulte a próxima seção para obter instruções sobre como configurar e definir o bucket do Amazon S3.

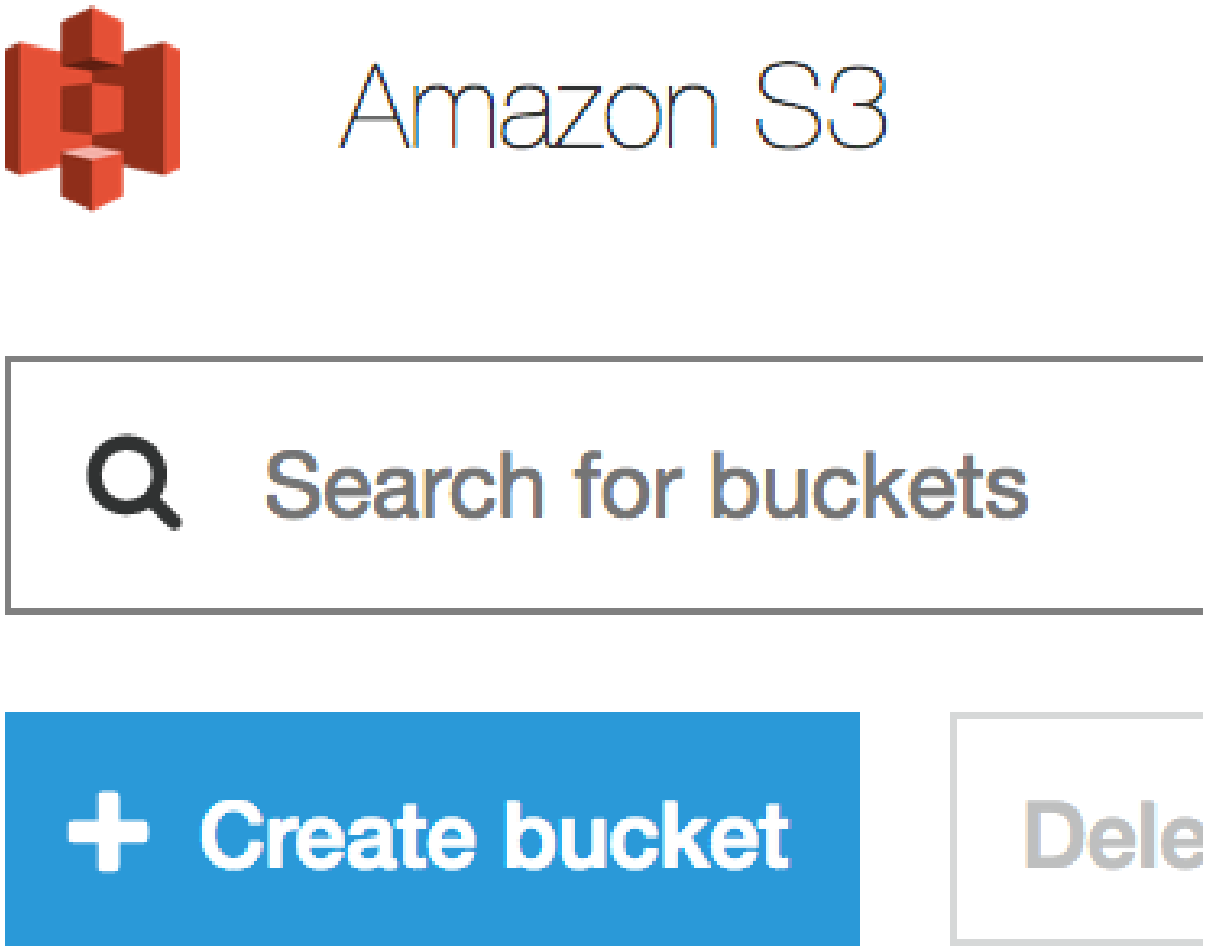
Configurando seu Amazon S3 Bucket

1. Comece fazendo login no AWS Console e selecionando "S3" na lista de opções em Armazenamento.



115012842106

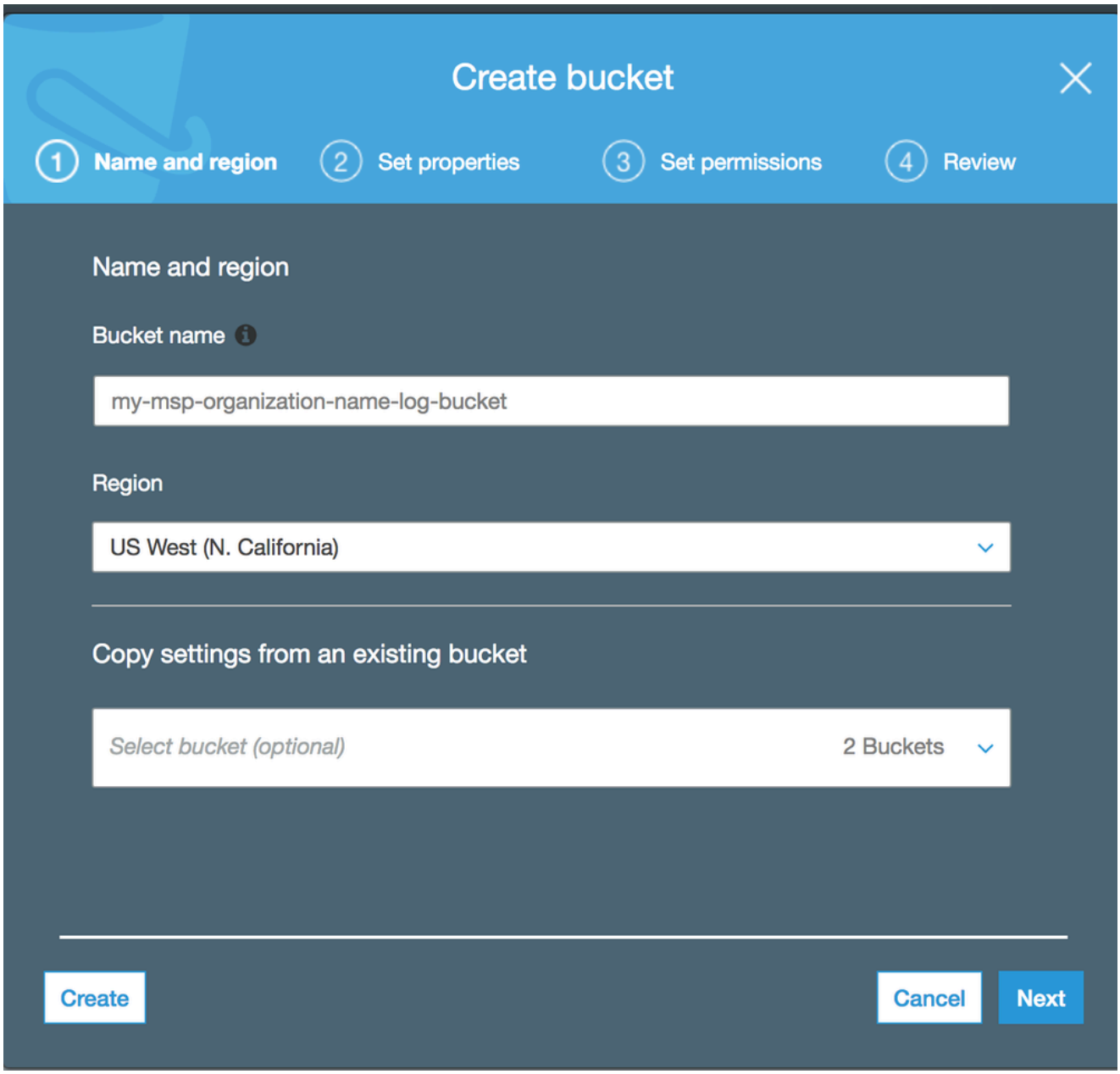
2. Você verá uma tela de introdução que o acolhe no Amazon Simple Storage System
3. Em seguida, se ainda não tiver um bucket, você deseja criar um. Clique em Criar Recipiente



115012842326

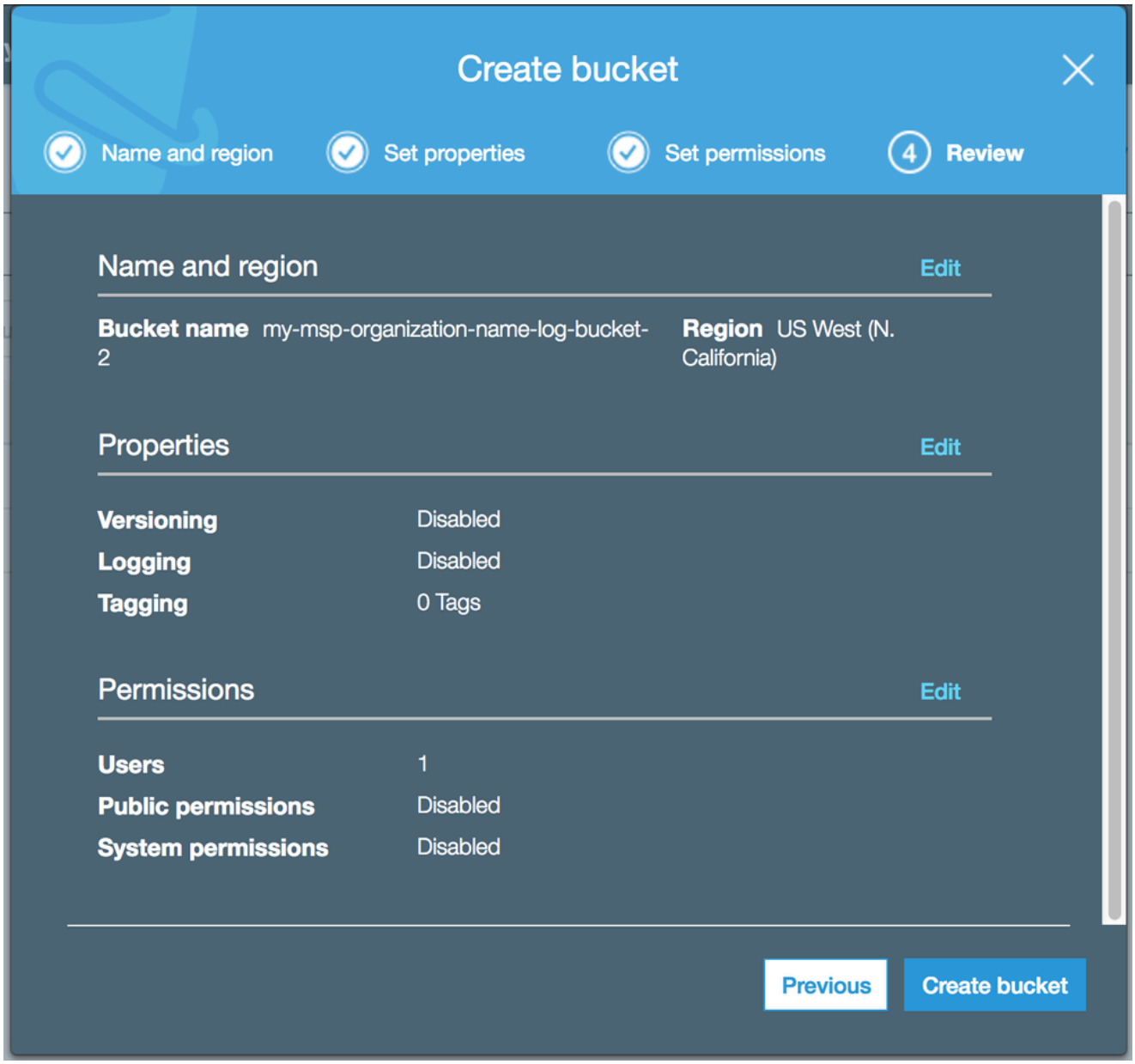
.

4. Comece informando um Nome de Período
   O nome do balde deve ser universalmente exclusivo, não apenas para o seu AWS ou seu Umbrella, mas para todo o Amazon AWS. O uso de algo pessoal, como "my-organization-name-log-bucket", pode ajudá-lo a ignorar o requisito de nome de bucket universalmente exclusivo. O nome do bucket deve usar apenas letras minúsculas e não pode conter espaços ou pontos, e deve estar em conformidade com as convenções de nomenclatura de DNS. Para obter mais informações sobre restrições de nomes, leia aqui. Para obter mais informações sobre a criação do bucket, incluindo a nomenclatura, leia aqui.



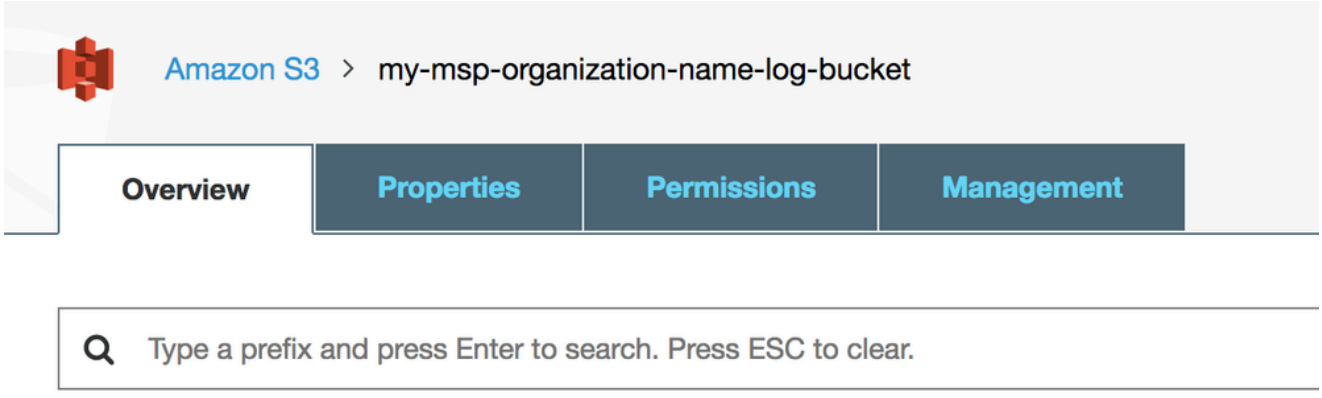
115013010503

5. Selecione a região que melhor se adapta ao seu local e clique em Criar. Não copiar as configurações de outro bucket
6. Na etapa "Definir propriedades", clique em Avançar. Eles podem ser ajustados posteriormente
7. Na etapa "Definir permissões", clique em Avançar. Vamos revisitar as permissões mais tarde para configurar o bucket para carregamento
8. Finalize o processo de revisão e clique em Criar bucket



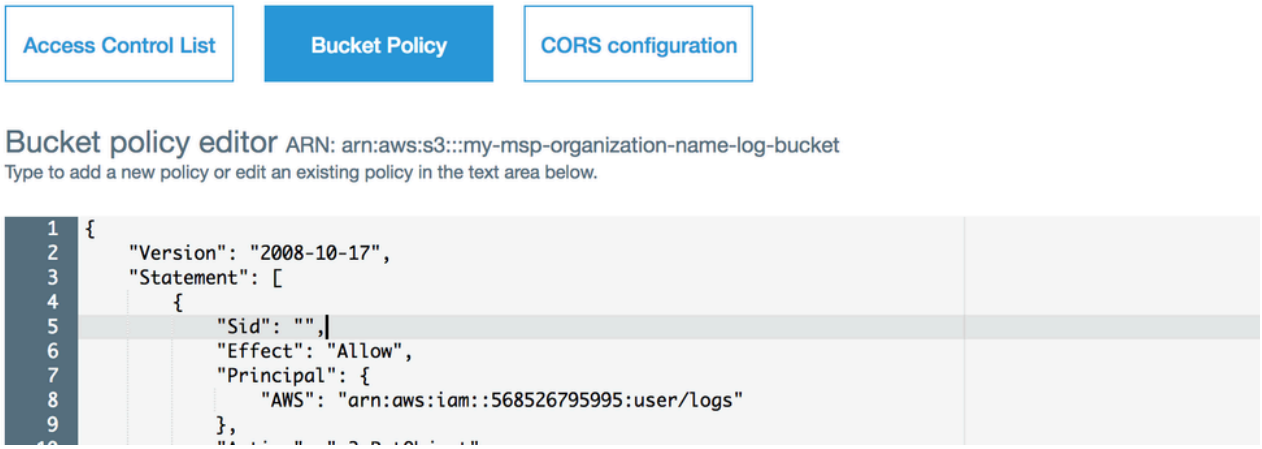
115012842686

9. Em seguida, você precisa configurar o bucket para aceitar carregamentos do Umbrella Service. Em S3, isso é conhecido como política de bucket. Clique no nome do bucket recém-configurado e selecione a guia Permissões na parte superior da interface



115012842906

10. Selecione Política de Balde e você será solicitado a colar no balde



115012843006

11. Copie e cole a cadeia de caracteres JSON abaixo, que contém a política de bucket, em um editor de texto ou simplesmente cole-a na janela. Substitua o nome exato do bucket onde nome do bucket é especificado abaixo. A falha em fazer isso resulta em uma mensagem de erro

{
"Versão" "17-10-2008",
"Declaração": [
{
"Sid" "",
"Efeito": "Permitir",
"Responsável principal": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Ação" "s3:PutObject",
"Recurso": "arn:aws:s3:::bucketname/*"
},
{
"Sid" "",
"Efeito": "Negar",
"Responsável principal": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Ação" "s3:GetObject",
"Recurso": "arn:aws:s3:::bucketname/*"
},

{
"Sid" "",
"Efeito": "Permitir",
"Responsável principal":

{ "AWS": "arn:aws:iam::568526795995:user/logs" }

,
"Ação" "s3:GetBucketLocation",
"Recurso": "arn:aws:s3:::bucketname"
},

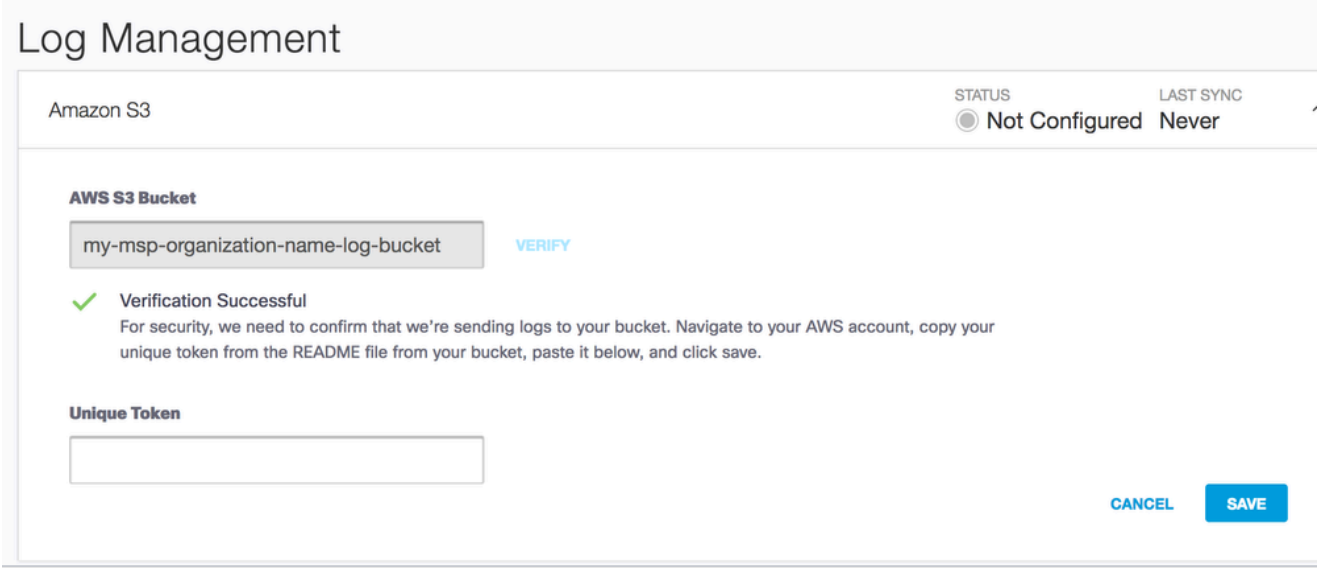
{
"Sid" "",
"Efeito": "Permitir",
"Responsável principal": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Ação" "s3:ListBucket",
"Recurso": "arn:aws:s3:::bucketname"
}
]
}

12. Clique em Salvar para confirmar esta alteração

Verificando seu Amazon S3 Bucket

Passo 1:

1. Volte para o Console do Umbrella e navegue para Configurações > Gerenciamento de logs
2. Clique em "Amazon S3" para expandir a janela
3. No campo Nome do bucket, digite ou cole o nome exato do bucket criado no S3 e clique em Verificar
   Você recebe uma mensagem de confirmação em seu painel indicando que o período foi verificado com êxito.



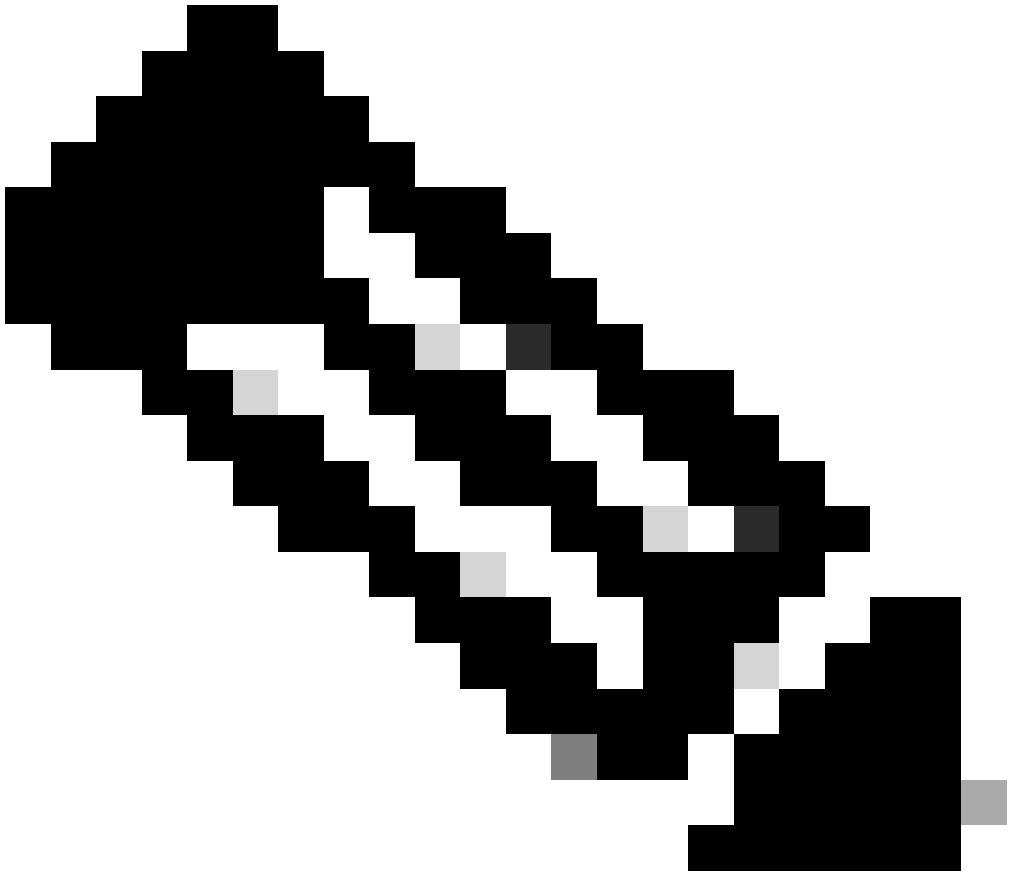
115012847146

Se você receber um erro indicando que o bucket não pôde ser verificado, verifique novamente a sintaxe do nome do bucket e revise a configuração. Se os problemas persistirem, abra um caso com nosso departamento de suporte

Passo 2:

Como precaução secundária para garantir que o bucket correto seja especificado, o Umbrella solicita que você insira um token de ativação exclusivo. O token de ativação pode ser obtido revisitando seu bucket de S3. Como parte do processo de verificação, um arquivo chamado README_FROM_UMBRELLA.txt foi carregado do Umbrella para o seu bucket do Amazon S3 e aparece lá.

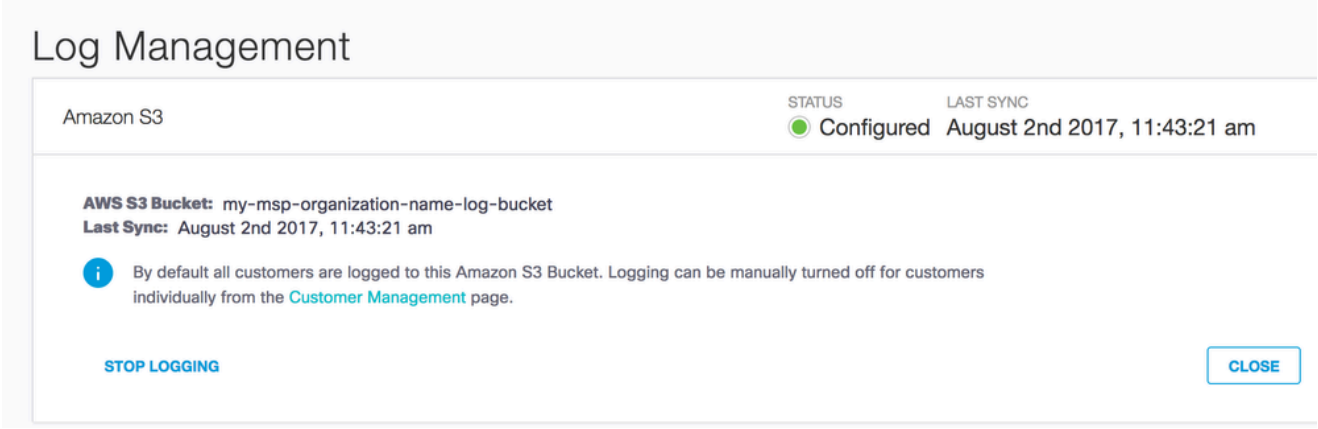
1. Faça o download do arquivo readme clicando nele duas vezes e, em seguida, abra-o em um editor de texto. Dentro do arquivo, há um token exclusivo ligando seu bucket S3 ao painel do Umbrella



Note: Talvez seja necessário atualizar o bucket de S3 no navegador para ver o arquivo LEIAME depois que ele for carregado.

2. Retorne ao painel do Umbrella e cole o token no campo rotulado "Token exclusivo" e clique

em Salvar. Neste ponto, a configuração é
concluído. Para revisar sua configuração, basta clicar no nome do Amazon S3 na seção Gerenciamento de logs



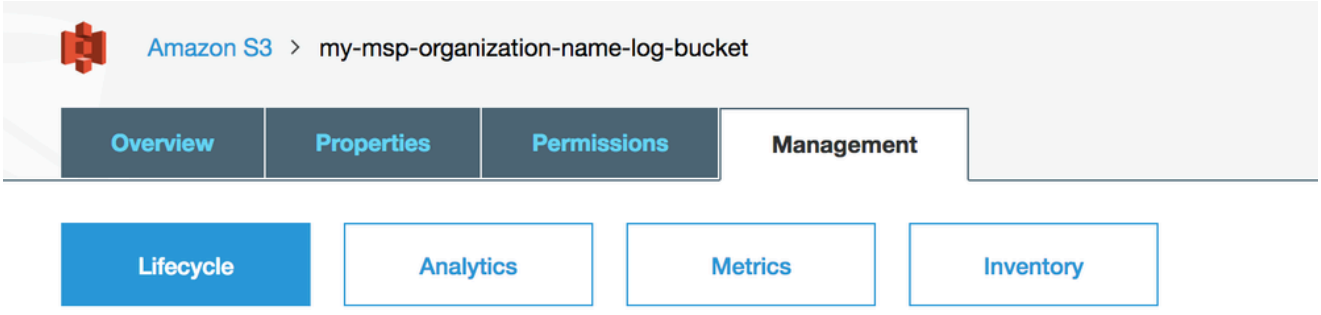
115012848126

Gerenciamento do ciclo de vida do log

Ao usar o S3, você pode gerenciar o ciclo de vida dos dados dentro do bucket para estender a duração do tempo durante o qual você gostaria de manter logs. Dependendo do motivo pelo qual você está usando o gerenciamento de log externo, a duração pode ser muito curta ou muito longa. Por exemplo, você pode simplesmente baixar os logs do bucket de S3 após 24 horas e armazená-los off-line ou manter os logs indefinidamente na nuvem. Por padrão, o Amazon armazena os dados em um bucket indefinidamente, mas o armazenamento ilimitado aumenta o custo de manutenção do bucket. Para obter mais informações sobre os ciclos de vida de S3, leia aqui.

Para configurar o ciclo de vida do seu período:

1. Selecione Gerenciamento e clique em Ciclo de vida



115012848246

2. Clique em Adicionar uma regra e, em seguida, em Aplicar a regra ao bucket inteiro (ou a uma subpasta, se você a tiver configurado como tal).
3. Selecione uma Ação em Objetos, como Excluir ou Arquivar, em seguida, selecione o período de tempo e se você gostaria de usar o armazenamento Glacier para ajudar a reduzir os custos da Amazon. (Glaciar é que é o armazenamento off-line, que, embora mais lento para acessar, é menos caro.)

4. Se você preferir gerenciar logs com outro método (como sua solução de backup interno),

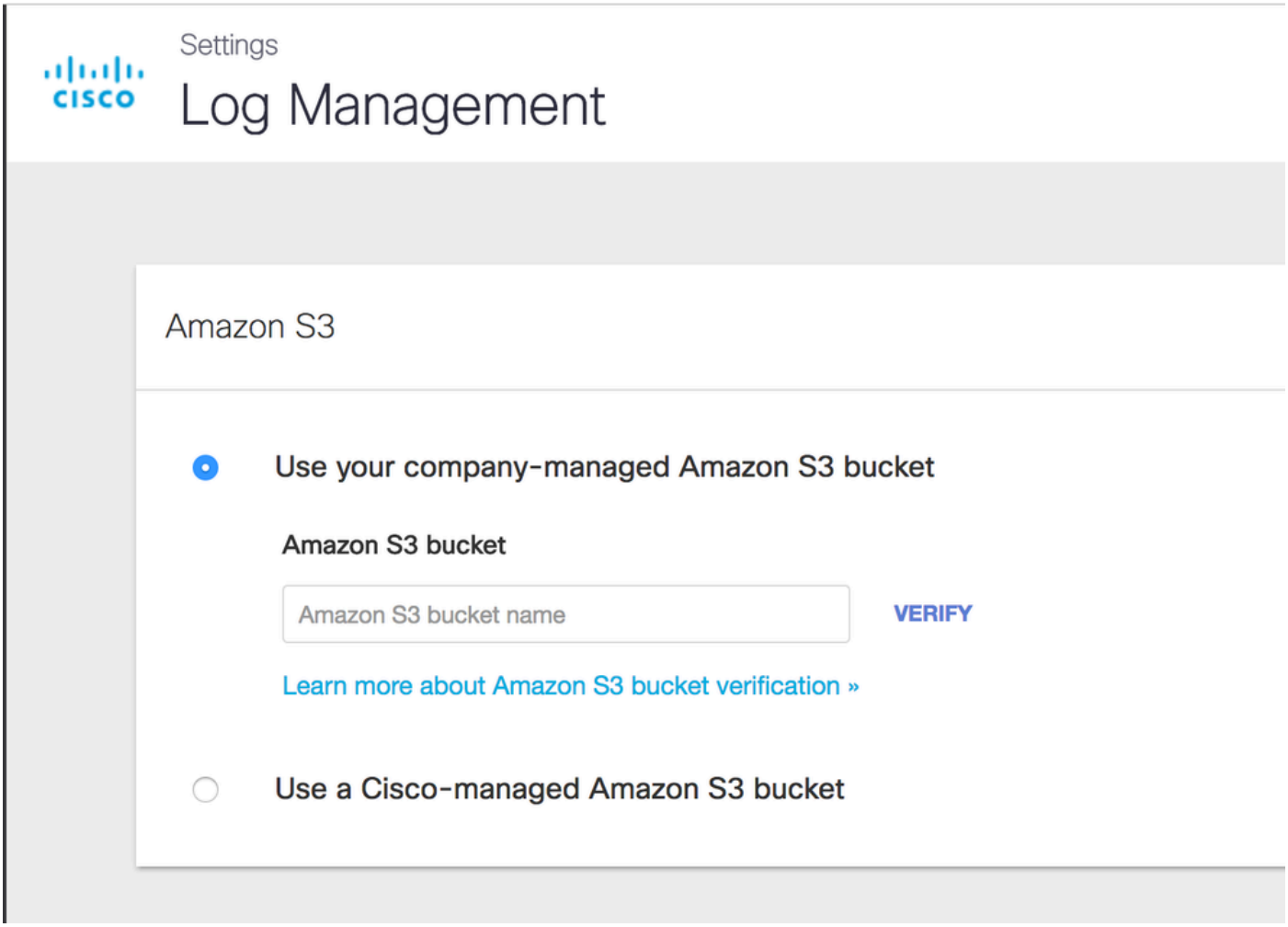
poderá simplesmente fazer download dos logs do S3 e preservá-los de outra forma e, em seguida, definir o tempo de retenção para alguns dias.

Configuração de um bucket S3 gerenciado pela Cisco

Navegue para Configurações > Gerenciamento de logs no painel do Umbrella.

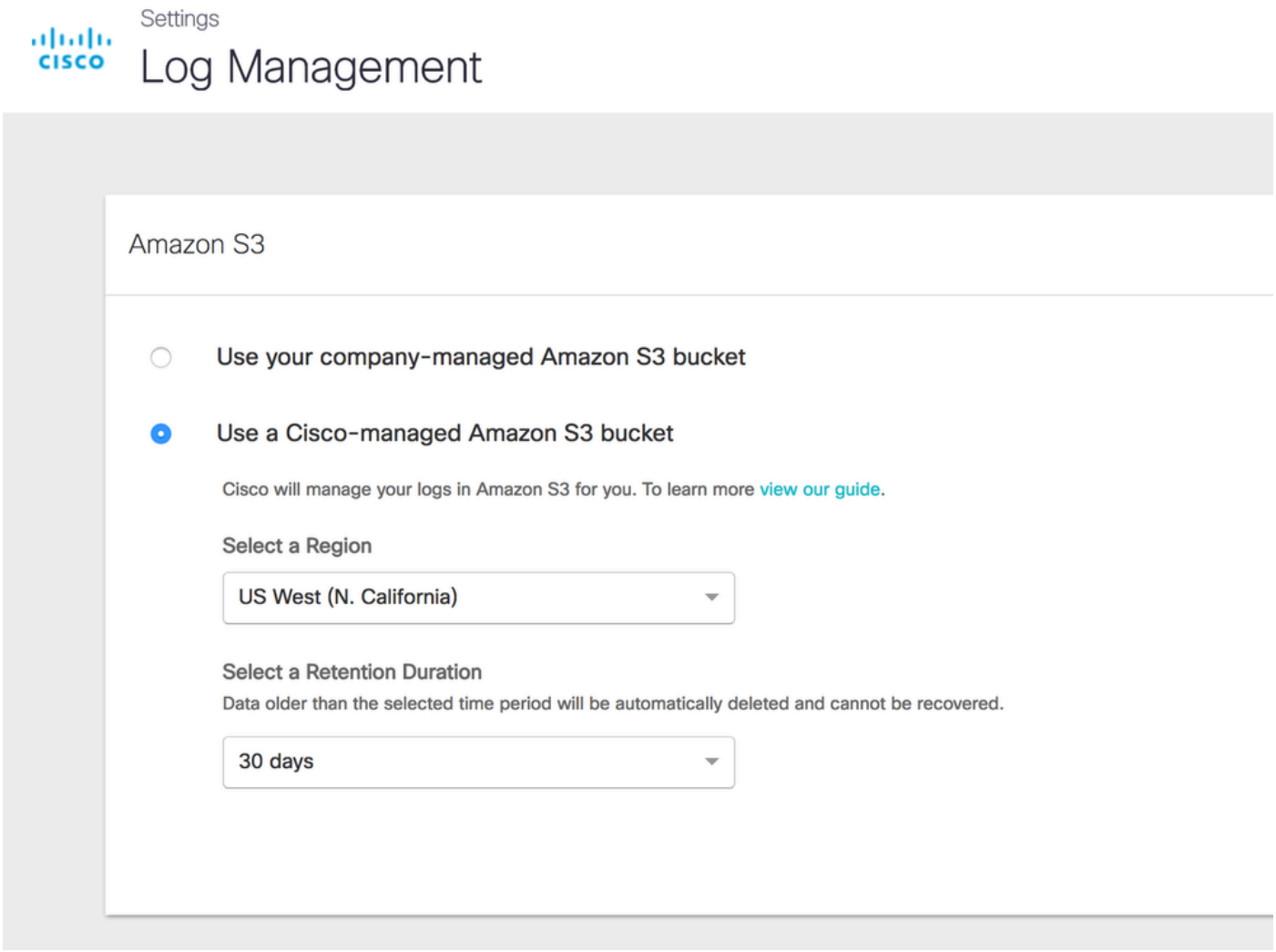
Há duas opções:

- Use o balde Amazon S3 gerenciado pela sua empresa
- Use um bucket do Amazon S3 gerenciado pela Cisco



25231151138964

Escolha "Usar um recipiente Amazon S3 gerenciado pela Cisco" e você receberá duas novas opções: "Selecione uma região" e "Selecione uma duração de retenção".



25231151158036

Selecione uma região

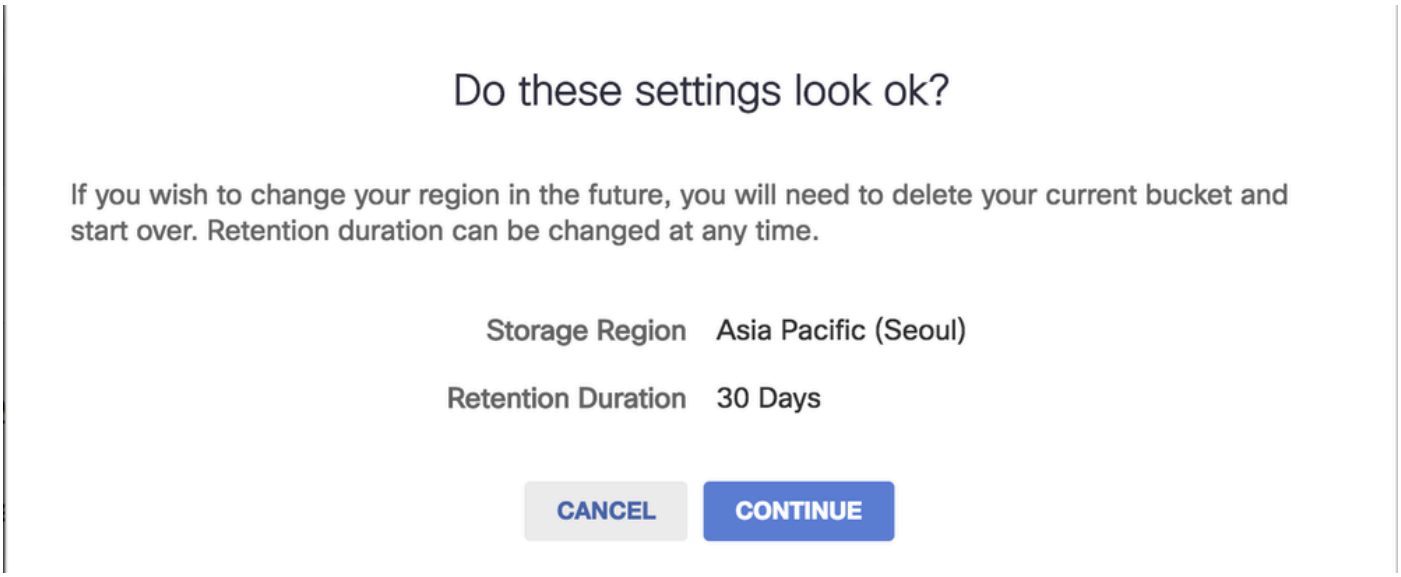
Os endpoints regionais são importantes para minimizar a latência ao baixar logs para seus servidores. As regiões listadas correspondem àquelas disponíveis no Amazon S3, mas nem todas as regiões estão disponíveis. Por exemplo, a China não consta da lista.

Selecione a região mais próxima de você no menu suspenso. Se desejar alterar sua região no futuro, você precisará excluir suas configurações atuais e começar novamente.

Selecione uma duração de retenção

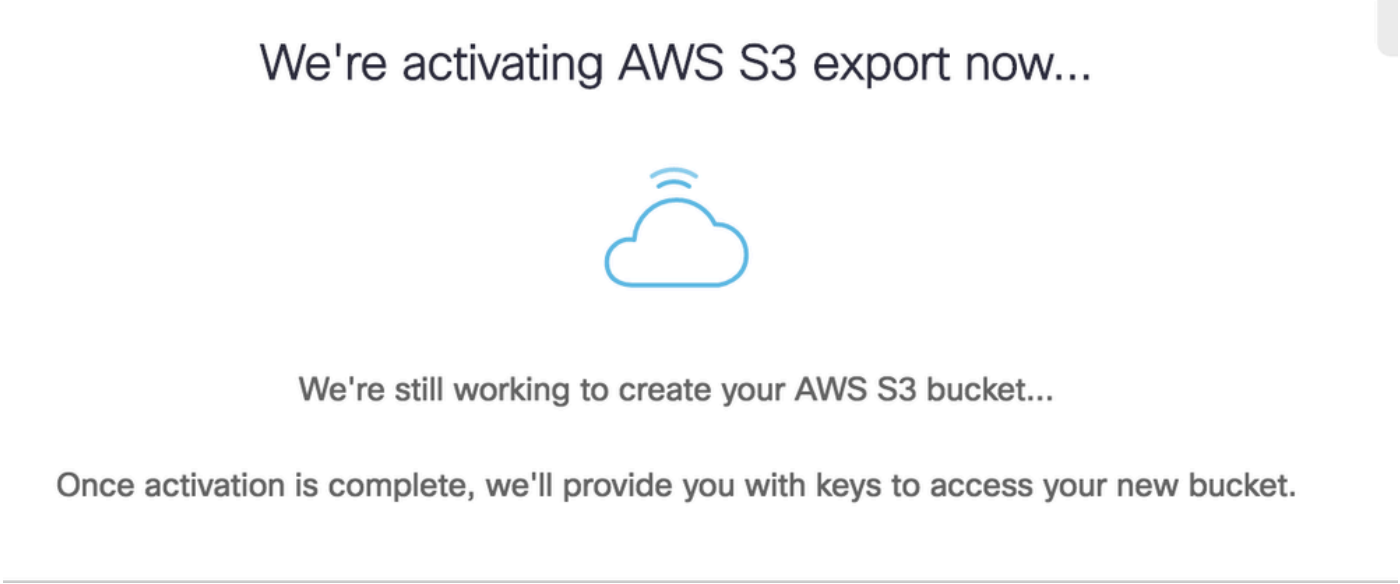
A duração da retenção é de apenas 7, 14 ou 30 dias. Após o período de tempo selecionado, todos os dados são limpos e não podem ser recuperados, não importa o que aconteça. Se o seu ciclo de ingestão for regular, recomendamos um período de tempo mais curto. A duração da retenção pode ser alterada posteriormente.

Depois de fazer suas seleções, clique em Avançar e você será solicitado a confirmar sua região e duração



25231181211796

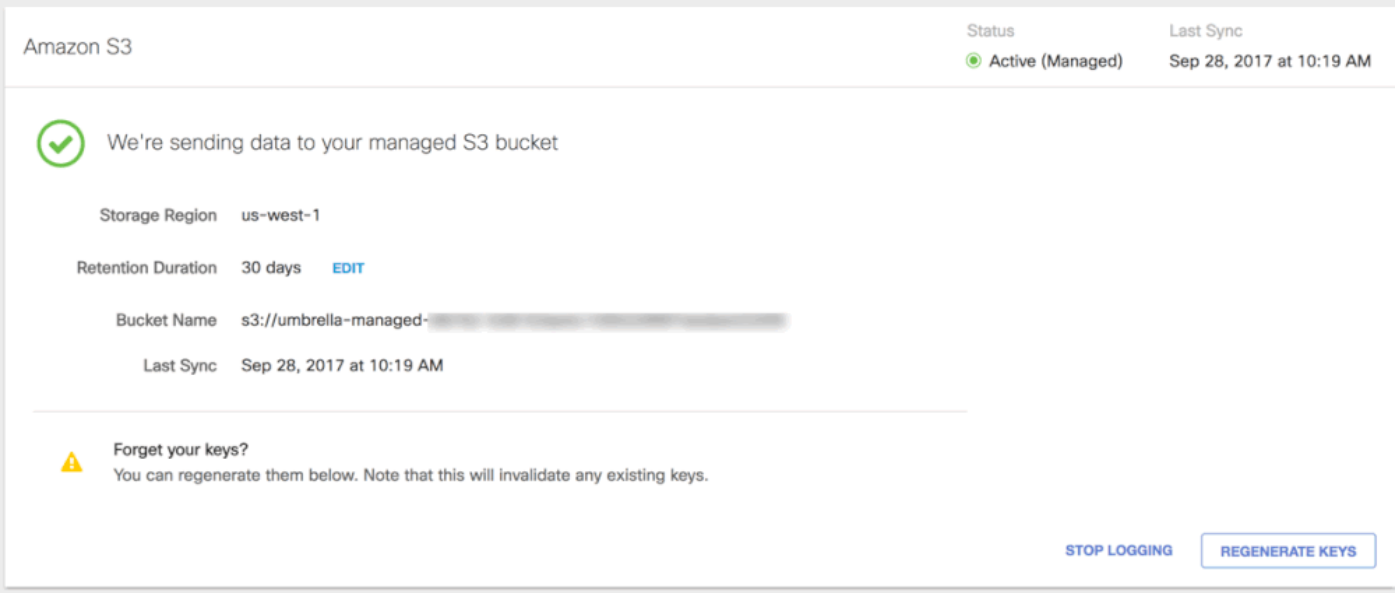
Depois de concordar em continuar, você receberá uma notificação de ativação.



25231181218708

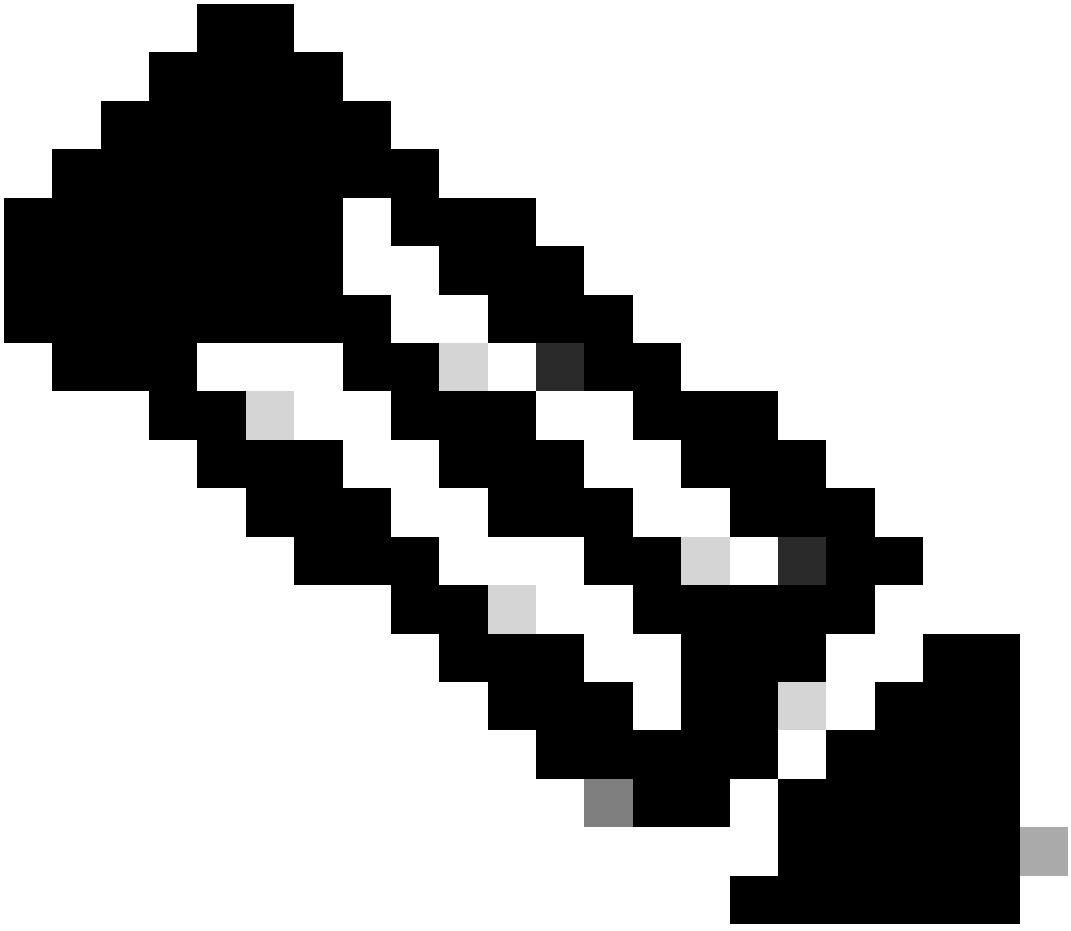
Em seguida, você recebe uma chave de acesso e a chave secreta do . Você deve aceitar (clique em "Got it!") porque esta é a única vez que você consegue ver qualquer uma das chaves. As chaves de acesso e secretas são necessárias para acessar seu bucket e baixar seus logs.

Por fim, você verá a tela de resumo mostrando a configuração e, mais importante, o nome do seu bucket.



25231181228180

Você pode ativar ou desativar o processo de login quando for mais conveniente.



Note: A Cisco continua a limpar os logs com base na duração de retenção selecionada, mesmo que o registro tenha sido desativado.

Opções de pós-configuração

Falhas no Carregamento de Log

Em caso de falha ao carregar registros do Cisco Umbrella para o seu bucket S3, há um período de carência de quatro horas durante o qual o serviço tentará novamente a cada 20 minutos. Após quatro horas, um caso é aberto com nossa equipe de suporte, que inicia uma investigação sobre a causa do problema e entra em contato com você de forma proativa para informá-lo sobre o problema.

Verificando Logs Carregados e Formato

Os logs são carregados em intervalos de dez minutos da fila de logs do Umbrella para os buckets S3. Após concluir a configuração, o primeiro log é carregado no bucket do S3 dentro de duas horas, embora o processo geralmente seja imediato ou próximo a imediato. No entanto, o upload de qualquer coisa exige a existência de dados de registro recém-gerados, portanto, se você estiver tentando isso em um ambiente de teste, verifique se os dados da rede estão sendo registrados na Pesquisa de atividade.

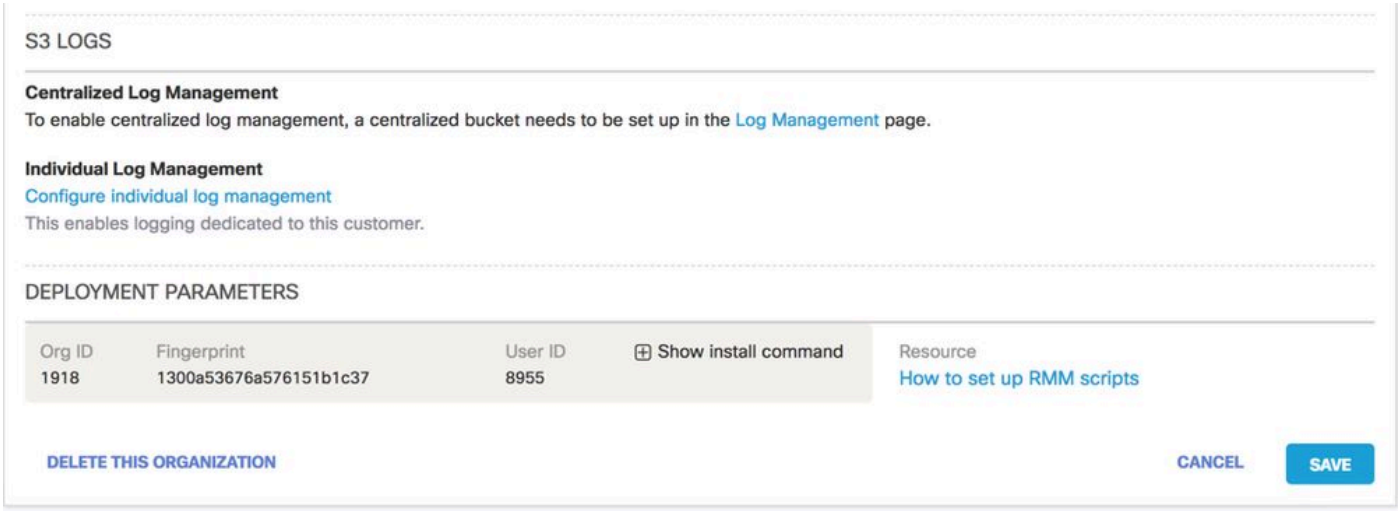
Para verificar se tudo está funcionando, a hora da Última sincronização no painel Umbrella atualiza e registra em seu bucket S3.

Dentro do seu período, cada cliente ou organização é rotulada com sua ID da organização, de modo que a estrutura de pastas é:

```
Amazon S3/<bucket-name>/<orgID>/<subfolder>
```

<bucket-name> é o nome do seu bucket, <orgID> é a sua organização, é o ID e <subfolder> são dnslogs, proxylogs ou iplogs, dependendo dos tipos de logs contidos em.

Para clientes MSP e MSSP, a orgID corresponde à que está nas Configurações do cliente sob cada detalhe de cliente na seção Parâmetros de implantação. Os clientes de várias organizações podem reunir a orgID fazendo login em cada sub-organização individual e anotando a orgID na URL do navegador: (https://dashboard.umbrella.com/o/######/).



360002271623

Atualmente, a versão do formato de log para clientes MSP, MSSP e Multi-org é a versão 1.1. Os logs aparecem em um formato GZIP e são carregados em buckets S3 na subpasta apropriada com este formato de nome:

```
<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz
```

<subfolder> é dnslogs, proxylogs ou iplogs, dependendo dos tipos de logs contidos em. <xxxx> é uma sequência de caracteres aleatória de quatro caracteres alfanuméricos, que impede a substituição de nomes de arquivos duplicados.

Por exemplo:

```
dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz
```

Se você não vir logs em seu bucket dentro de 10 minutos, entre em contato com o suporte, descrevendo as etapas que você realizou até agora.

Depois que os logs forem exibidos, recomendamos revisar os dados descompactando o conteúdo dos primeiros carregamentos de log recebidos para garantir que os dados possam ser exibidos em um editor de texto (ou até mesmo no Microsoft Excel, geralmente o padrão para .CSV). Para obter informações sobre quais campos no registro representam, leia aqui.

Se um carregamento de log do Cisco Umbrella para o seu bucket S3 falhar, há um período de carência de quatro horas no qual o serviço tentará novamente a cada 20 minutos. Após quatro horas, um caso é aberto em nossa equipe de suporte, que inicia uma investigação sobre a causa do problema e entra em contato com você de forma proativa para informá-lo sobre o problema.

Ativar registro em uma base por cliente

Pronto para uso, esse recurso é habilitado para todos os clientes, a menos que seja especificado de outra forma. O recurso pode ser desativado para clientes individuais, o que é útil se você tiver diferentes níveis de serviço para clientes que possuem o recurso. Abaixo de cada clientede suas configurações no Console. A captura de tela na seção anterior mostra a alternância para desativá-la.

Também é possível criar usuários do IAM no Amazon e atribuir esses usuários do IAM a uma única organização ou a subpastas do bucket. Ao fazer isso, você pode permitir que um usuário final acesse seus logs, mas apenas seus logs.

Download de logs, Entendendo o formato e a integração Splunk / QRadar

Para baixar os logs de retenção ou consumo, há algumas abordagens para baixar os logs de DNS do S3. Weit criou um artigo descrevendo algumas abordagens para esse problema aqui.

Você também pode ter algumas perguntas sobre o formato do log e como ele difere um pouco dos logs exibidos no painel do Umbrella. Para obter mais informações sobre o formato de log exportado, leia este artigo.

Por fim, um dos principais usos para exportar logs DNS é a integração com ferramentas SIEM. Embora a configuração de um SIEM ao lidar com registros como esse possa frequentemente se resumir a um administrador como preferências pessoais, temos algumas orientações para os SIEMs mais populares.

Para obter mais informações sobre como configurar o plug-in Splunk para o Amazon AWS S3 e o Umbrella, leia aqui.

Para obter informações sobre como configurar o IBM QRadar para extrair logs do Amazon S3 e digeri-los, leia aqui.

Qual é o tamanho dos registros S3?

O tamanho dos registros S3 depende do número de eventos que ocorrem, que depende do volume do tráfego DNS.

Você pode encontrar o formato de log para o registro S3 aqui.

A entrada do exemplo é 220 bytes, mas o tamanho de cada linha de registro varia com base em um número de itens (comprimento do nome de domínio, número de categorias, etc). Supondo que cada linha de log tenha 220 bytes, um milhão de solicitações seria de 220 MB.

Para obter uma estimativa de quantas consultas DNS são vistas por dia:

1. No painel Umbrella, navegue até Reporting > Activity Search.
2. Em Filtros, execute um relatório para as últimas 24 horas e clique no ícone Exportar CSV.
3. Abra o arquivo .csv baixado. O número de linhas (menos uma para o cabeçalho) é o número de consultas DNS por dia; multiplique isso por 220 bytes para obter a estimativa para um dia.

Em termos de custo, embora seja variável, descobrimos que mesmo nossos clientes mais volumosos gastam apenas alguns dólares por mês no serviço. Um custo está ligado ao tempo de armazenamento e outro ao download de dados do S3 para o seu ambiente. Consulte a Amazon para obter mais detalhes.

Assim como ocorre com qualquer um de nossos recursos, avalie a isd love para saber o que você acha, especialmente em relação às integrações do SIEM ou a quaisquer questões adicionais que sejam abordadas nesta documentação. Se você tiver algum comentário a fazer, entre em contato conosco!

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.