Comprendere la gestione centralizzata dei registri con il servizio S3 di Amazon per i clienti MSP, MSSP e multi-org

Sommario

Introduzione

Questo documento descrive la gestione centralizzata dei registri Umbrella con il servizio S3 di Amazon per i clienti MSP, MSSP e multi-org.

Panoramica

Le console MSP, MSSP e Multi-org sono in grado di archiviare i registri DNS, URL e IP dei clienti offline nello storage cloud. Lo storage si trova in Amazon S3 e, dopo il caricamento dei log, è possibile scaricarli e conservarli per motivi di conformità o analisi di sicurezza.

Questa documentazione aiuta a comprendere questa funzione, configurarla sia nel dashboard Umbrella che nella console Amazon S3, ed eseguire diverse opzioni per la configurazione, inclusa la durata di tempo che si desidera che i log siano conservati in S3.

Umbrella per MSP, MSSP e Multi-Org hanno tutti la capacità di caricare i log attività traffico dalle

organizzazioni figlio della console e archiviarli nel cloud. AWS S3 (Simple Storage Service) di Amazon è il servizio che archivia i log e viene talvolta indicato come storage offline o conservazione islog.

L'archiviazione dei log può essere utile per diversi motivi, a seconda delle esigenze. Per alcuni utenti, i registri esportati e archiviati possono essere importati in strumenti di analisi dei dati o di difesa della sicurezza, ad esempio SIEM. Per altri, un archivio di registri delle attività può essere utile per la scienza forense dei dati in caso di incidenti relativi alla sicurezza o per i record relativi alle risorse umane.

AWS S3 memorizza i registri in un archivio compresso (gzip) in formato CSV. Poiché i registri vengono caricati ogni dieci minuti, si verifica un ritardo di almeno dieci minuti tra il traffico di rete proveniente dalla rete, registrato da Umbrella, e quindi reso disponibile per il download da S3.

Il numero orgID della console

Ogni organizzazione cliente carica i propri log singolarmente, utilizzando il numero orgID dalla Console per mappare ogni cliente a una cartella. La funzione può anche essere abilitata o disabilitata per cliente/per organizzazione.

Due tipi di gestione dei registri Umbrella

La gestione dei log viene eseguita caricando i log in ciò che viene chiamato isbucketit (essenzialmente una cartella all'interno dell'ambiente AWSit è S3). Esistono due modi per ospitare un bucket per i registri Umbrella:

- Amministrato, gestito e pagato dall'utente, l'amministratore aziendale.
- Amministrata, gestita e retribuita da Cisco Umbrella.

La gestione del secchio S3 da parte di Cisco comporta vantaggi e svantaggi.

Vantaggi di Cisco nella gestione del bucket:

- Facile da configurare. L'operazione richiede solo un paio di minuti e dopo è estremamente facile da gestire.
- Il servizio di gestione degli intervalli di Cisco è incluso nel costo della licenza con Umbrella, rendendo il servizio gratuito. Anche se è poco costoso avere un proprio secchio, il costo comune di gestione di un'altra fattura può essere proibitivo.

I vantaggi della gestione di un'istanza S3:

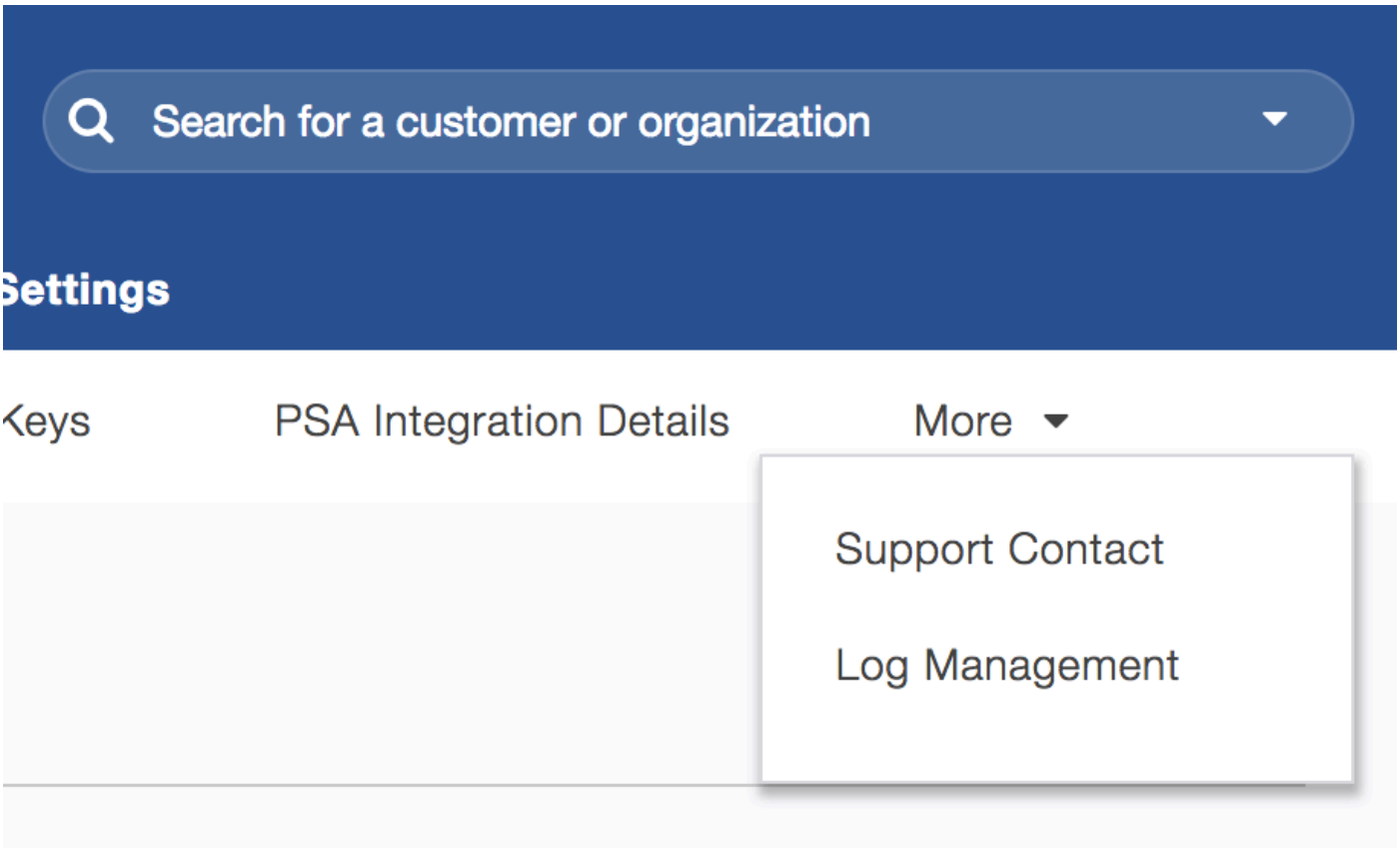
- Non vi sono limiti alla durata di archiviazione offline dei dati. Cisco limita lo storage offline a 30 giorni al massimo.
- È possibile aggiungere qualsiasi elemento al bucket, inclusi i file di log di Umbrella, in modo che il bucket possa essere utilizzato anche da altre applicazioni.
- È possibile ottenere supporto direttamente da Amazon per assistenza nella configurazione avanzata, ad esempio per l'automazione o per la riga di comando.

Per la maggior parte dei clienti il costo di manutenzione di un secchio è molto conveniente, ma

può rivelarsi complicato.

Per iniziare

La funzione Log Management è disponibile in Console in Impostazioni > Log Management (è possibile fare clic sulla freccia a discesa).



115012963103

Configurazione di un bucket S3 autogestito

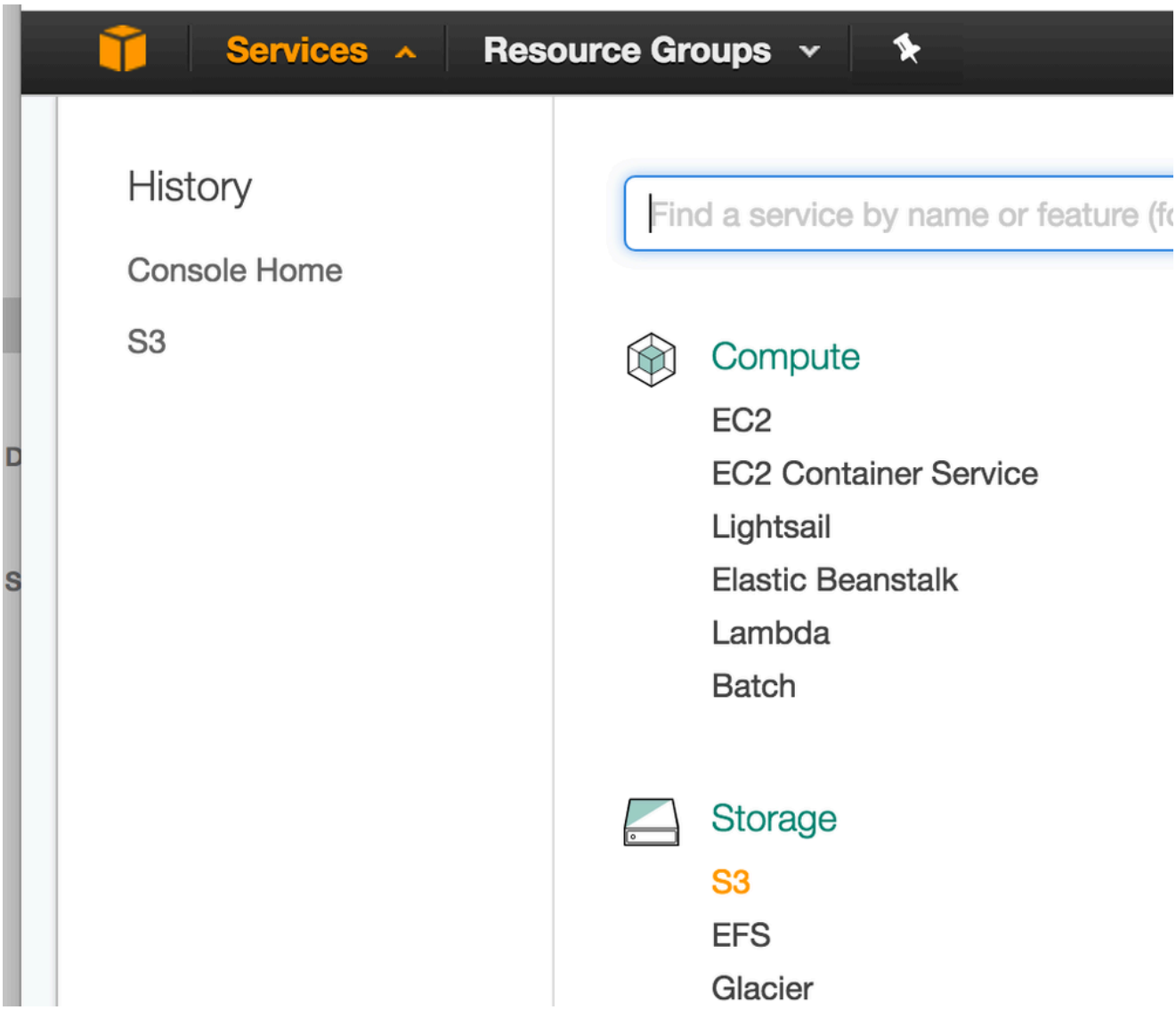
Prerequisiti

Per archiviare i registri, è necessario soddisfare i seguenti requisiti:

- Accesso amministrativo completo a Cisco Umbrella MSP, MSSP o Multi-org Console.
- Un accesso al servizio Amazon AWS (https://aws.amazon.com/console/). Se non si dispone di un account, Amazon offre l'iscrizione gratuita per S3. Tuttavia, richiedono una carta di credito nel caso in cui l'utilizzo superi l'utilizzo del piano gratuito.
- Un bucket configurato in Amazon S3 per lo storage dei log. Vedere la sezione successiva per istruzioni sulla configurazione e l'impostazione del bucket S3 Amazon.

Configurazione del secchiello Amazon S3

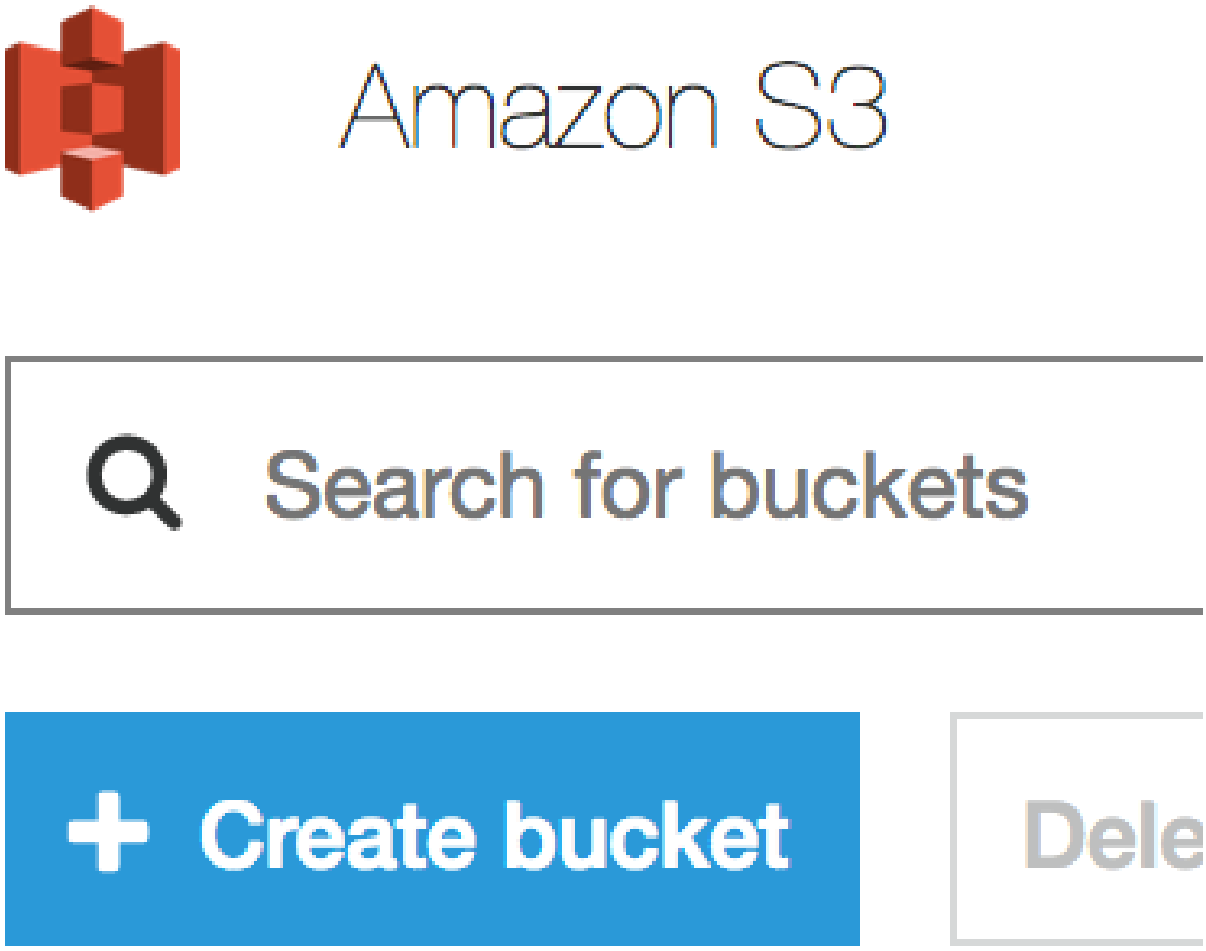
1. Accedere innanzitutto alla console AWS e selezionare "S3" dall'elenco di opzioni in Archiviazione.



115012842106

2. Viene visualizzata una schermata introduttiva che dà il benvenuto al sistema di storage semplice Amazon

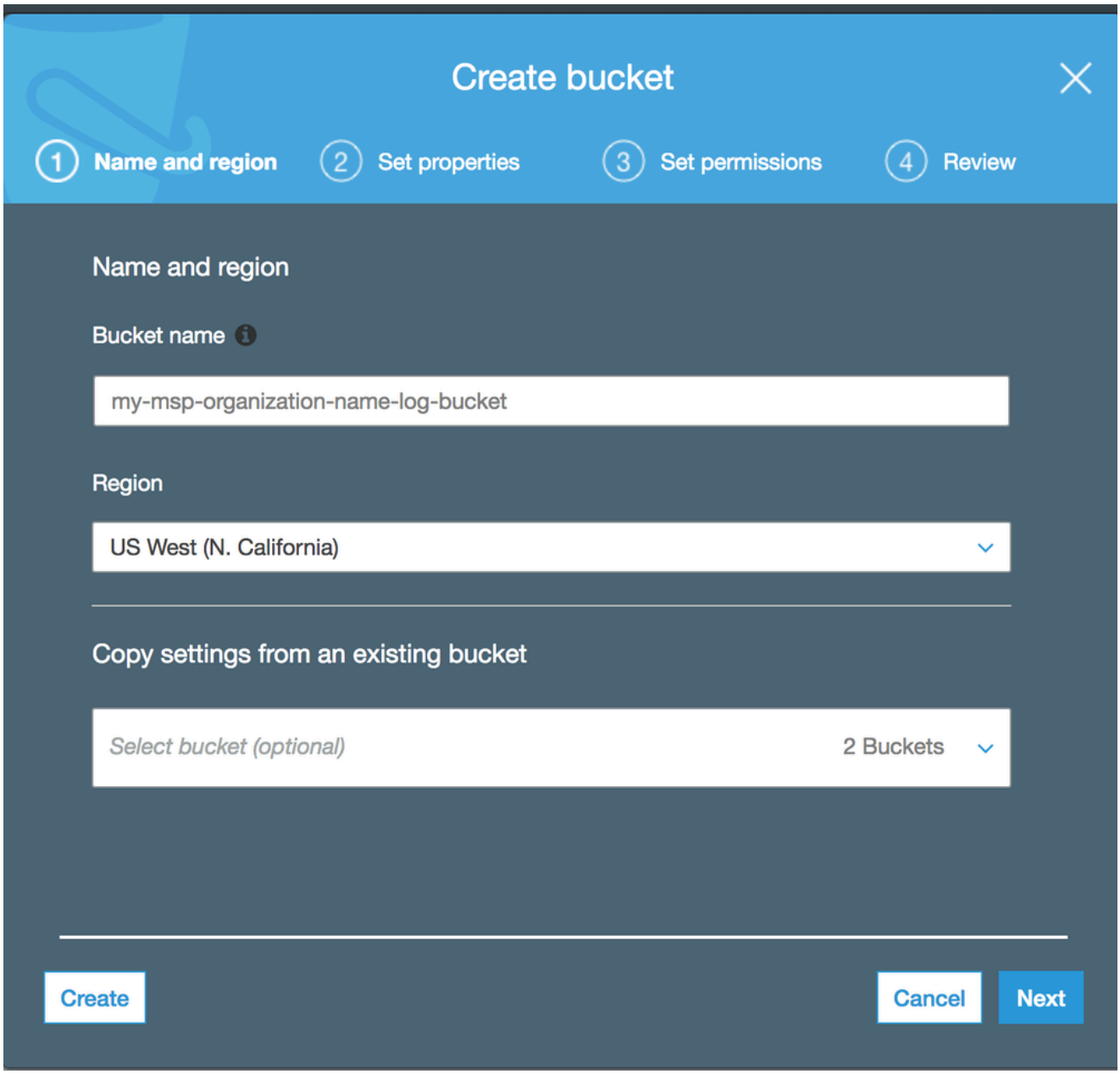
3. Se non si dispone di un periodo fisso, crearne uno. Fare clic su Crea bucket



115012842326

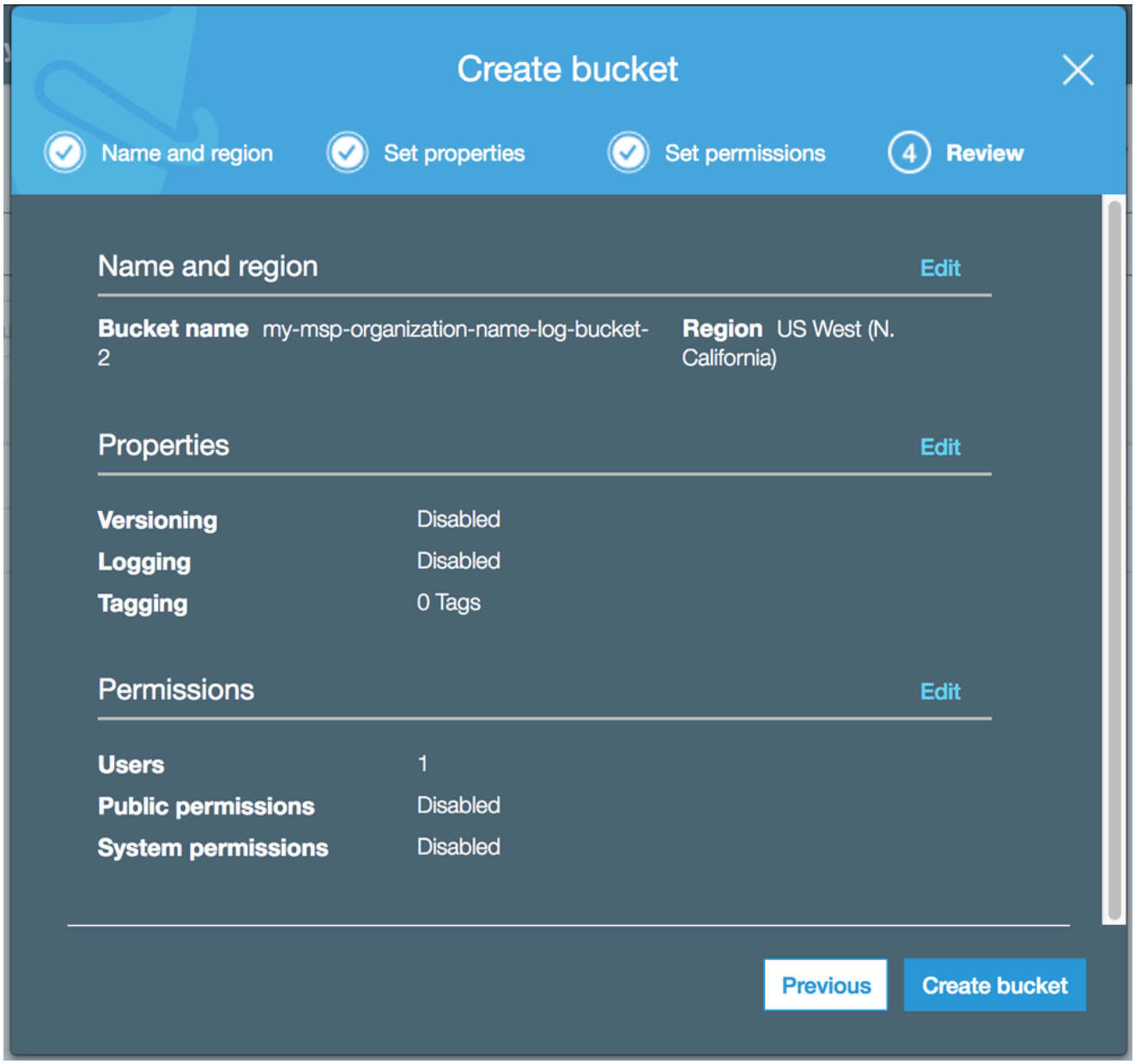
.

4. Iniziare immettendo il nome di un bucket
   Il nome del secchio deve essere universalmente univoco, non solo per il vostro AWS o il vostro Umbrella, ma per tutto Amazon AWS. L'utilizzo di un elemento personale, ad esempio "nome-organizzazione-registro-bucket", consente di evitare di utilizzare nomi di bucket universalmente univoci. Il nome del bucket deve contenere solo lettere minuscole, non spazi o punti e deve essere conforme alle convenzioni di denominazione DNS. Per ulteriori informazioni sulle limitazioni dei nomi, leggere qui. Per ulteriori informazioni sulla creazione di bucket, inclusa la denominazione, leggere qui.



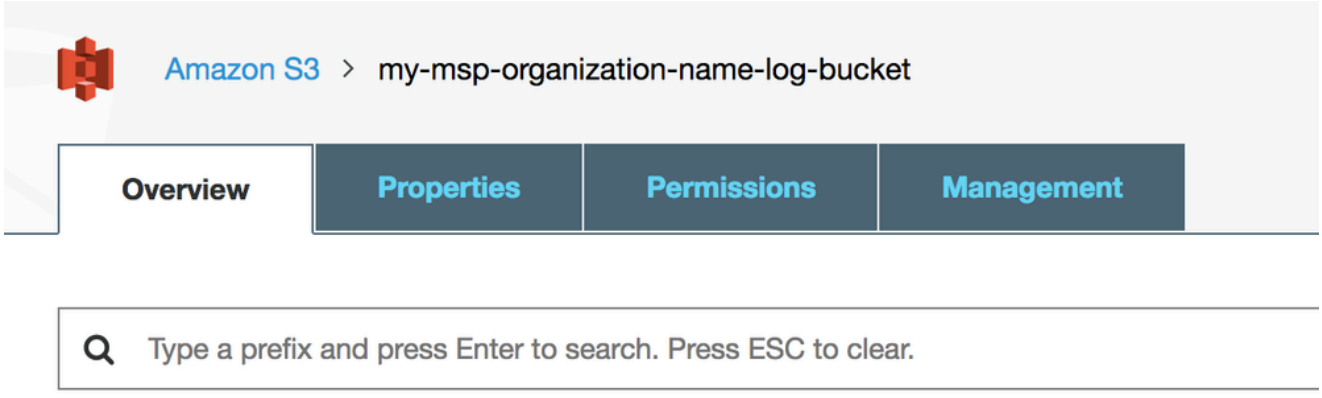
115013010503

5. Selezionare la regione più adatta alla propria posizione e fare clic su Crea. Non copiare le impostazioni da un altro bucket
6. Nel passaggio "Imposta proprietà", fare clic su Avanti. Queste impostazioni possono essere modificate in seguito
7. Nel passaggio "Imposta autorizzazioni", fare clic su Avanti. Le autorizzazioni verranno riesaminate in seguito per impostare il bucket per il caricamento
8. Completare il processo di revisione e fare clic su Crea bucket



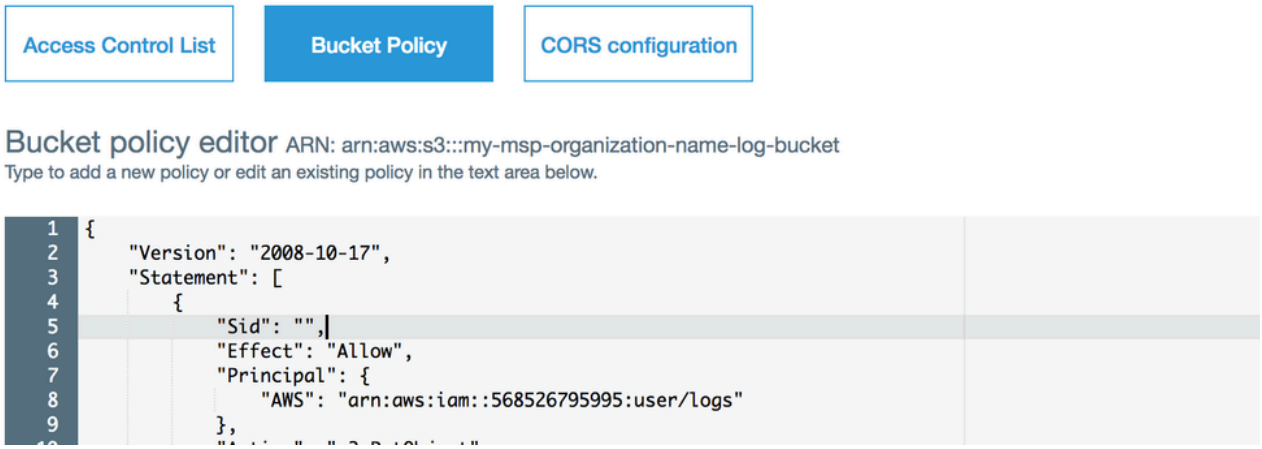
115012842686

9. È quindi necessario configurare il bucket in modo che accetti caricamenti dal servizio Umbrella. In S3, questo tipo di regola viene definita regola periodo fisso. Fare clic sul nome del bucket appena configurato e quindi selezionare la scheda Autorizzazioni nella parte superiore dell'interfaccia



115012842906

10. Selezionare Criterio bucket, quindi viene richiesto di incollare nel bucket



115012843006

11. Copiare e incollare la stringa JSON seguente, che contiene il criterio bucket, in un editor di testo o semplicemente incollarla nella finestra. Sostituire il nome esatto del periodo fisso in cui bucketname è specificato di seguito. In caso contrario, verrà visualizzato un messaggio di errore

{
"Versione" "2008-10-17",
"Dichiarazione": [
{
"Sid": "",
"Effetto": "Consenti"
"committente": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Azione": "s3:PutObject"
"Risorsa": "arn:aws:s3::nomebucket/*"
},
{
"Sid": "",
"Effetto": "Nega",
"committente": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Azione": "s3:GetObject",
"Risorsa": "arn:aws:s3::nomebucket/*"
},

{
"Sid": "",
"Effetto": "Consenti"
"committente":

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

,
"Azione": "s3:GetBucketLocation",
"Risorsa": "arn:aws:s3::nomebucket"
},

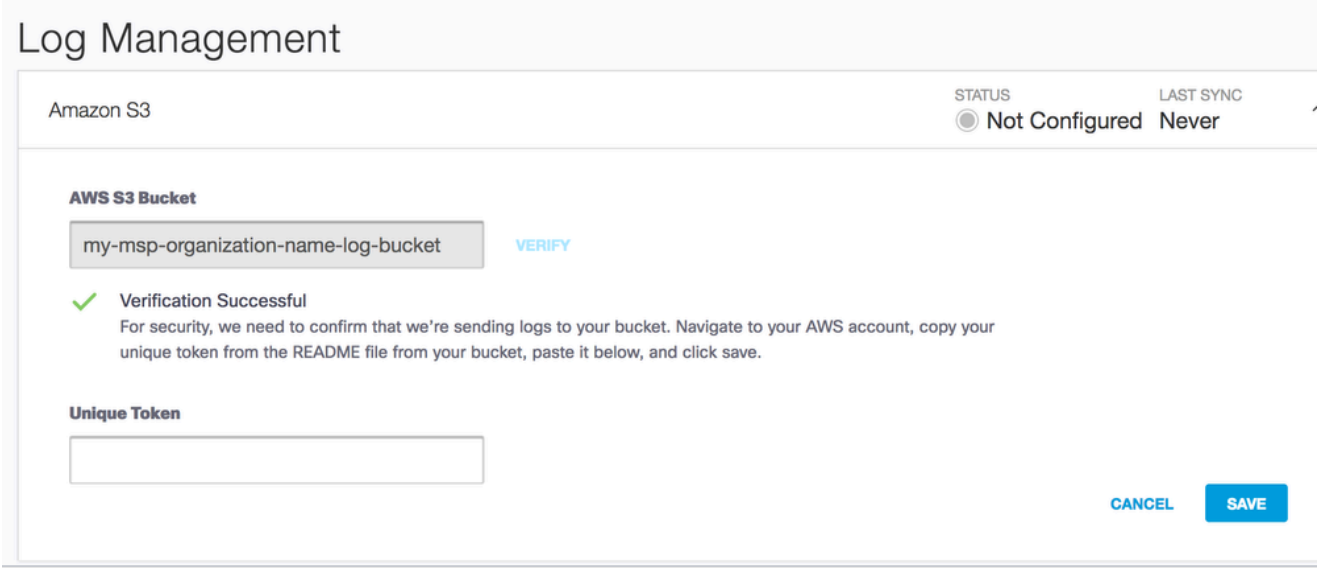
{
"Sid": "",
"Effetto": "Consenti"
"committente": {
"AWS" "arn:aws:iam::568526795995:user/logs"
},
"Azione": "s3:ListBucket"
"Risorsa": "arn:aws:s3::nomebucket"
}
]
}

12. Fare clic su Salva per confermare la modifica

Verifica del secchiello Amazon S3

Passaggio 1:

1. Tornare a Umbrella Console e selezionare Impostazioni > Gestione registro
2. Clicca su Amazon S3 per espandere la finestra
3. Nel campo Nome bucket, digitare o incollare il nome esatto del bucket creato in S3 e fare clic su Verifica
   Nel dashboard viene visualizzato un messaggio di conferma che indica che il bucket è stato verificato correttamente.



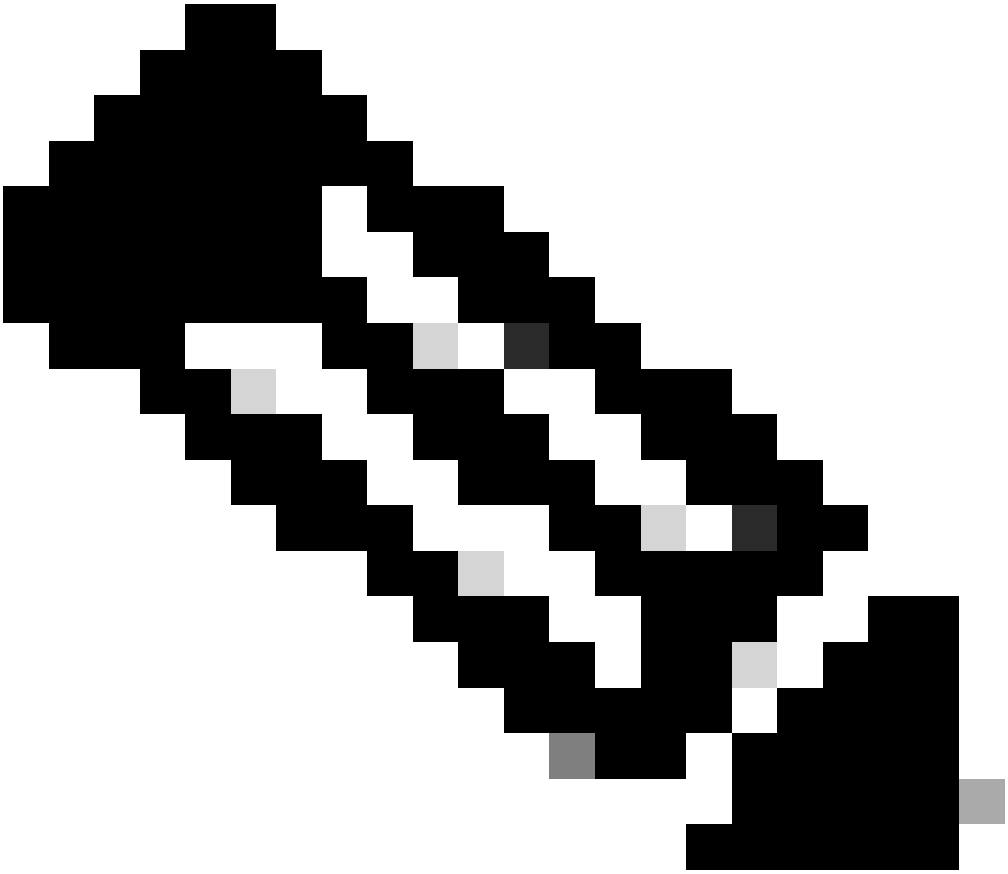
115012847146

Se viene visualizzato un errore che indica che non è stato possibile verificare il bucket, controllare nuovamente la sintassi del nome del bucket ed esaminare la configurazione. Se i problemi persistono, apri una richiesta presso il nostro reparto di assistenza

Passaggio 2:

Come precauzione secondaria per assicurarsi che sia stato specificato il bucket corretto, Umbrella richiede l'immissione di un token di attivazione univoco. È possibile ottenere il token di attivazione modificando il bucket S3. Come parte del processo di verifica, un file denominato README_FROM_UMBRELLA.txt è stato caricato da Umbrella nel bucket S3 di Amazon e vi appare.

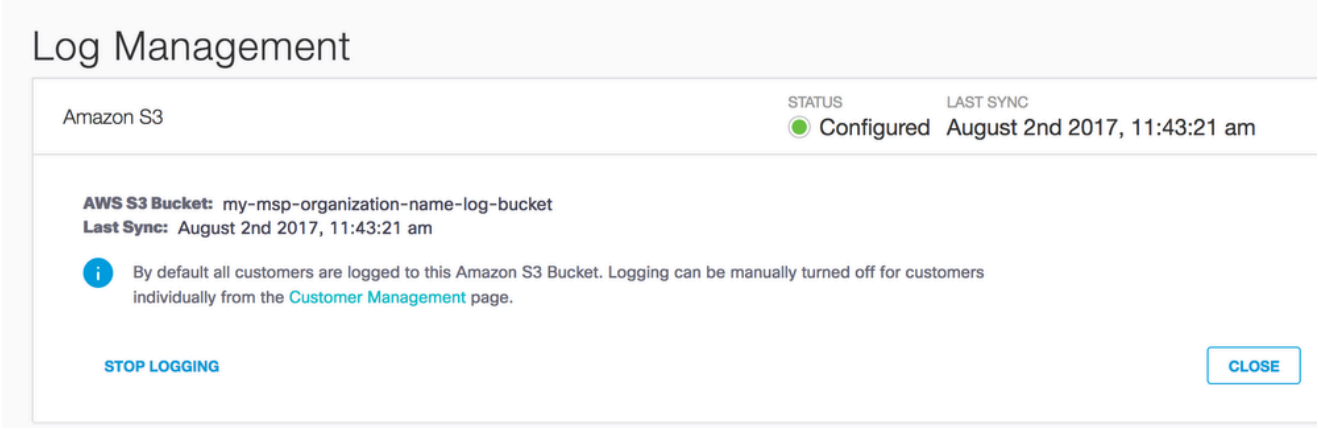
1. Scaricare il file Leggimi facendo doppio clic su di esso e quindi aprirlo in un editor di testo. All'interno del file è presente un token univoco che lega il bucket S3 al dashboard Umbrella



Nota: Potrebbe essere necessario aggiornare il bucket S3 nel browser per visualizzare il file README dopo il caricamento.

2. Torna al dashboard Umbrella e incolla il token nel campo con etichetta "Token univoco", quindi fai clic su Salva. A questo punto, la configurazione è

completato. Per rivedere la configurazione, fare clic sul nome Amazon S3 nella sezione Log Management



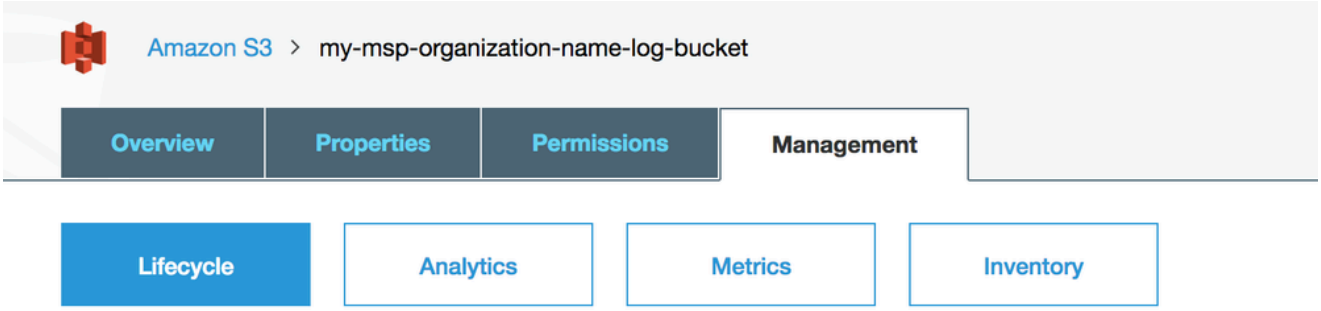
115012848126

Gestione del ciclo di vita dei log

Quando si utilizza S3, è possibile gestire il ciclo di vita dei dati all'interno del bucket per estendere la durata di conservazione dei log. A seconda del motivo per cui si utilizza la gestione del registro esterno, la durata potrebbe essere molto breve o molto lunga. Ad esempio, è possibile semplicemente scaricare i log dal bucket S3 dopo 24 ore e archiviarli offline, oppure conservarli indefinitamente nel cloud. Per impostazione predefinita, Amazon archivia i dati in un bucket in modo indefinito ma una quantità illimitata di storage aumenta il costo di manutenzione del bucket. Per ulteriori informazioni sui cicli di vita S3, leggere qui.

Per configurare il ciclo di vita del bucket:

1. Selezionare Gestione, quindi fare clic su Ciclo di vita



115012848246

2. Fare clic su Aggiungi regola, quindi su Applica la regola all'intero bucket o a una sottocartella, se configurata come tale.
3. Selezionare un'azione sugli oggetti, ad esempio Elimina o Archivia, quindi selezionare il periodo di tempo e se si desidera utilizzare lo storage Ghiacciaio per ridurre i costi Amazon. (Il ghiacciaio è che iscoldit è storage off-line, che, mentre l'accesso è più lento, è meno costoso.)

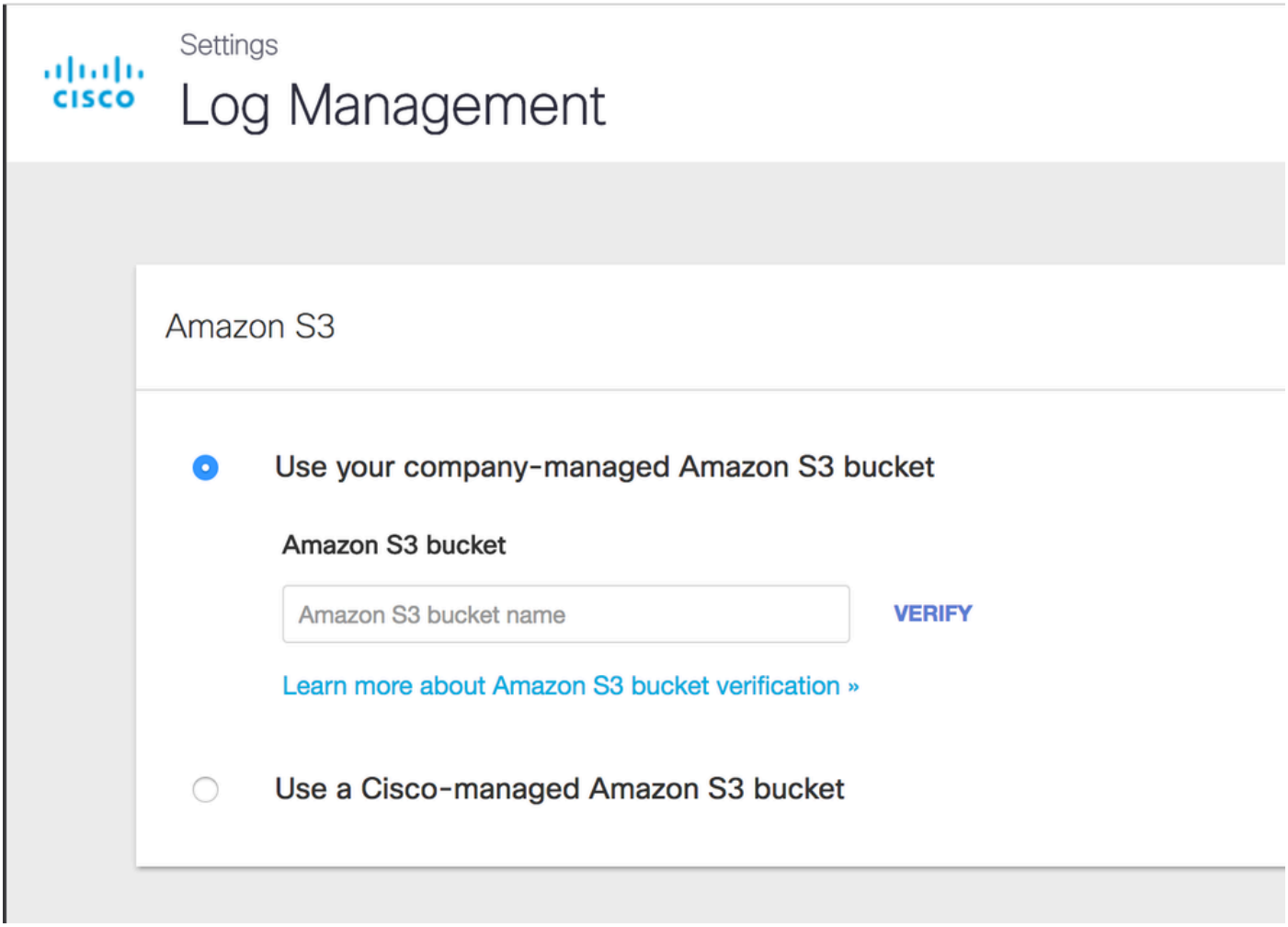
4. Se si preferisce gestire i registri con un altro metodo, ad esempio con la soluzione di backup interno, è sufficiente scaricare i registri da S3 e conservarli in un altro modo, quindi impostare il tempo di conservazione su alcuni giorni.

Configurazione di un bucket S3 gestito da Cisco

Passare a Impostazioni > Gestione log nel dashboard Umbrella.

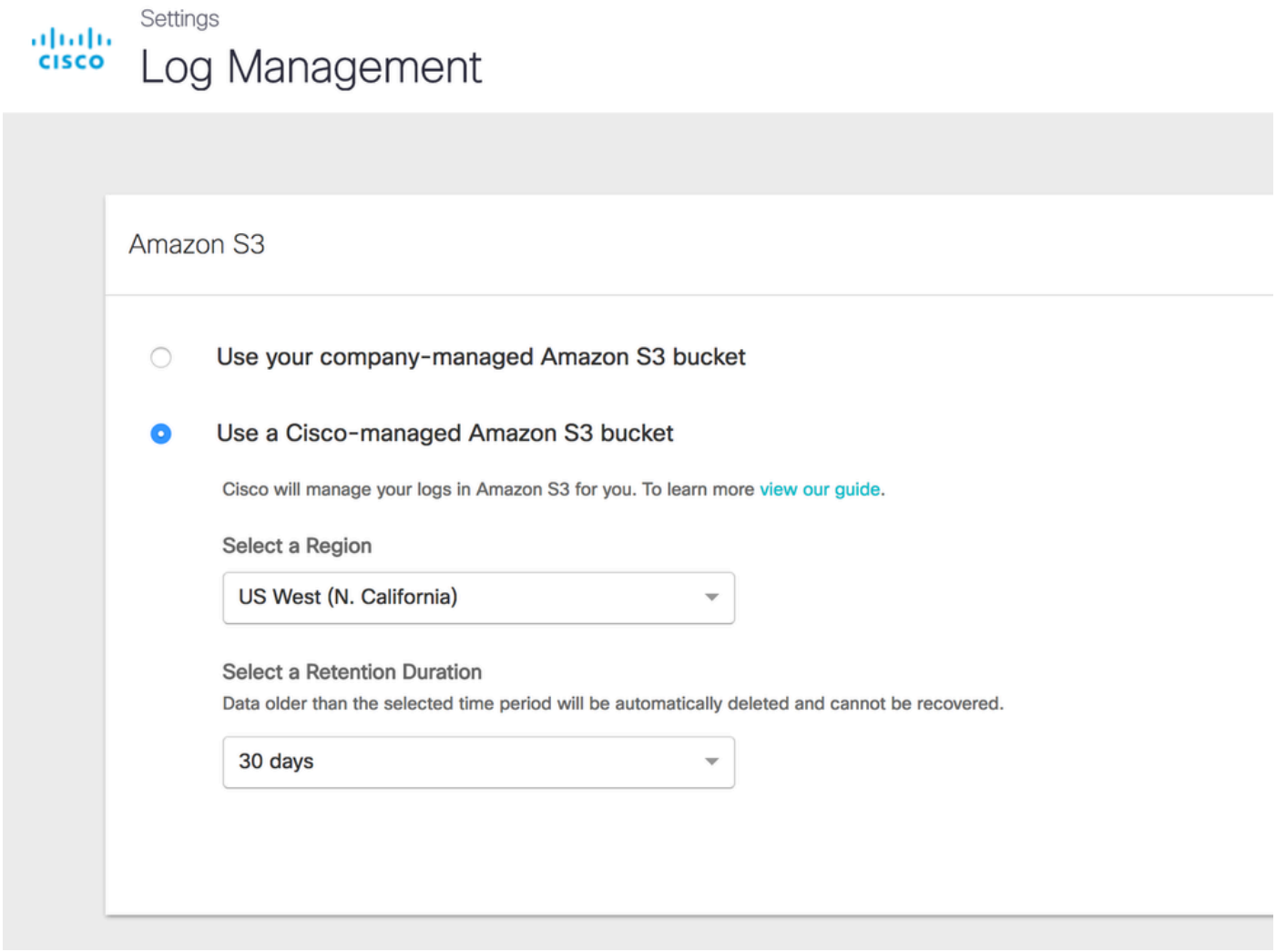
Sono disponibili due opzioni:

- Usa il secchio Amazon S3 gestito dalla tua azienda
- Usa un bucket Amazon S3 gestito da Cisco



25231151138964

Selezionare "Use a Cisco-managed Amazon S3 bucket" (Usa un bucket S3 Amazon gestito da Cisco) e sono disponibili due nuove opzioni: "Seleziona una regione" e "Seleziona una durata di conservazione".



252311511158036

Seleziona una regione

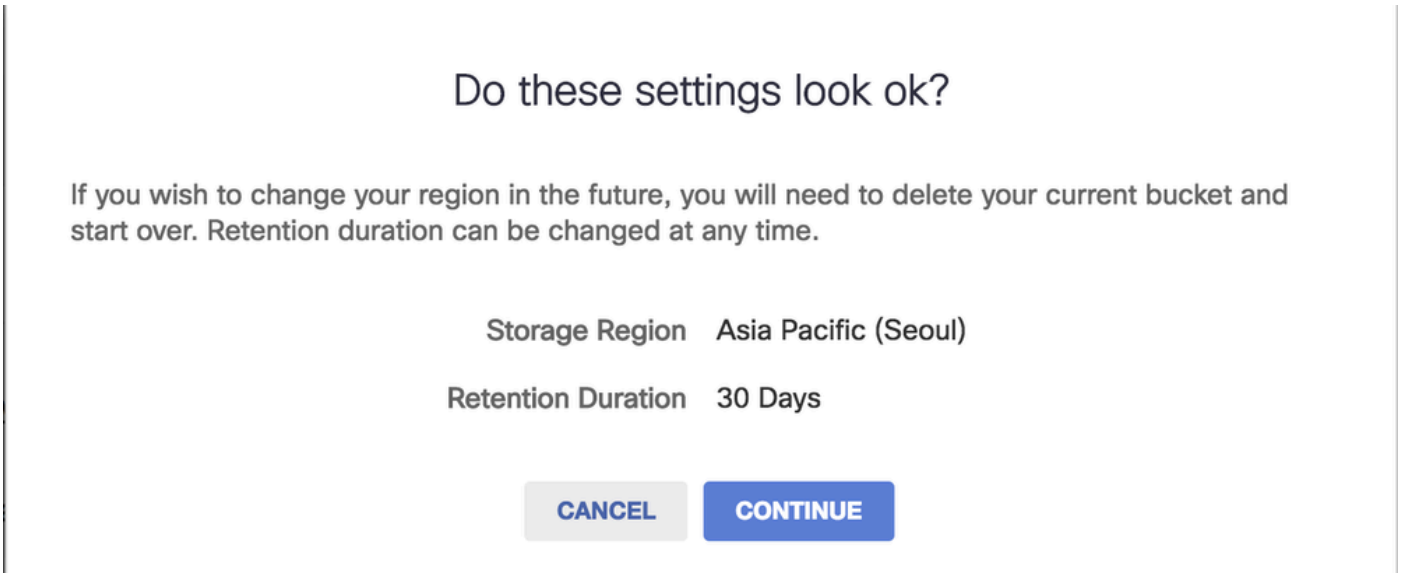
Gli endpoint regionali sono importanti per ridurre al minimo la latenza durante il download dei log nei server. Le regioni elencate corrispondono a quelle disponibili in Amazon S3, ma non tutte sono disponibili. La Cina, ad esempio, non è presente nell'elenco.

Selezionare l'area più vicina all'utente dall'elenco a discesa. Se si desidera modificare la propria regione in futuro, è necessario eliminare le impostazioni correnti e ricominciare.

Selezionare una durata di conservazione

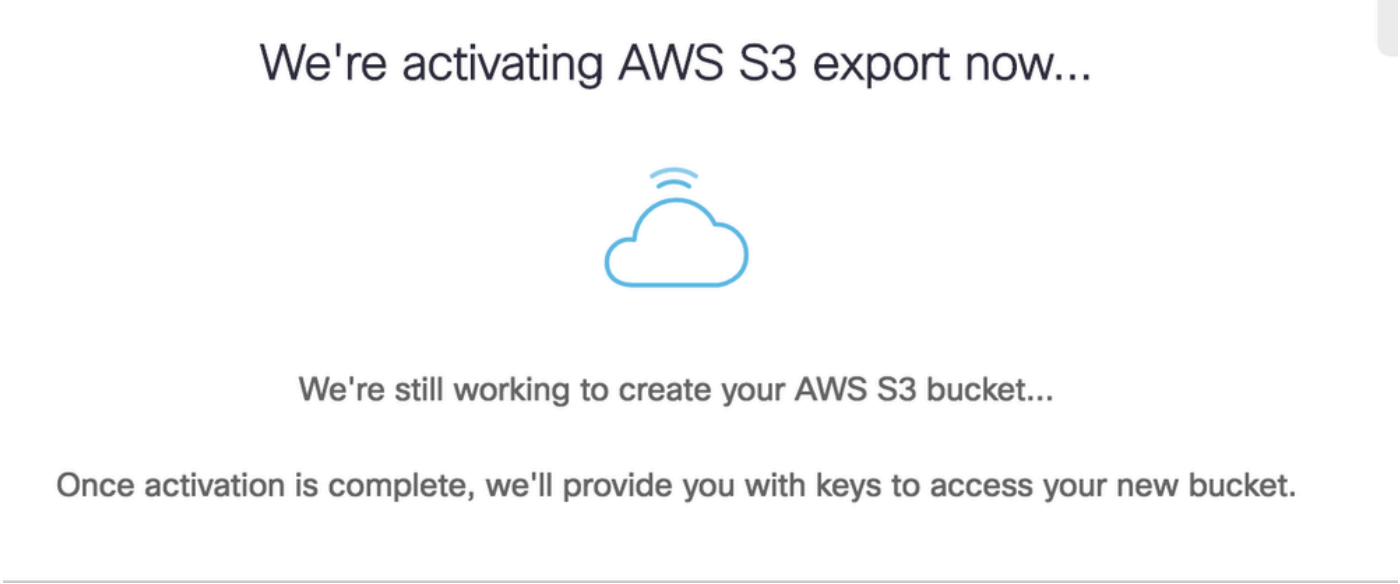
La durata di conservazione è semplicemente di 7, 14 o 30 giorni. Dopo il periodo di tempo selezionato, tutti i dati vengono eliminati e non possono essere recuperati. Se il ciclo di acquisizione è regolare, si consiglia un periodo di tempo inferiore. La durata di conservazione può essere modificata in un secondo momento.

Dopo aver effettuato le selezioni, fare clic su Avanti per confermare la regione e la durata



25231181211796

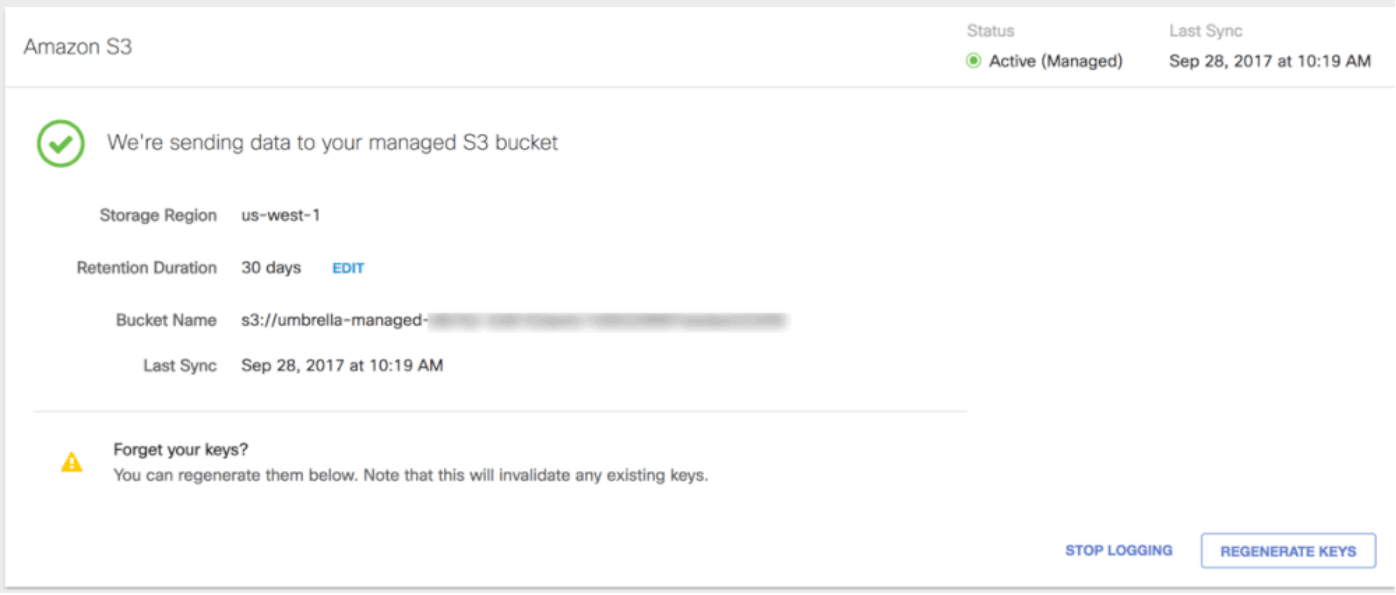
Dopo aver accettato di continuare, si riceverà una notifica di attivazione.



25231181218708

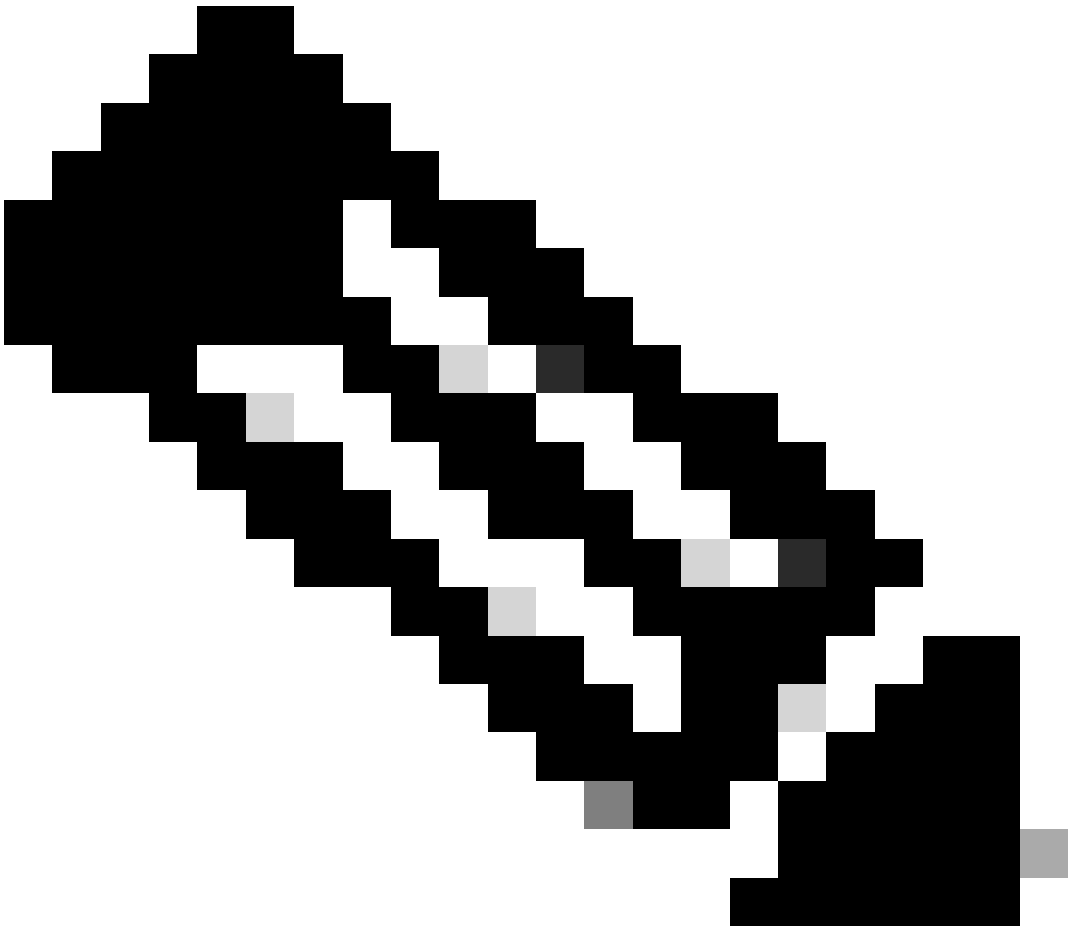
Si riceveranno quindi una chiave di accesso e la relativa chiave segreta. È necessario accettare (fare clic su "Ricevuto!") perché questa è l'unica volta che si ottiene per vedere una delle chiavi. Le chiavi di accesso e segrete sono necessarie per accedere al bucket e scaricare i log.

Infine, viene visualizzata la schermata di riepilogo che mostra la configurazione e, soprattutto, il nome del bucket.



25231181228180

È possibile attivare o disattivare la registrazione in base alle proprie esigenze.



Nota: Cisco continua a eliminare i registri in base alla durata di conservazione selezionata, anche se la registrazione è stata disattivata.

Opzioni post-configurazione

Errori di caricamento del log

In caso di mancato caricamento dei log da Cisco Umbrella nel bucket S3, è previsto un periodo di tolleranza di quattro ore durante il quale il servizio ritenta ogni 20 minuti. Dopo quattro ore, viene aperto un caso con il nostro team di supporto, che inizia un'indagine sulla causa del problema e si rivolge proattivamente a te per comunicarti il problema.

Controllo dei log caricati e della formattazione

I log vengono caricati a intervalli di dieci minuti dalla coda di log Umbrella ai bucket S3. Dopo aver completato la configurazione, il primo log viene caricato nel bucket S3 entro due ore, anche se il processo è in genere immediato o vicino all'immediato. Tuttavia, poiché il caricamento di qualsiasi elemento richiede l'esistenza di dati di log appena generati, se si sta provando a eseguire questa operazione in un ambiente di test, verificare che i dati di rete vengano registrati in Ricerca attività.

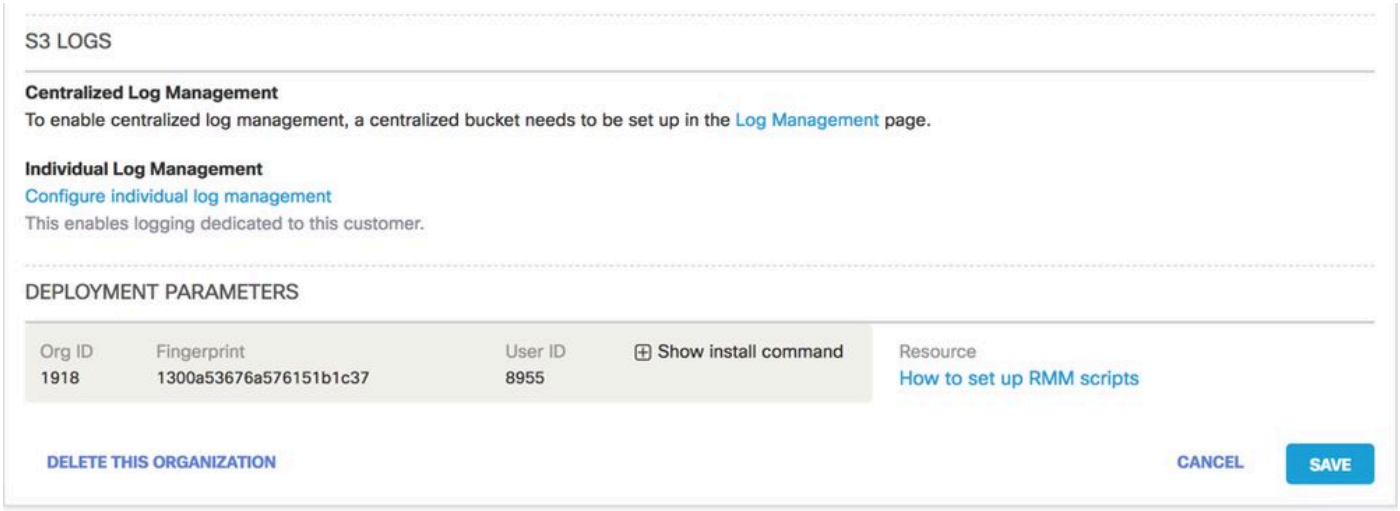
Per verificare se tutto funziona, l'ora dell'ultima sincronizzazione nel dashboard Umbrella viene visualizzata nel bucket S3.

All'interno del periodo fisso, a ogni cliente o organizzazione viene assegnata un'etichetta con il relativo ID organizzazione, in modo che la struttura della cartella sia la seguente:

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

<bucket-name> è il nome del bucket, <orgID> è l'ID dell'organizzazione e <sottocartella> sono dnslog, proxylog o iplog, a seconda dei tipi di log contenuti.

Per i clienti MSP e MSSP, l'ID organizzazione corrisponde a quello indicato in Impostazioni cliente sotto ogni dettaglio cliente nella sezione Parametri di distribuzione. I clienti di più organizzazioni possono raccogliere l'identificativo dell'organizzazione accedendo a ogni singola organizzazione secondaria e annotando l'identificativo dell'organizzazione nell'URL del browser: (https://dashboard.umbrella.com/o/######/).



360002271623

Attualmente, la versione del formato di log per i clienti MSP, MSSP e multi-org è la 1.1. I log vengono visualizzati in formato GZIP e caricati nei bucket S3 nella sottocartella appropriata con questo formato di denominazione:

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

<sottocartella> può essere dnslogs, proxylogs o iplog, a seconda dei tipi di log in cui si trova. <xxxx> è una stringa casuale di quattro caratteri alfanumerici che impedisce la sovrascrittura dei nomi di file duplicati.

Ad esempio:

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

Se non si visualizzano i registri nel bucket entro 10 minuti, contattare il supporto tecnico indicando i passaggi eseguiti fino a questo momento.

Una volta visualizzati i log, si consiglia di esaminare i dati decomprimendo il contenuto dei primi caricamenti di log ricevuti per assicurarsi che i dati siano visualizzabili in un editor di testo (o anche in Microsoft Excel, spesso l'impostazione predefinita per .CSV). Per informazioni su cui ogni campo nel registro rappresenta leggere qui.

Se il caricamento di un log da Cisco Umbrella nel bucket S3 ha esito negativo, è previsto un periodo di tolleranza di quattro ore durante il quale il servizio ritenta ogni 20 minuti. Dopo quattro ore, viene aperto un caso all'interno del team di supporto, che avvia un'indagine sulla causa del problema e si rivolge proattivamente al cliente per informarlo del problema.

Abilita registrazione per cliente

Questa funzione è abilitata per tutti i clienti, se non diversamente specificato. La funzione può essere disattivata per i singoli clienti, il che è utile se si dispone di livelli di servizio diversi per i clienti che dispongono di tale funzione. Questa è in ogni impostazione del cliente in Console. La schermata nella sezione precedente mostra come attivare o disattivare la funzione.

È inoltre possibile creare utenti IAM in Amazon e assegnare tali utenti IAM a singole sottocartelle orgit del bucket. In questo modo, è possibile consentire a un utente finale l'accesso ai propri registri, ma solo ai registri.

Scaricamento dei log, informazioni sul formato e sull'integrazione tra Splunk e QRadar

Per scaricare i log per la conservazione o il consumo, ci sono alcuni approcci per scaricare i log DNS da S3. Weit ha creato un articolo che delinea alcuni approcci a questo problema qui.

È inoltre possibile porre alcune domande sul formato del registro e su come questo differisca leggermente dai registri visualizzati nel dashboard Umbrella. Per ulteriori informazioni sul formato del registro esportato, leggere questo articolo.

Infine, uno degli utilizzi principali per l'esportazione dei registri DNS è l'integrazione con gli strumenti SIEM. Sebbene la configurazione di un SIEM quando si tratta di registri di questo tipo possa spesso dipendere dalle preferenze personali dell'amministratore, sono disponibili alcune linee guida per i SIEM più diffusi.

Per ulteriori informazioni sull'impostazione del plug-in Splunk per Amazon AWS S3 e Umbrella, leggere qui.

Per informazioni sulla configurazione di IBM QRadar per estrarre i registri da Amazon S3 e digerirli, leggere qui.

Dimensioni dei log S3

Le dimensioni dei registri S3 dipendono dal numero di eventi che si verificano, che dipende dal volume del traffico DNS.

In questa sezione è possibile trovare il formato di registrazione per S3 Logging.

La voce di esempio è 220 byte, ma le dimensioni di ogni riga di registro variano in base a un numero di elementi (lunghezza del nome di dominio, numero di categorie e così via). Supponendo che ogni linea di registro sia di 220 byte, un milione di richieste equivarrebbe a 220 MB.

Per ottenere una stima del numero di query DNS visualizzate ogni giorno:

1. Nel dashboard Umbrella, passare a Report > Ricerca attività.

2. In Filtri eseguire un report per le ultime 24 ore e quindi fare clic sull'icona Esporta CSV.
3. Aprire il file .csv scaricato. Il numero di righe (meno una per l'intestazione) è il numero di query DNS al giorno; moltiplicarlo per 220 byte per ottenere la stima per un giorno.

In termini di costo, anche se variabile, scopriamo che anche i nostri clienti più voluminosi spendono solo pochi dollari al mese per il servizio. Un costo è legato al tempo di storage e un altro al download dei dati da S3 all'ambiente. Per ulteriori dettagli, consultate Amazon.

Come per tutte le nostre funzionalità, a Weit piace sapere cosa ne pensi, soprattutto per quanto riguarda le integrazioni SIEM o qualsiasi altra domanda che viene trattata in questa documentazione. Se vuoi aggiungere un commento, contattaci!

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).