Umbrella DNS für Aruba WLAN-Administratoren bereitstellen

Inhalt

Einleitung

In diesem Dokument wird die Bereitstellung des Umbrella DNS-Service für Aruba WLAN-Administratoren beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Aruba Networks umfasst die folgenden drei Wireless LAN (WLAN)-Produktlinien und -Betriebssysteme für unterschiedliche Marktsegmente und Bereitstellungsszenarien:

- ArubaOS: für große Unternehmen und Bereitstellungen mit hoher Dichte
- Aruba Instant/InstantOS: für kleine bis mittlere Unternehmen und verteilte Unternehmen
- Aruba Instant On: für Privatanwender und Benutzer in kleinen Büros

Dieser Artikel enthält Richtlinien für Aruba WLAN-Administratoren zur Einführung und Bereitstellung des Umbrella DNS-Service.

Bereitstellungsmethoden

Die Bereitstellungsmethoden hängen von Ihrem Aruba-Betriebssystem und von Ihrer Planung für die Verwendung von Umbrella ab.

Wenn Sie eines der drei zuvor genannten Aruba Betriebssysteme verwenden, können Sie Umbrella DNS bereitstellen, indem Sie das Umbrella Benutzerhandbuch konsultieren. Video-Tutorials sind ebenfalls verfügbar.

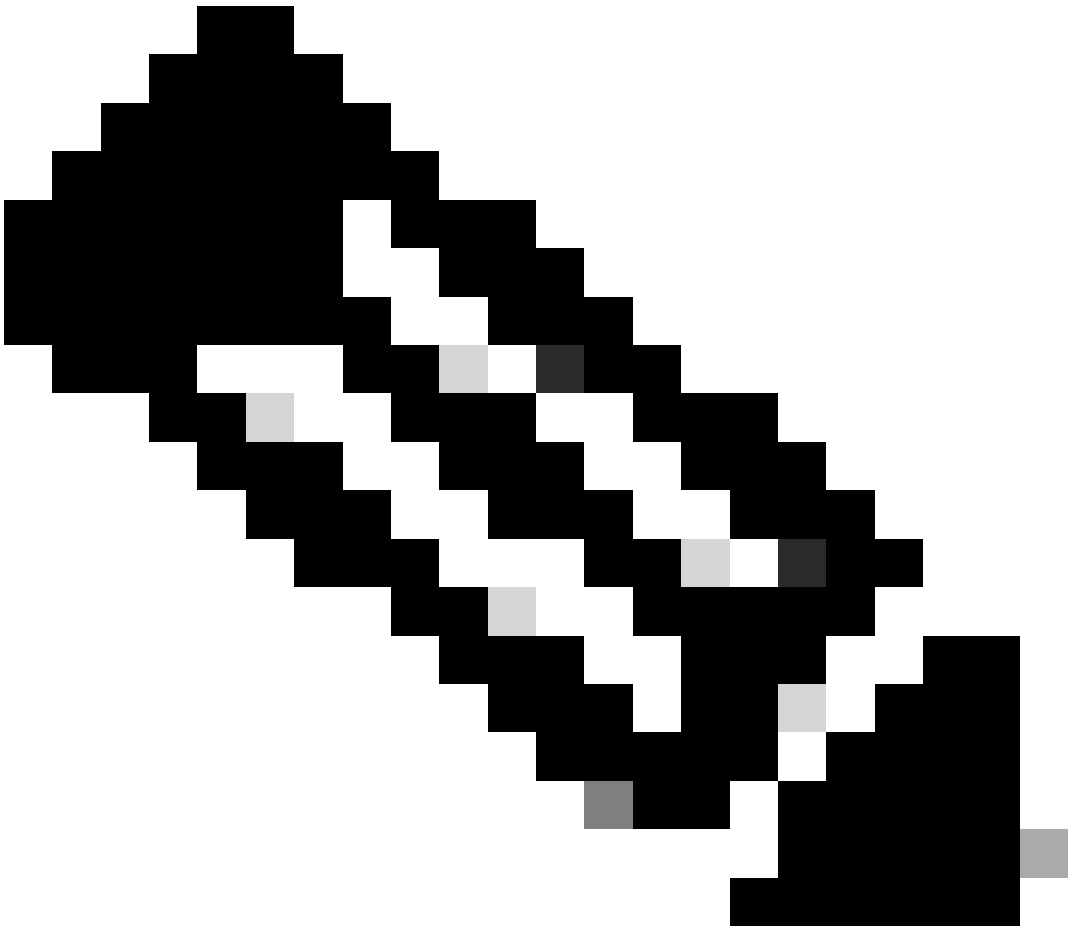
Wenn Sie Aruba Instant ausführen, haben Sie eine zusätzliche Möglichkeit, die in InstantOS verfügbare Umbrella-Netzwerkgeräteintegration zu verwenden. Beachten Sie jedoch, dass bei Auswahl dieser Option die internen/privaten IP-Adressen von Wireless-Clients im WLAN nicht in Umbrella-Berichten angezeigt werden, z. B. der Aktivitätssuchbericht. DNS-Abfragen von Clients werden den Netzwerkgeräteidentitäten der Instant AP-Cluster in Umbrella zugeordnet, und Informationen zu den einzelnen Clients sind nicht verfügbar. Aus Sicht der Umbrella Cloud können DNS-Abfragen von den Instant AP-Clustern und nicht von den Wi-Fi-Clients kommen.

Wenn Sie daher die DNS-Abfragen einzelner Clients verfolgen oder DNS-Richtlinien für einzelne Clients in einem WLAN anpassen müssen, können Sie Umbrella mithilfe der im Umbrella DNS-Benutzerhandbuch beschriebenen Standardmethoden bereitstellen (ohne die Integration der Netzwerkgeräte über Aruba Instant zu verwenden) und Umbrella virtuelle Appliances in ihre Bereitstellungspläne einbeziehen.

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

Aruba Instant-Integration

Die Netzwerkgeräteintegration von Aruba Instant's Umbrella (OpenDNS) kann in Umgebungen von Vorteil sein, in denen alle Wi-Fi-Clients, die mit einem Instant AP-Cluster verbunden sind, einer einzigen Umbrella DNS-Richtlinie unterliegen und in denen es nicht erforderlich ist, die DNS-Abfragen einzelner Clients in Umbrella-Berichten zu überprüfen. In diesem Abschnitt wird erläutert, wie Sie die Integration einrichten.



> Anmerkung: Bei der Integration wird eine ältere Version der Umbrella-API für Netzwerkgeräte verwendet. In der alten Version müssen Kunden keine API-Token aus ihren Umbrella-Dashboards generieren, in den neueren Versionen ist dies jedoch der Fall.

Umbrella Legacy-APIs haben am 01.09.2023 das Ende ihres Lebenszyklus erreicht. Nach diesem Datum wird die Integration nicht mehr unterstützt. Wenn bei der Integration nach dem 01.09.2023 Probleme auftreten, füllen Sie bitte den Abschnitt "Erste Schritte" im Bereitstellungsleitfaden aus, um Umbrella ohne die Integration bereitzustellen.

Um die Integration nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Auf den APs muss InstantOS Version 8.10.0.1 oder höher ausgeführt werden (Stand: Mai 2022).
- Das für die Integration verwendete Umbrella Dashboard-Konto muss die Rolle "Full Admin" haben.
- Die E-Mail-Adresse des Kontos kann nicht mehr als einem Umbrella Dashboard zugeordnet werden. Wenn Sie sich nicht sicher sind, ob die E-Mail-Adresse nur mit einem Dashboard verknüpft ist, können Sie sich an den Cisco Umbrella Support wenden, um dies zu überprüfen.
- Single Sign-on (SSO) und Two-Factor Authentication (2FA) können für das Konto nicht aktiviert werden.
- Wenn zwischen den APs und dem Internet eine Netzwerksicherheits-Appliance (wie eine Firewall) vorhanden ist, muss die Appliance ungefilterte und nicht überprüfte Verbindungen mit den Appliances 208.67.220.220, 208.67.222.222, 67.215.92.210 zulassen. 146.112.255.152/29 (.152 ~ .159).

Konfiguration

Auf oberster Ebene gibt es vier Konfigurationsschritte für die Integration:

1. Legen Sie einen Namen für das AP-Cluster fest.

2. Geben Sie Anmeldeinformationen ein.

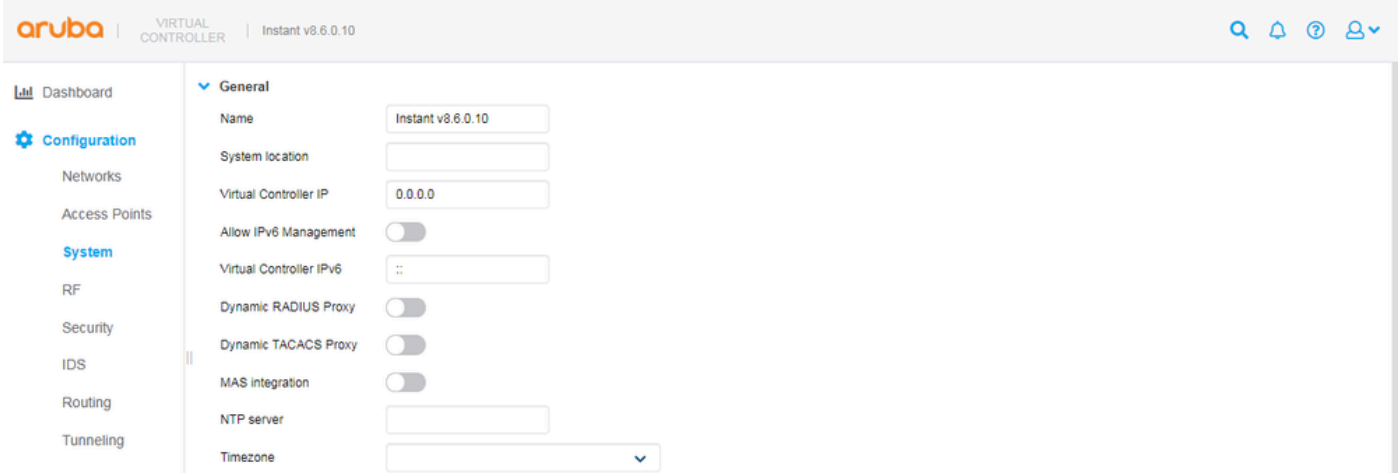
3. DNS-Abfragen abfangen

4. Anwenden der DNS-Richtlinie

Festlegen eines Namens für den AP-Cluster

Wenn sich ein Instant-Cluster zum ersten Mal erfolgreich bei einem Umbrella Dashboard registriert, wird dem Umbrella Dashboard unter Bereitstellungen > Netzwerkgeräte ein Netzwerkgeräteeintrag hinzugefügt. Der Gerätename eines neuen Eintrags stammt aus dem Systemnamen, der auf dem virtuellen Controller eines Clusters konfiguriert wurde.

Um den Systemnamen auf einem virtuellen Instant Controller festzulegen, navigieren Sie zu Configuration > System.



4404011628308

Beachten Sie, dass der Namenswert bei der Erstregistrierung nur einmal kopiert wird. Wenn ein System-/Gerätename auf der Instant- oder Umbrella-Seite geändert wird, müssen Sie den Namen auf der anderen Seite manuell aktualisieren.

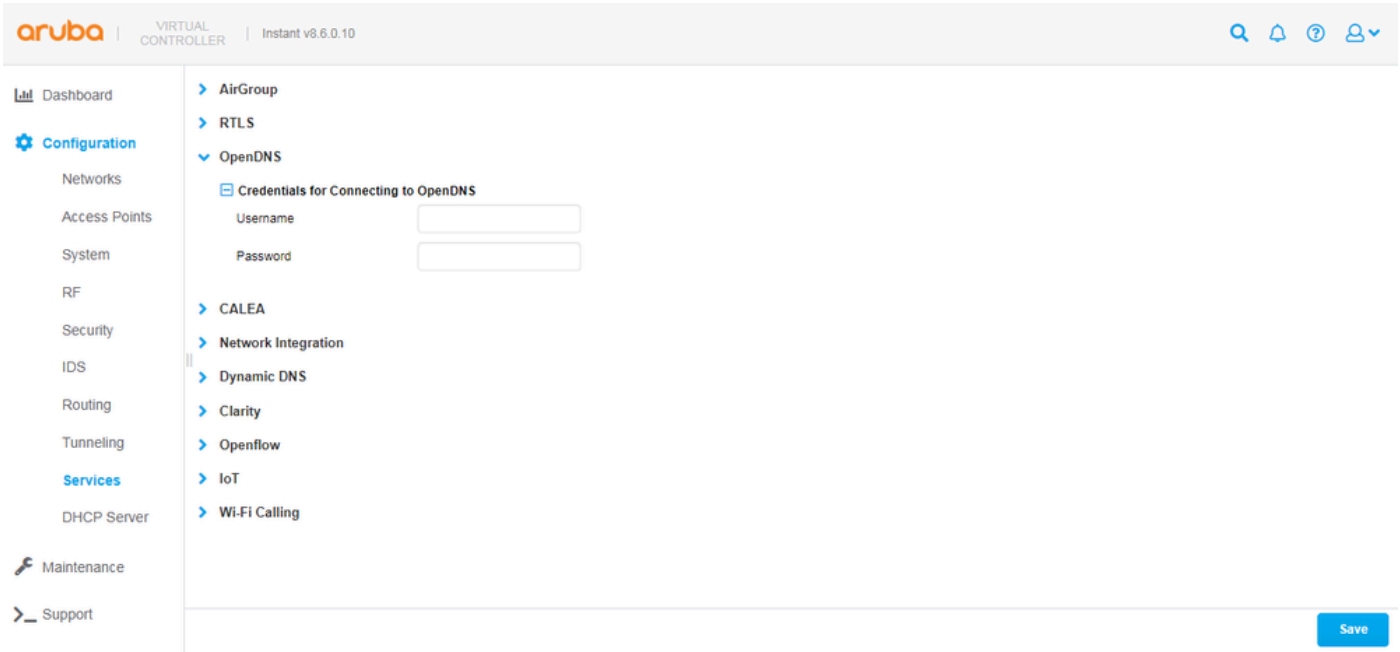
Kontoanmeldeinformationen eingeben

Wenn die im Abschnitt Voraussetzungen aufgeführten Anforderungen erfüllt sind, können Sie Ihrem Umbrella Dashboard als Netzwerkgerät einen Instant Cluster hinzufügen. Gehen Sie dazu vom virtuellen Controller eines Clusters aus wie folgt vor:

1. Navigieren Sie zu Konfiguration > Dienste > OpenDNS.

2. Geben Sie die Anmeldeinformationen eines Umbrella-Kontos ein.

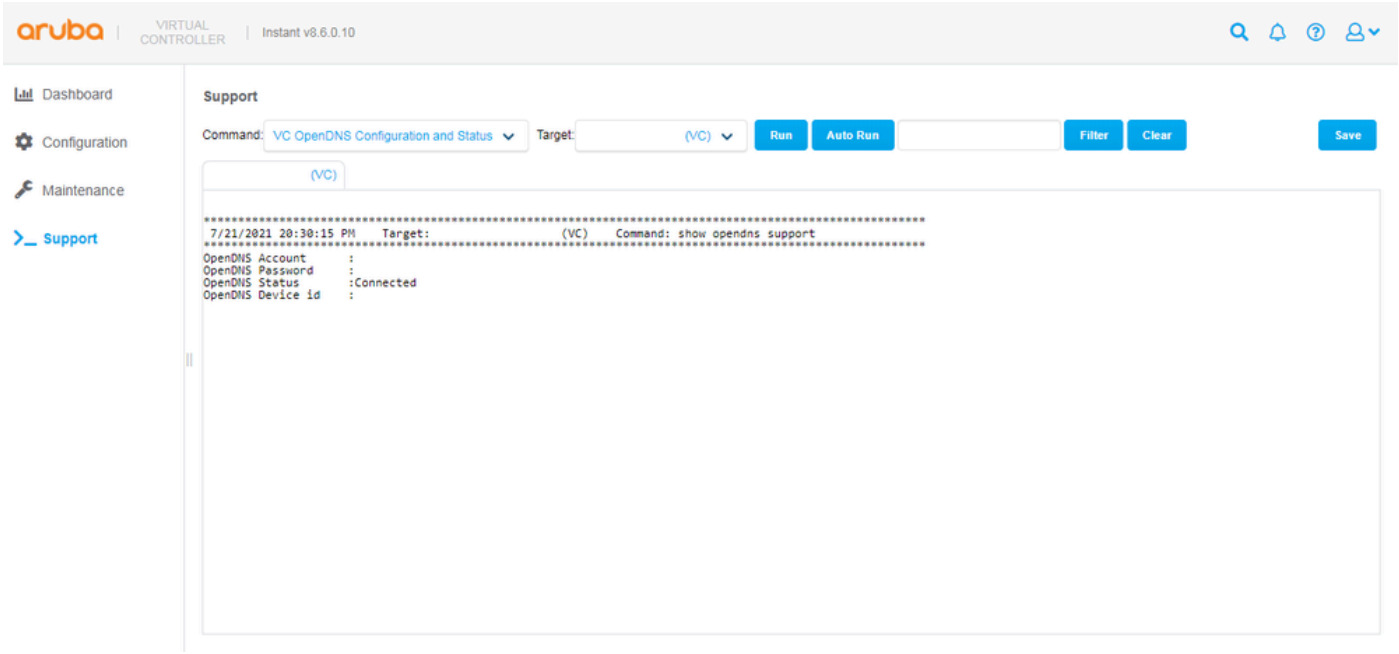
3. Wählen Sie Speichern.



4404019266196

Wenn der virtuelle Controller (VC) erfolgreich eine Verbindung zu Umbrella herstellt, wird der Status Verbunden angezeigt, wenn Sie zu Support navigieren und den Befehl "VC OpenDNS Configuration and Status" (`show opendns support`) ausführen.

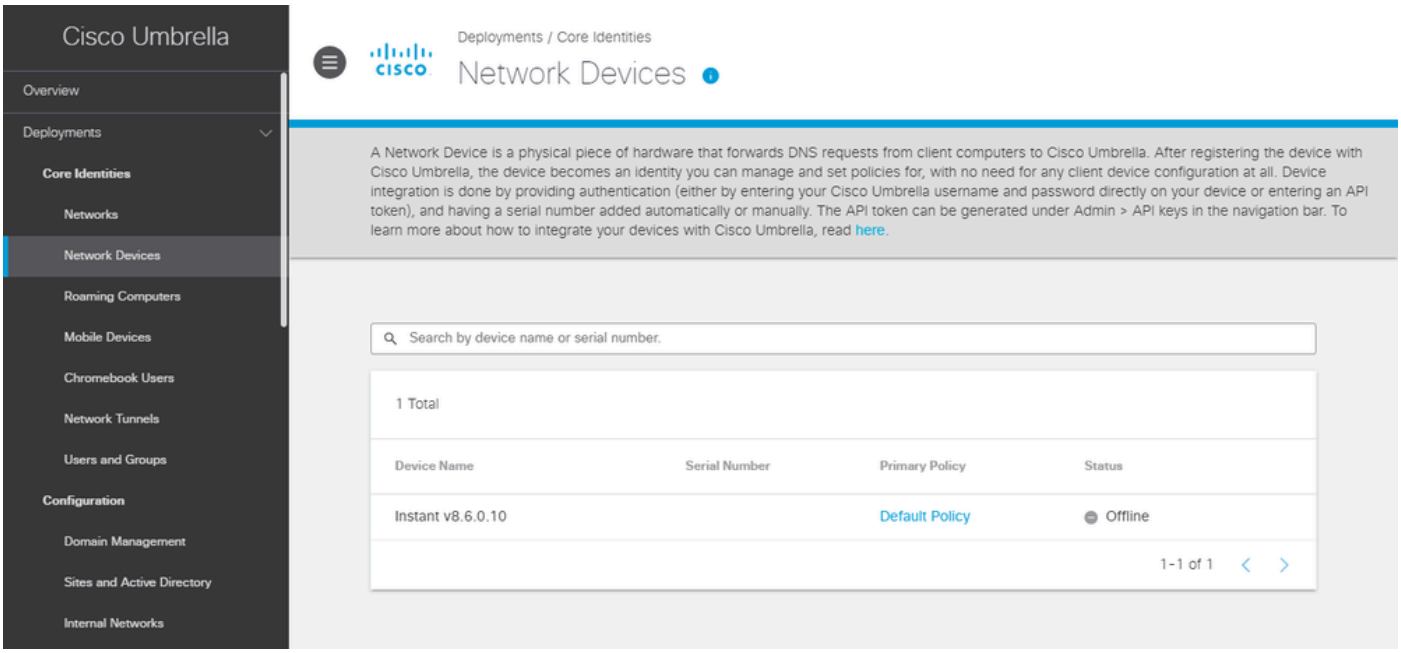
Sie können auch eine Geräte-ID sehen, die von Umbrella generiert wird, wenn ein neues Netzwerkgerät erstellt und in der Instant VC-Konfiguration gespeichert wird. Letzterer Teil ist wichtig. Da jeder Instant-Cluster über eine eindeutige Umbrella-Netzwerkgerät-ID verfügen muss, darf die Geräte-ID nicht von der Konfiguration eines Clusters in eine andere kopiert werden. Eine gültige Geräte-ID besteht in der Regel aus 16 Ziffern.



4404019268116

Wenn die Befehlsausgabe den Status Nicht verbunden anzeigt, können Sie versuchen, den Grund herauszufinden, indem Sie "AP Tech Support Dump" (`show tech-support`) und "AP Tech Support Dump Supplemental" (`show tech-support additional`)-Befehle ausführen und dann in den Protokollen nach "OpenDNS" suchen. Die Befehlsausgaben können zur Fehlerbehebung auch an das Aruba TAC weitergegeben werden.

Wenn alles korrekt funktioniert, können Sie einen neuen Eintrag im Umbrella Dashboard unter Bereitstellungen > Netzwerkgeräte sehen, wo Sie nach einem Instant AP Cluster anhand seines Namens suchen oder einen vorhandenen Eintrag löschen können, wenn Sie eine neue Geräte-ID generieren möchten.



4404011658516

Abfangen von DNS-Abfragen

Wenn Sie bestätigen, dass ein Cluster erfolgreich als Netzwerkgerät zu Ihrem Umbrella Dashboard hinzugefügt wurde, können Sie festlegen, dass der Cluster DNS-Abfragen abfangen soll, die von Wireless-Clients gesendet werden (die mit den APs im Cluster verbunden sind). Nach der Einrichtung können die DNS-Abfragen der Clients unabhängig von den IP-Adressen der DNS-Server auf den Netzwerkkarten der Wireless-Clients vom Cluster abgefangen und an die Anycast-Resolver von Umbrella unter 208.67.220.220 und 208.67.222.222 weitergeleitet werden.

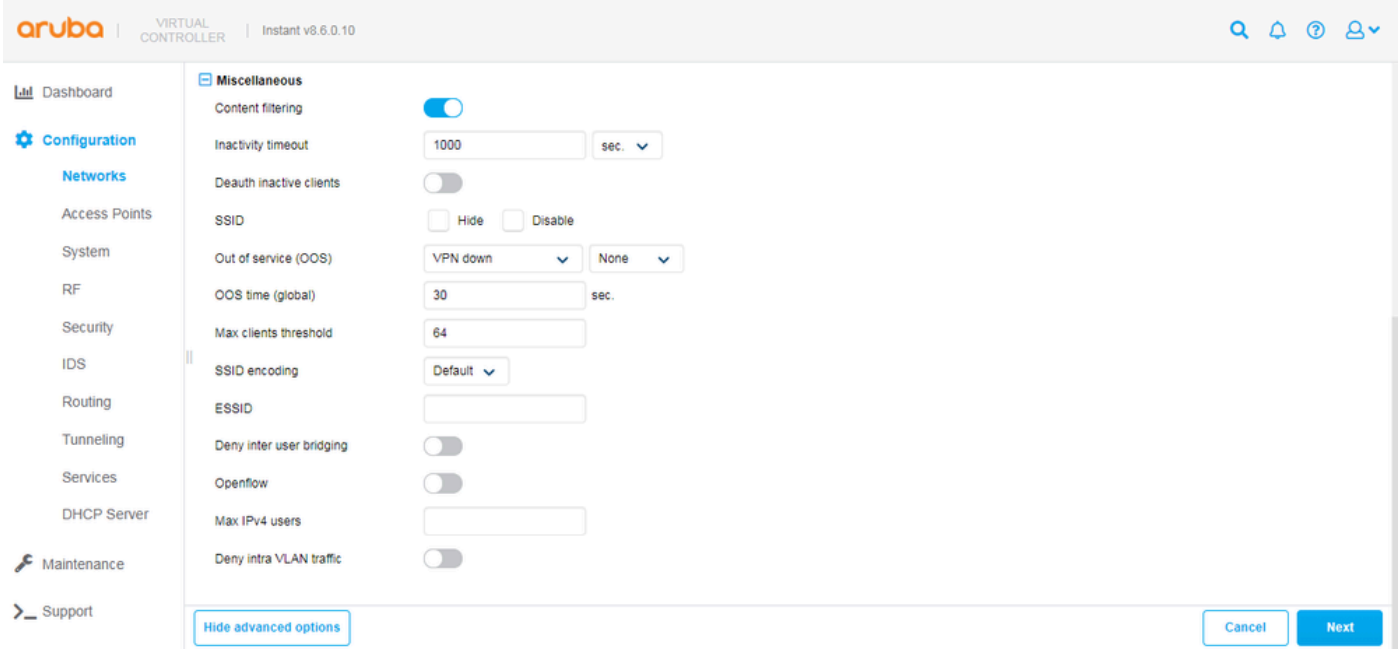
So unterbrechen Sie DNS-Abfragen:

1. Navigieren Sie zum virtuellen Controller eines Clusters unter Konfiguration > Netzwerke.

2. Wählen Sie ein Wireless-Netzwerk aus.

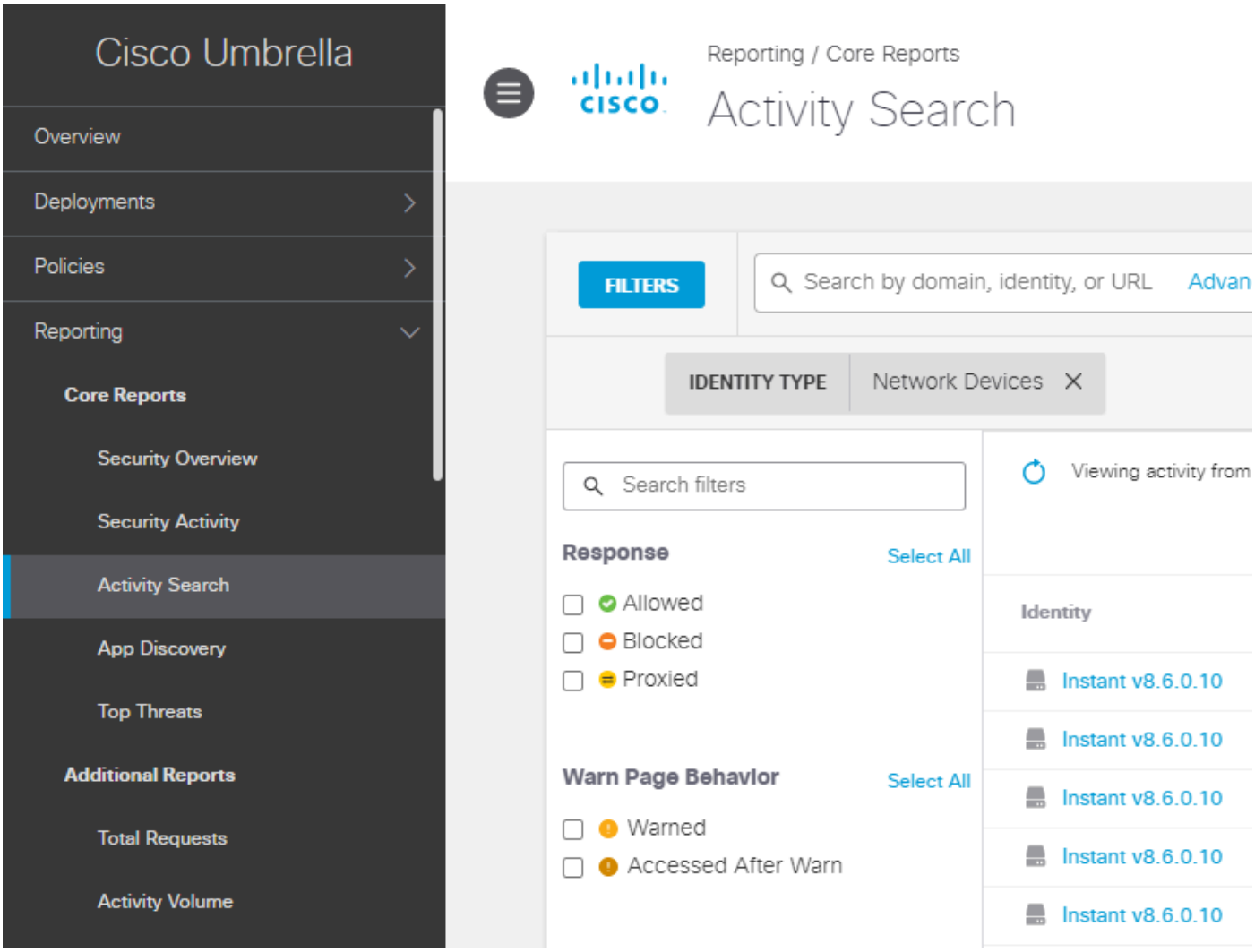
3. Bearbeiten Sie das Netzwerk, wählen Sie Erweiterte Optionen anzeigen aus, und blättern Sie zum Abschnitt Verschiedenes.

4. Aktivieren Sie die Option Inhaltsfilter, und wählen Sie Weiter aus, bis Sie die Schaltfläche Beenden auswählen können, um die Änderung zu speichern.



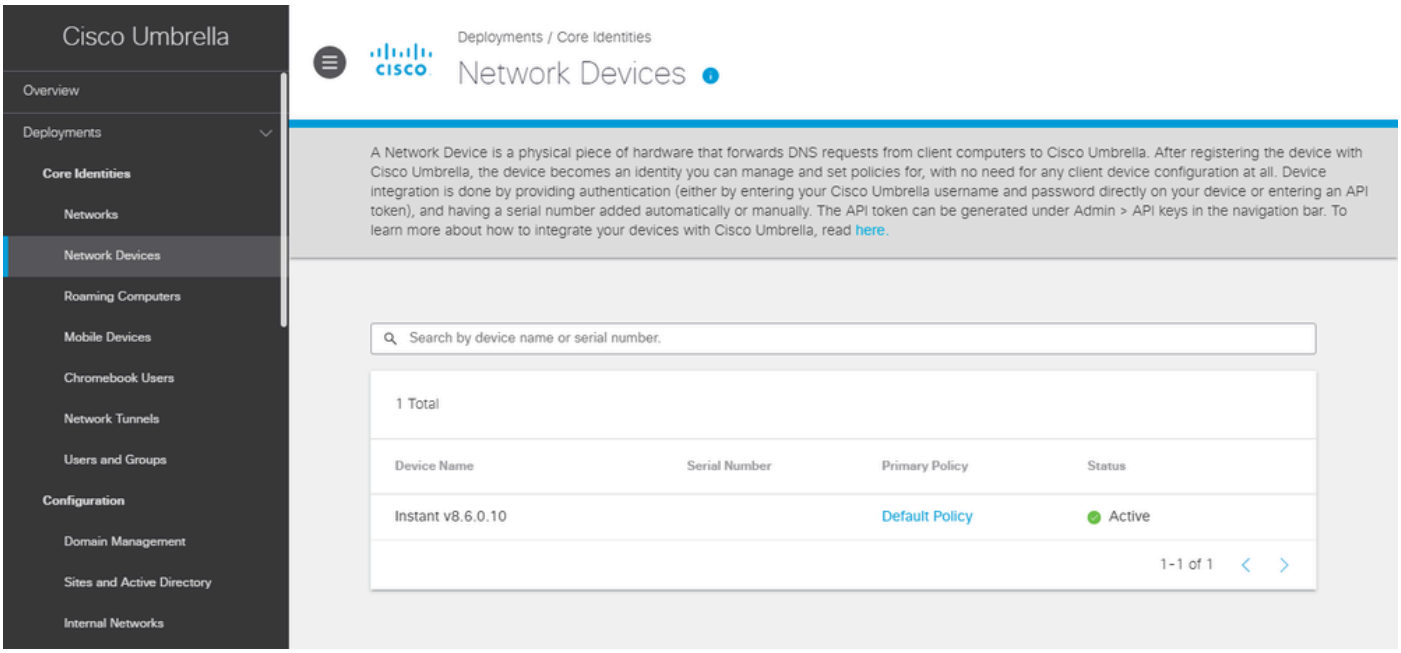
4404011668500

Nachdem die Option aktiviert wurde, können Sie DNS-Abfragen im Umbrella Dashboard unter Reporting > Activity Search anzeigen.Die Identität der Abfragen kann einem Netzwerkgerätenamen zugeordnet werden, der in der Regel der Systemname ist, der auf dem virtuellen Controller eines AP-Clusters konfiguriert ist. Beachten Sie, dass es einige Zeit (ca. 15 Minuten) dauern kann, bis Abfragen verarbeitet und in der Dashboard-GUI angezeigt werden.



4404011721620

Im Umbrella Dashboard unter Deployments > Network Devices kann es bis zu 24 Stunden dauern, bis ein Gerät in einen Aktiv/Online-Status wechselt. Der Status eines Netzwerkgeräts gibt lediglich an, ob DNS-Anfragen vom Gerät abgefangen und in den 24 Stunden zuvor an Umbrella weitergeleitet wurden. Die Kommunikation zwischen einem Gerät und Umbrella wird dadurch nicht beeinflusst. Ein Offline/Inaktiv-Status kann einfach bedeuten, dass in den letzten 24 Stunden kein Wireless-Client mit einem AP-Cluster verbunden war, und kann den Cluster nicht daran hindern, den Umbrella-Service zu nutzen.

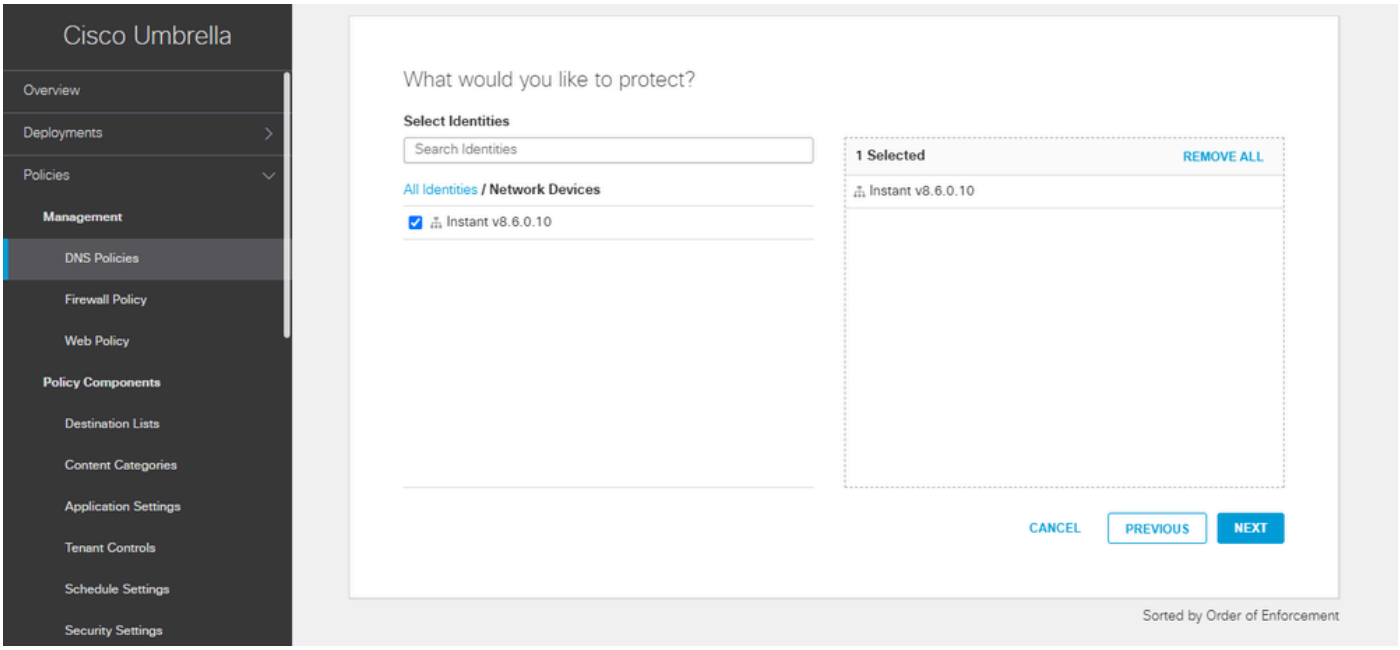


4404011756308

DNS-Richtlinie anwenden

Bei Umbrella umfasst die "Standardrichtlinie" automatisch alle Identitäten (wie Netzwerkgeräte), die einem Dashboard hinzugefügt wurden. Es ist nicht erforderlich, zusätzliche DNS-Richtlinien zu erstellen, wenn für alle AP-Cluster in Ihrer Bereitstellung dieselbe Richtlinie gelten kann. Wenn dies für Sie der Fall ist, fahren Sie mit dem nächsten Abschnitt fort.

Wenn Sie eine benutzerdefinierte Richtlinie auf ein bestimmtes Netzwerkgerät anwenden möchten, müssen Sie eine neue Richtlinie im Umbrella Dashboard unter Policies > All Policies (DNS Policies) (Richtlinien > Alle Richtlinien (DNS-Richtlinien) hinzufügen und das Netzwerkgerät in der Richtlinie auswählen.



4404011773588

Wenn auf der Seite "DNS Policies (All Policies)" (DNS-Richtlinien (Alle Richtlinien)) mehr als eine Richtlinie vorhanden ist, werden die Richtlinien von oben nach unten auf Basis der ersten Übereinstimmung ausgewertet. Weitere Informationen finden Sie in der Dokumentation zum Richtlinienvorrang und den Best Practices für die Definition von Richtlinien.

Interner DNS

In einer Umgebung, in der interne DNS-Server vorhanden sind und Sie DNS-Abfragen für bestimmte (interne) Domänen an die internen DNS-Server weiterleiten möchten, können Sie die Funktion Enterprise Domains in Instant verwenden.

DNS-Abfragen können vom AP-Cluster weiterhin abgefangen werden, nachdem die Funktion aktiviert wurde, mit der Ausnahme, dass Abfragen für die angegebenen Domänen nicht mehr an Umbrella weitergeleitet werden können. Stattdessen können sie an die IP-Adressen des DNS-Servers weitergeleitet werden, die ursprünglich auf den Netzwerkkarten der Wireless-Clients konfiguriert waren (wie etwa über DHCP). Diese Funktion ähnelt der Funktionalität interner Domänen, die bei Standardbereitstellungsmethoden für Umbrella (mit virtuellen Appliances) verfügbar ist, bei denen die Aruba Instant-Integration nicht verwendet wird.

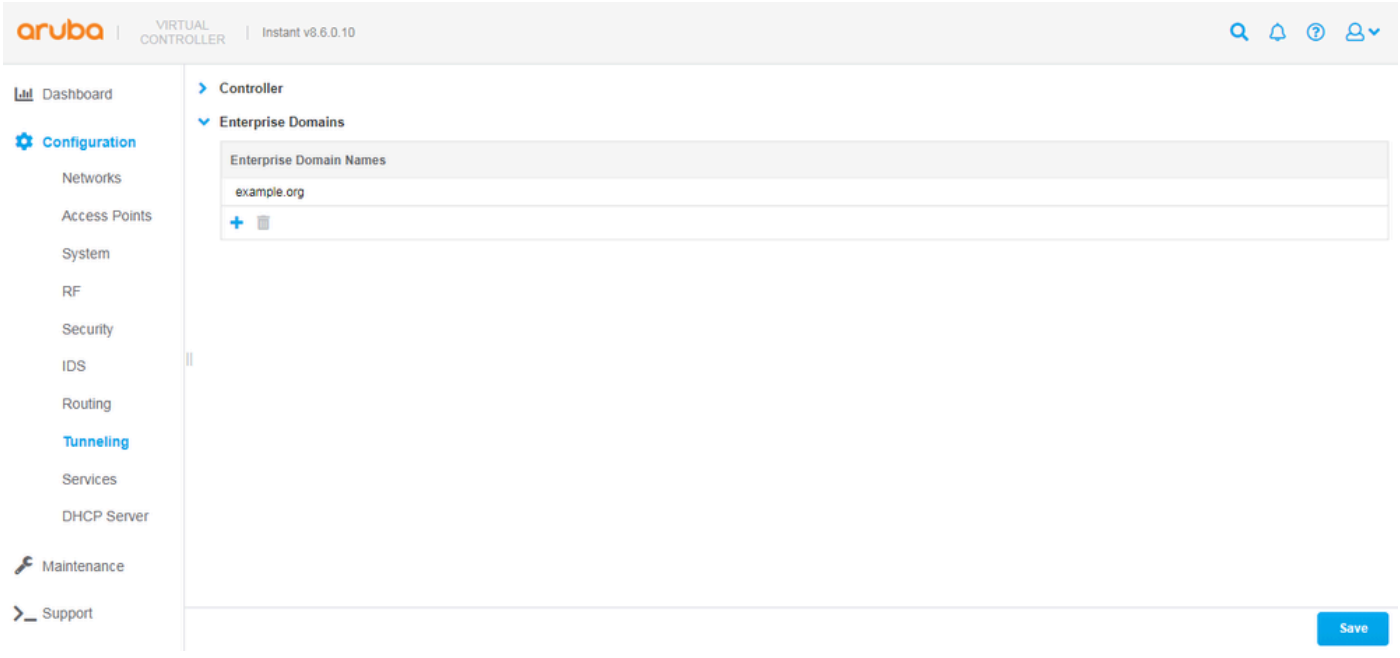
So konfigurieren Sie die Funktion auf einem virtuellen Instant Controller:

1. Navigieren Sie zu Configuration > Tunneling > Enterprise Domains (Konfiguration > Tunneling > Enterprise-Domänen).

2. Fügen Sie der Liste Enterprise Domain Names Domänen hinzu, oder entfernen Sie Domänen aus dieser Liste.

3. Wählen Sie Speichern.

Es gibt einen impliziten Platzhalter für alle Domänen, die der Liste hinzugefügt werden. example.org impliziert daher *.example.org.



4404238114452

Verifizierung

Unabhängig davon, ob Sie Umbrella mithilfe der im Abschnitt "Übersicht über die Bereitstellung" dieses Leitfadens genannten Standardmethoden in Ihrem WLAN bereitgestellt haben oder die im Abschnitt "Aruba Instant Integration" beschriebene Integration, können Sie überprüfen, ob Wireless-Clients Umbrella DNS verwenden, indem Sie von einem der Clients aus zu https://welcome.umbrella.com/ navigieren. Dann sehen Sie ein grünes Häkchen ähnlich dem Screenshot, der in der Umbrella-Dokumentation angezeigt wird.

4404011960212

Alternativ können Sie dies überprüfen, indem Sie diesen Befehl in der Eingabeaufforderung eines Wireless-Clients ausführen.

```
nslookup -type=txt debug.opendns.com.
```

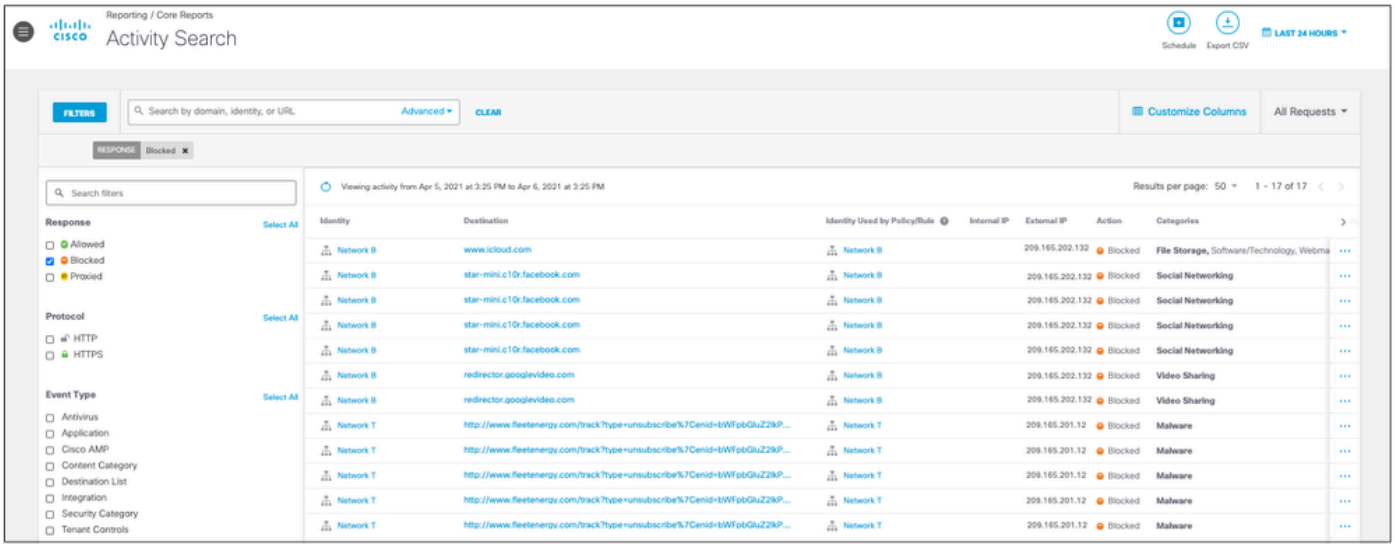
Sie können eine Ausgabe mit einer Anzahl von Textzeilen sehen, ähnlich wie in diesem Screenshot:

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id [redacted]
debug.opendns.com       text = "appliance id [redacted]
debug.opendns.com       text = "host id [redacted]
debug.opendns.com       text = "user id [redacted]
debug.opendns.com       text = "remoteip [redacted]
debug.opendns.com       text = "flags [redacted]
debug.opendns.com       text = "id [redacted]
debug.opendns.com       text = "source [redacted]
debug.opendns.com       text = "fw: flags [redacted]
debug.opendns.com       text = "fw: id [redacted]
debug.opendns.com       text = "fw: source [redacted]

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

Aus der Befehlsausgabe können Sie die Org-ID Ihres Umbrella-Dashboards in der Zeile "orgid" oder "organisation id" sehen, und wenn Sie die Instant-Integration verwenden, können Sie die zusätzliche Zeile "device" sehen, die eine Geräte-ID enthält.

Um DNS-Abfragen in Ihrem Umbrella Dashboard zu überprüfen, navigieren Sie zu Reporting > Activity Search. Beachten Sie, dass es einige Zeit (ca. 15 Minuten) dauern kann, bis Abfragen in der Dashboard-GUI angezeigt werden. Anleitungen zur Verwendung der Aktivitätssuche finden Sie in der Umbrella-Dokumentation unter.



4404019393044

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.