Distribuire il DNS Umbrella per gli amministratori WLAN Aruba

Sommario

Introduzione

Questo documento descrive come distribuire il servizio Umbrella DNS per gli amministratori WLAN Aruba.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Aruba Networks offre tre linee di prodotti WLAN (Wireless LAN) e sistemi operativi per diversi segmenti di mercato e scenari di implementazione:

- ArubaOS: per organizzazioni di grandi dimensioni e installazioni ad alta densità
- Aruba Instant/InstantOS: per le piccole e medie imprese e le imprese distribuite
- Aruba Instant On (Attivato): per utenti privati e piccoli uffici

In questo documento vengono fornite le linee guida per l'adozione e la distribuzione del servizio DNS Umbrella da parte degli amministratori WLAN di Aruba.

Metodi di distribuzione

I metodi di installazione dipendono dal sistema operativo Aruba utilizzato e da come si intende utilizzare Umbrella.

Se si esegue uno dei tre sistemi operativi Aruba precedentemente menzionati, è possibile iniziare a distribuire Umbrella DNS consultando la Guida per l'utente Umbrella. Sono inoltre disponibili esercitazioni video.

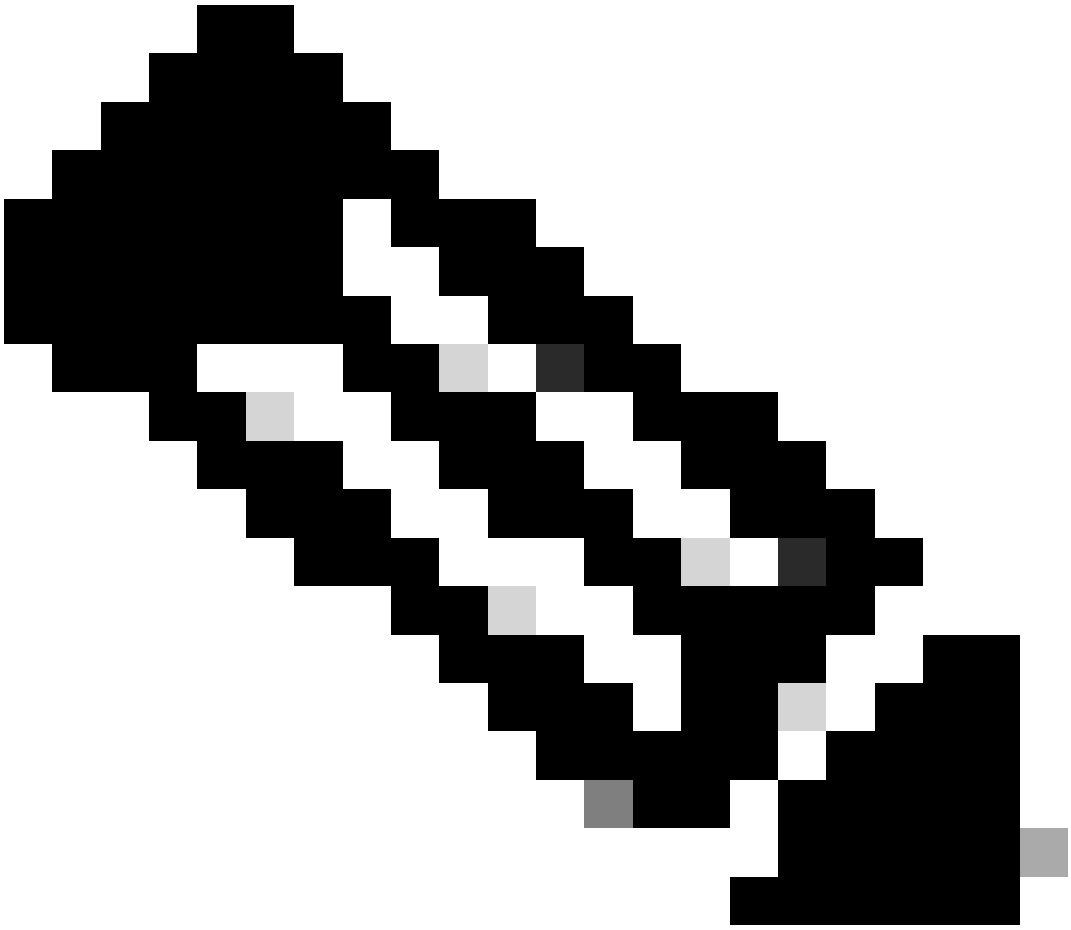
Se si esegue Aruba Instant, è disponibile un'opzione aggiuntiva per utilizzare l'integrazione dei dispositivi di rete Umbrella disponibile in InstantOS. Si noti, tuttavia, che se si sceglie questa opzione, non è possibile visualizzare gli indirizzi IP interni/privati dei client wireless sulla WLAN in Umbrella reporting, ad esempio il report Ricerca attività. Le query DNS dai client vengono mappate alle identità dei dispositivi di rete dei cluster Instant AP in Umbrella e le informazioni relative ai singoli client non sono disponibili. Dal punto di vista del cloud Umbrella, le query DNS possono sembrare provenienti dai cluster Instant AP piuttosto che dai client Wi-Fi.

Pertanto, se è necessario tenere traccia delle query DNS dei singoli client o personalizzare i criteri DNS per i singoli client su una WLAN, è possibile distribuire Umbrella tramite i metodi standard descritti nella guida per l'utente di Umbrella DNS (senza utilizzare l'integrazione dei dispositivi di rete tramite Aruba Instant) e prendere in considerazione l'inclusione di appliance virtuali Umbrella nei loro piani di distribuzione.

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.

Integrazione immediata di Aruba

L'integrazione dei dispositivi di rete Umbrella (OpenDNS) di Aruba Instant può essere vantaggiosa in ambienti in cui tutti i client Wi-Fi connessi a un cluster Instant AP sono soggetti a una singola regola DNS Umbrella e in cui non è necessario esaminare le query DNS dei singoli client nei report Umbrella. Questa sezione spiega come impostare l'integrazione.



> Nota: L'integrazione utilizza una versione legacy dell'API dei dispositivi di rete di Umbrella. La versione precedente non richiede ai clienti di generare token API dai propri dashboard Umbrella, a differenza delle versioni più recenti.

Le API legacy Umbrella hanno raggiunto la fine del ciclo di vita il 2023-09-01, dopodiché non viene più fornito il supporto per l'integrazione. In caso di problemi con l'integrazione dopo il 2023-09-01, completare la sezione "Guida introduttiva" nella guida alla distribuzione per distribuire Umbrella senza utilizzare l'integrazione.

Per utilizzare l'integrazione è necessario soddisfare i seguenti requisiti:

- Gli access point devono eseguire InstantOS versione 8.10.0.1 o successive (a maggio 2022).
- L'account dashboard Umbrella utilizzato per l'integrazione deve avere il ruolo di amministratore completo.
- L'indirizzo di posta elettronica dell'account non può essere associato a più dashboard Umbrella. Se non si è certi che l'indirizzo e-mail sia associato solo a un singolo dashboard, è possibile contattare il supporto Cisco Umbrella per la verifica.
- Impossibile abilitare l'Single Sign-On (SSO) e l'autenticazione a due fattori (2FA) per l'account.
- Se tra i punti di accesso e Internet è presente un'appliance di sicurezza di rete (ad esempio un firewall), è necessario consentire connessioni non filtrate e non ispezionate a 208.67.220.220, 208.67.222.222, 67.215.92.210 e 146.112.255.152/29 (.152 ~ .159).

Configurazione

Ad alto livello, per abilitare l'integrazione sono necessarie quattro fasi di configurazione:

1. Impostare un nome per il cluster AP

2. Immettere le credenziali dell'account

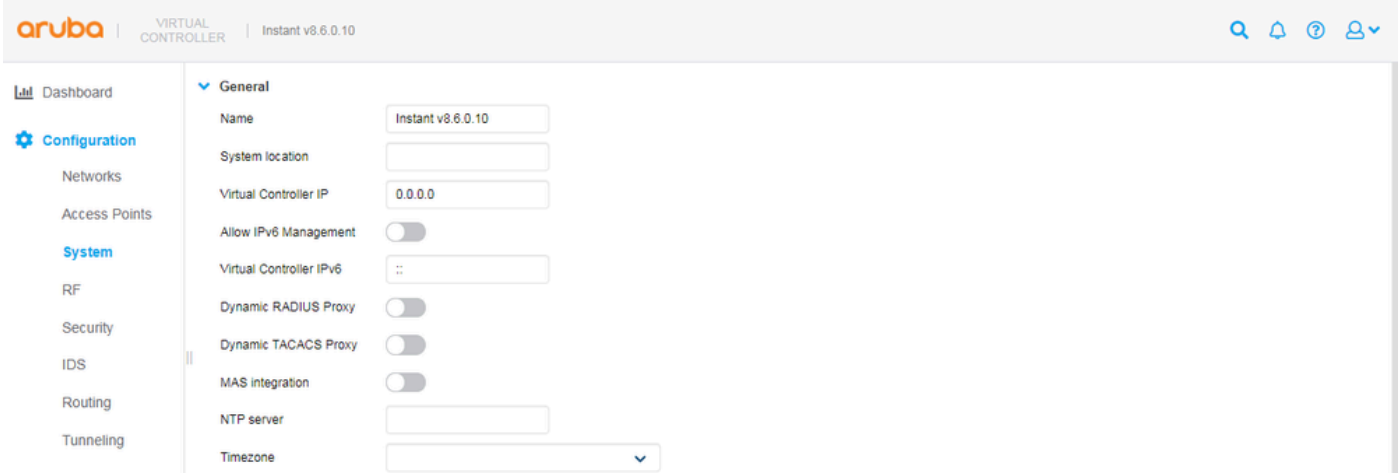
3. Intercetta query DNS

4. Applica criteri DNS

Imposta un nome per il cluster PA

Quando un cluster istantaneo riesce a registrarsi in un dashboard Umbrella per la prima volta, una voce relativa al dispositivo di rete viene aggiunta al dashboard Umbrella in Distribuzioni > Dispositivi di rete. Il nome dispositivo di una nuova voce deriva dal nome di sistema configurato nel controller virtuale di un cluster.

Per impostare il nome del sistema su un controller virtuale immediato, selezionare Configurazione > Sistema.



4404011628308

Il valore del nome viene copiato una sola volta durante la registrazione iniziale. Se il nome di un sistema o di un dispositivo viene modificato successivamente sul lato Instant o Umbrella, è necessario aggiornare manualmente il nome sull'altro lato.

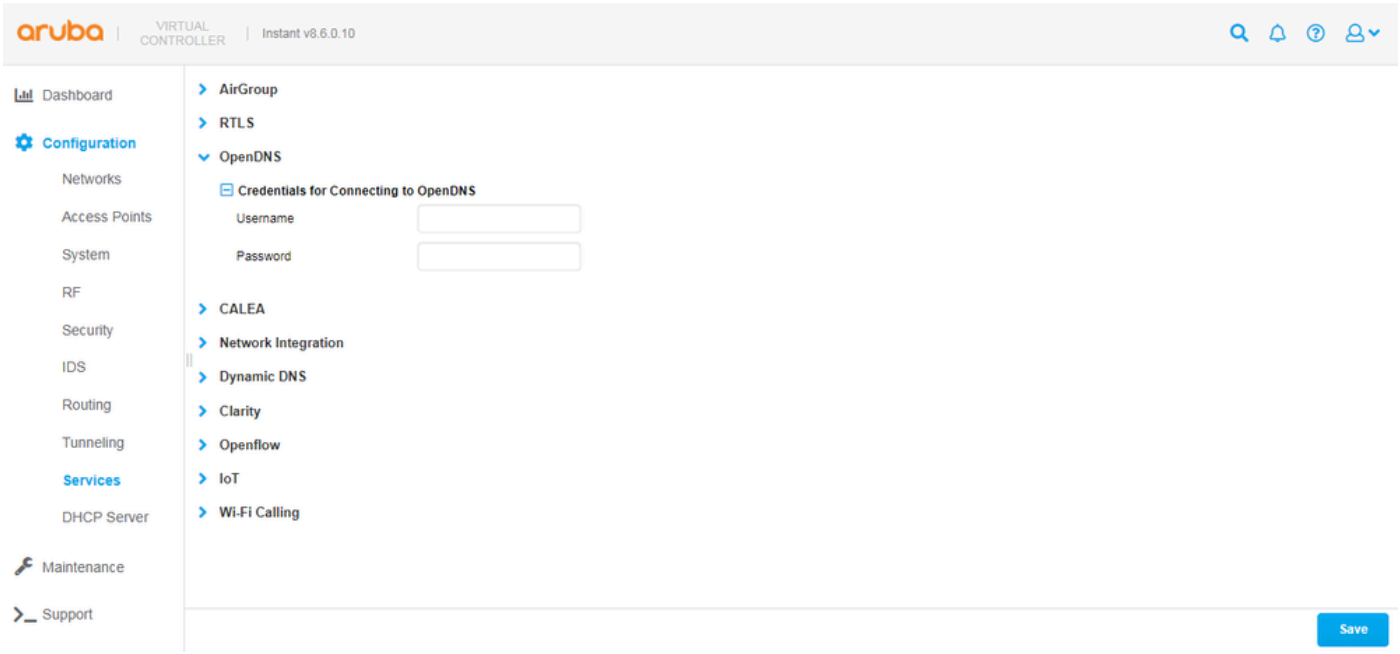
Immettere le credenziali dell'account

Se i requisiti elencati nella sezione Prerequisiti sono soddisfatti, è possibile aggiungere un cluster istantaneo al dashboard Umbrella come dispositivo di rete. Per eseguire questa operazione dal controller virtuale di un cluster:

1. Passare a Configurazione > Servizi > OpenDNS.

2. Inserire le credenziali di login di un account Umbrella.

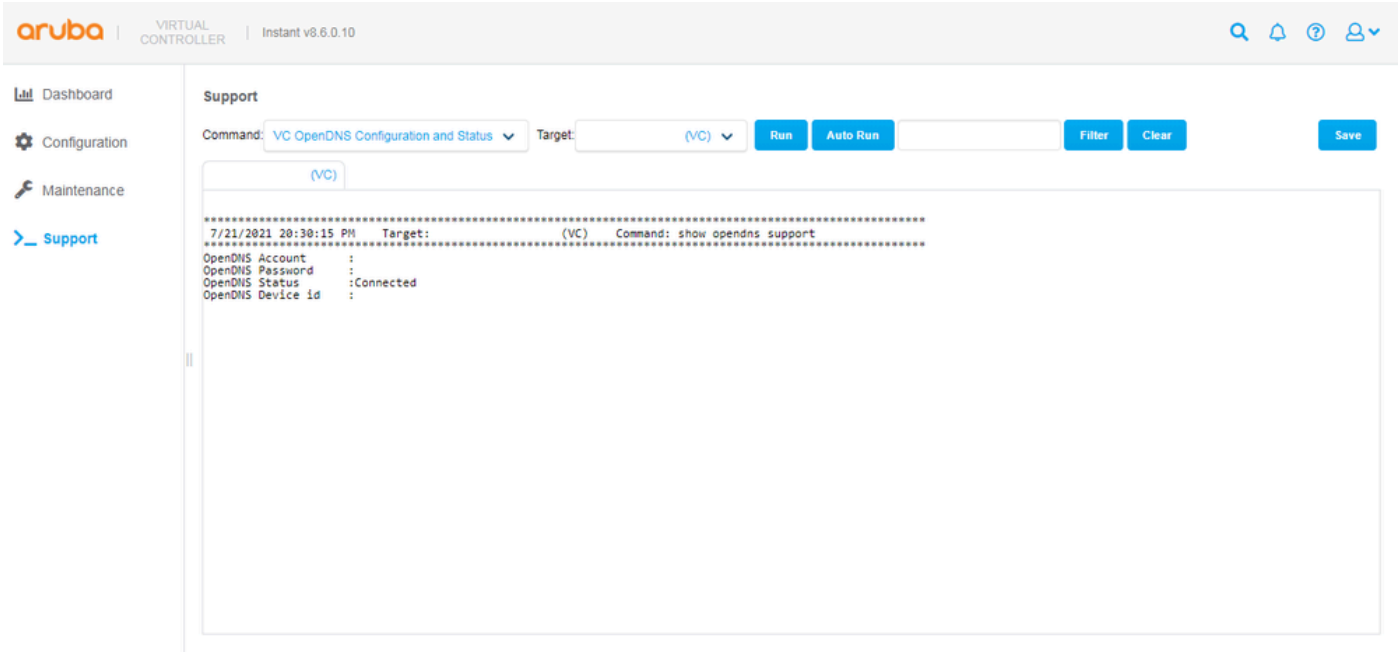
3. Selezionare Salva.



4404019266196

Se il controller virtuale (VC) si connette correttamente a Umbrella, è possibile visualizzare lo stato Connesso quando si passa a Supporto ed esegue il comando "Configurazione e stato VC OpenDNS" (`mostra supporto aperto`).

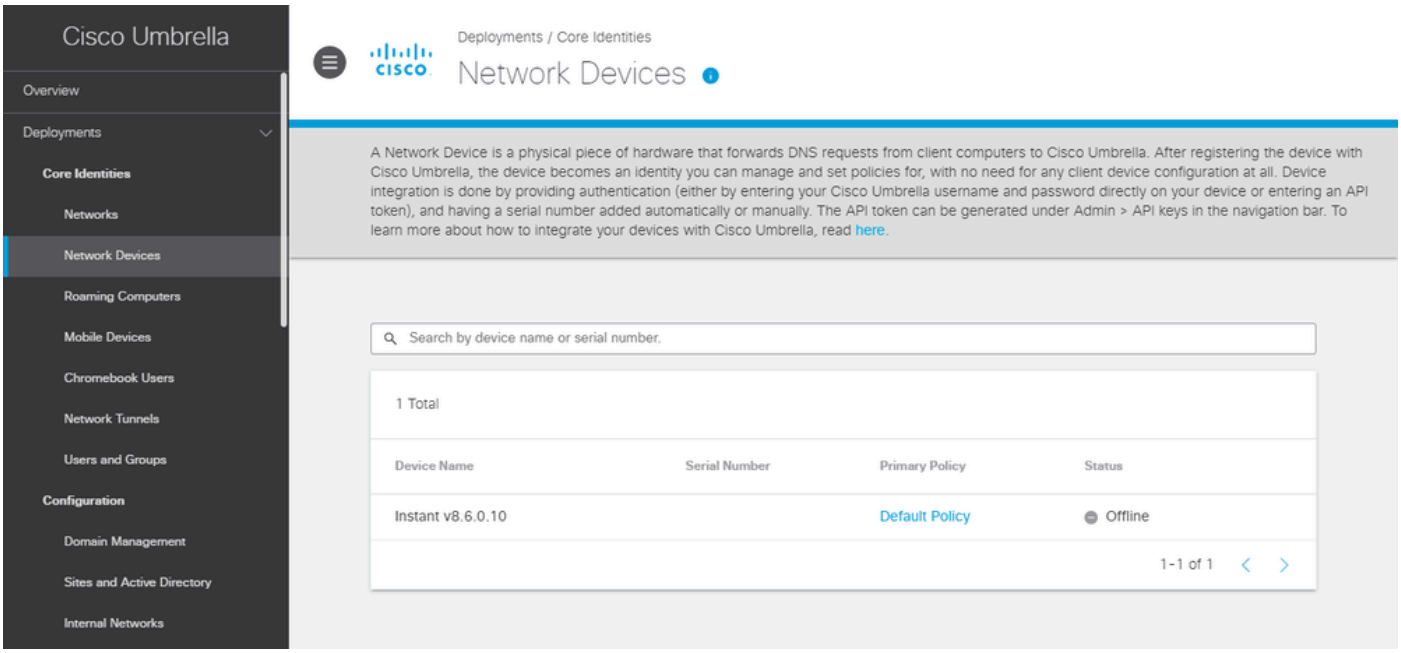
È inoltre possibile visualizzare l'ID di un dispositivo, generato da Umbrella quando viene creato e salvato un nuovo dispositivo di rete nella configurazione di Instant VC. Quest 'ultima parte è importante. Poiché ogni cluster Instant deve avere un ID dispositivo di rete Umbrella univoco, l'ID dispositivo non deve essere copiato dalla configurazione di un cluster a un altro. Un ID di dispositivo valido è in genere composto da 16 cifre.



4404019268116

Se l'output del comando mostra lo stato Non connesso, è possibile provare a scoprirlo eseguendo i comandi "AP Tech Support Dump" (`show tech-support`) e "AP Tech Support Dump Supplemental" (`show tech-support supplementare`) e quindi cercando "open" nei log. Gli output del comando possono essere condivisi con Aruba TAC per la risoluzione dei problemi.

Se tutto funziona correttamente, è possibile visualizzare una nuova voce nel dashboard Umbrella in Distribuzioni > Dispositivi di rete, in cui è possibile cercare un cluster Instant AP in base al nome o eliminare una voce esistente se si desidera generare un nuovo ID dispositivo.



4404011658516

Intercetta query DNS

Dopo aver confermato che un cluster è stato aggiunto correttamente al dashboard Umbrella come dispositivo di rete, è possibile impostare il cluster in modo che inizi a intercettare le query DNS inviate dai client wireless (connessi ai punti di accesso nel cluster). Una volta impostato, indipendentemente dagli indirizzi IP dei server DNS configurati sulle schede NIC dei client wireless, le query DNS dei client possono essere intercettate dal cluster e inoltrate ai resolver anycast di Umbrella agli indirizzi 208.67.220.220 e 208.67.222.222.

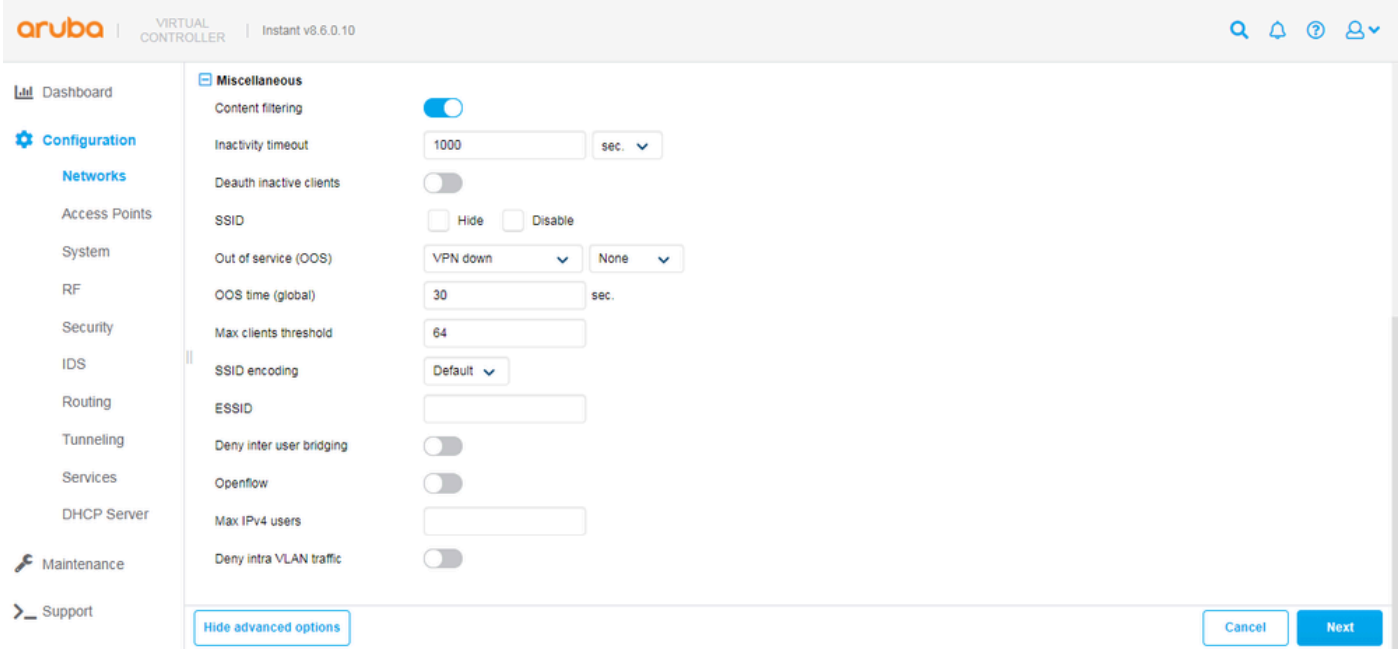
Per intercettare le query DNS:

1. Passare al controller virtuale di un cluster in Configurazione > Reti.

2. Selezionare una rete wireless.

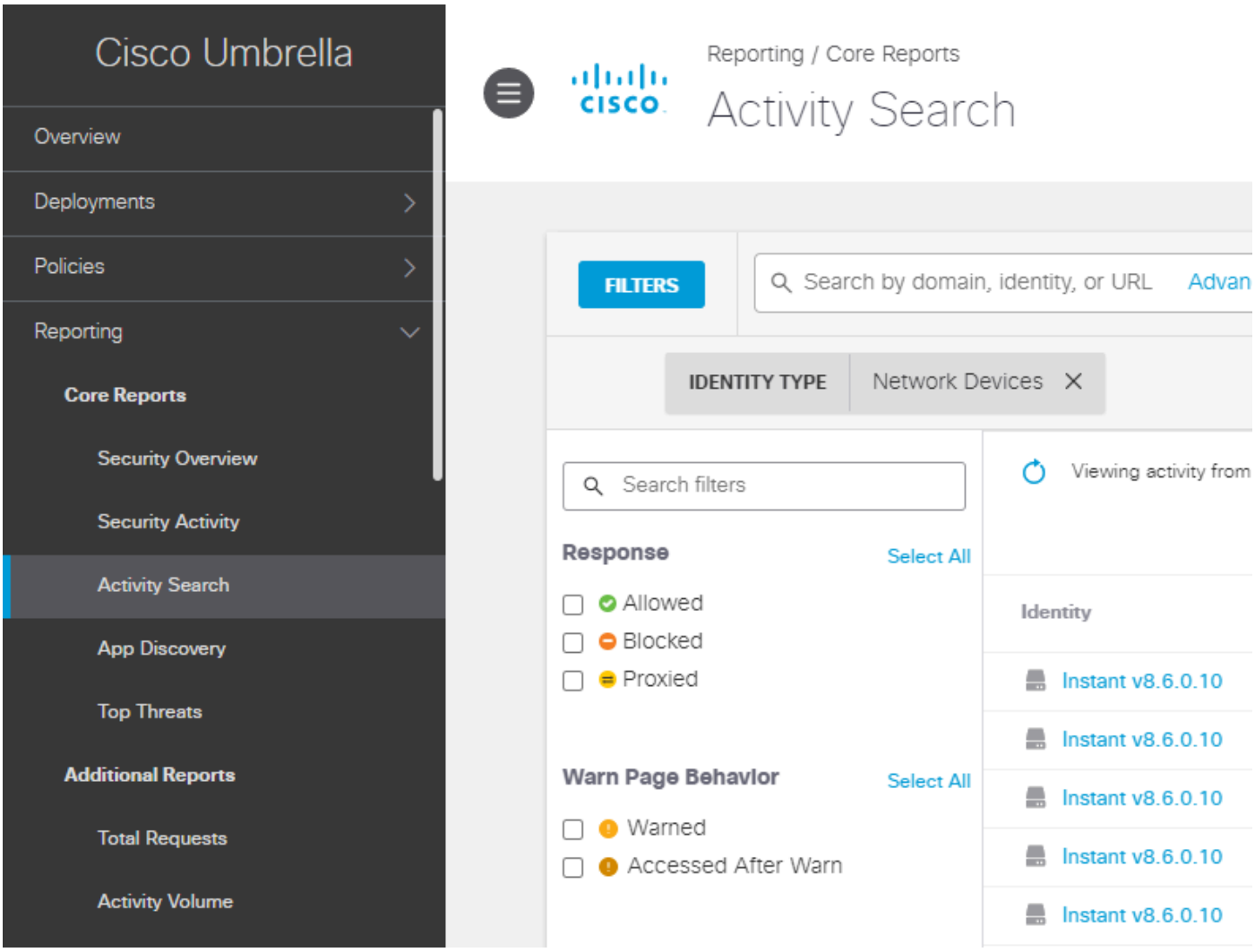
3. Modificare la rete, selezionare Mostra opzioni avanzate e scorrere fino alla sezione Varie.

4. Abilitare l'opzione Filtro contenuto e continuare a selezionare Successivo fino a quando non è possibile selezionare il pulsante Fine per salvare la modifica.



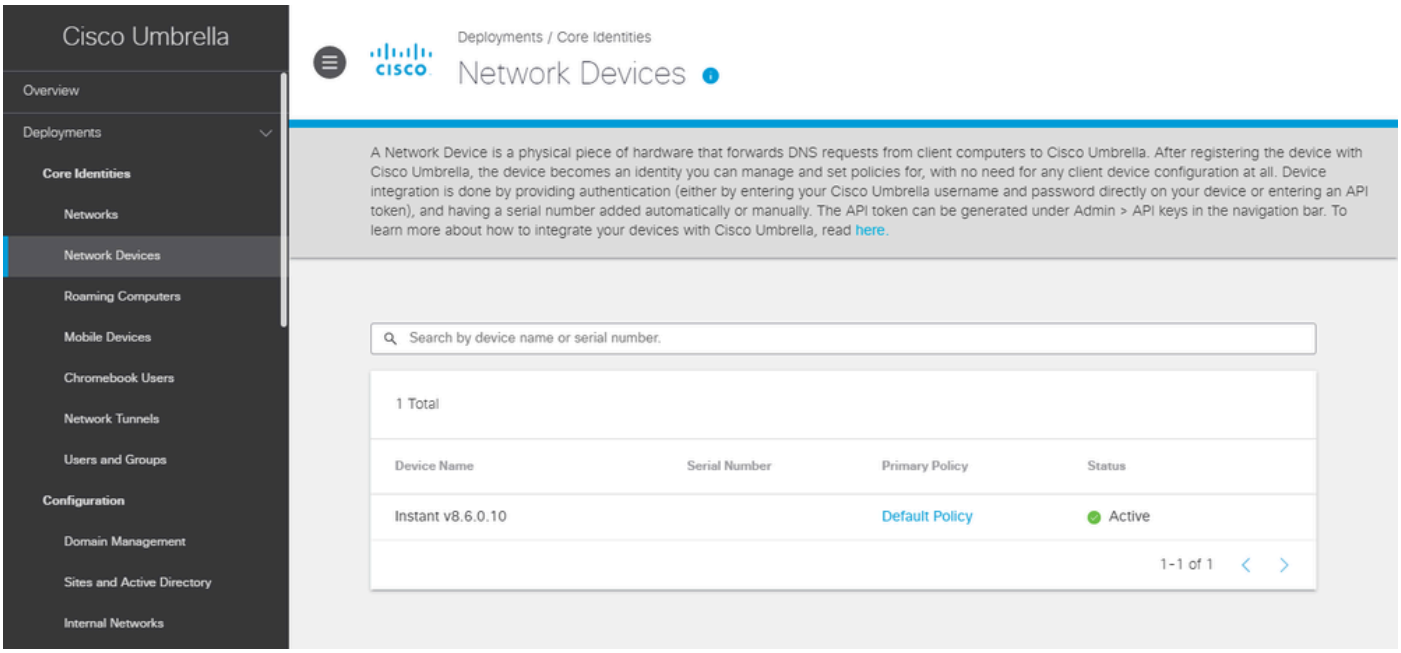
4404011668500

Dopo aver attivato l'opzione, è possibile iniziare a visualizzare le query DNS nel dashboard Umbrella in Report > Ricerca attività.L'identità delle query può essere mappata a un nome di dispositivo di rete, che in genere è il nome di sistema configurato sul controller virtuale di un cluster AP. Notare che l'elaborazione e la visualizzazione delle query nell'interfaccia utente del dashboard può richiedere tempo (circa 15 minuti).



4404011721620

Nel dashboard Umbrella in Distribuzioni > Dispositivi di rete, possono trascorrere fino a 24 ore prima che un dispositivo passi a uno stato attivo/in linea. Lo stato di un dispositivo di rete indica semplicemente se le query DNS sono state intercettate dal dispositivo e inoltrate a Umbrella nelle 24 ore precedenti e non influenza il modo in cui un dispositivo comunica con Umbrella. Lo stato non in linea/inattivo può semplicemente indicare che nessun client wireless è stato connesso a un cluster AP nelle ultime 24 ore e non può impedire al cluster di utilizzare il servizio Umbrella.

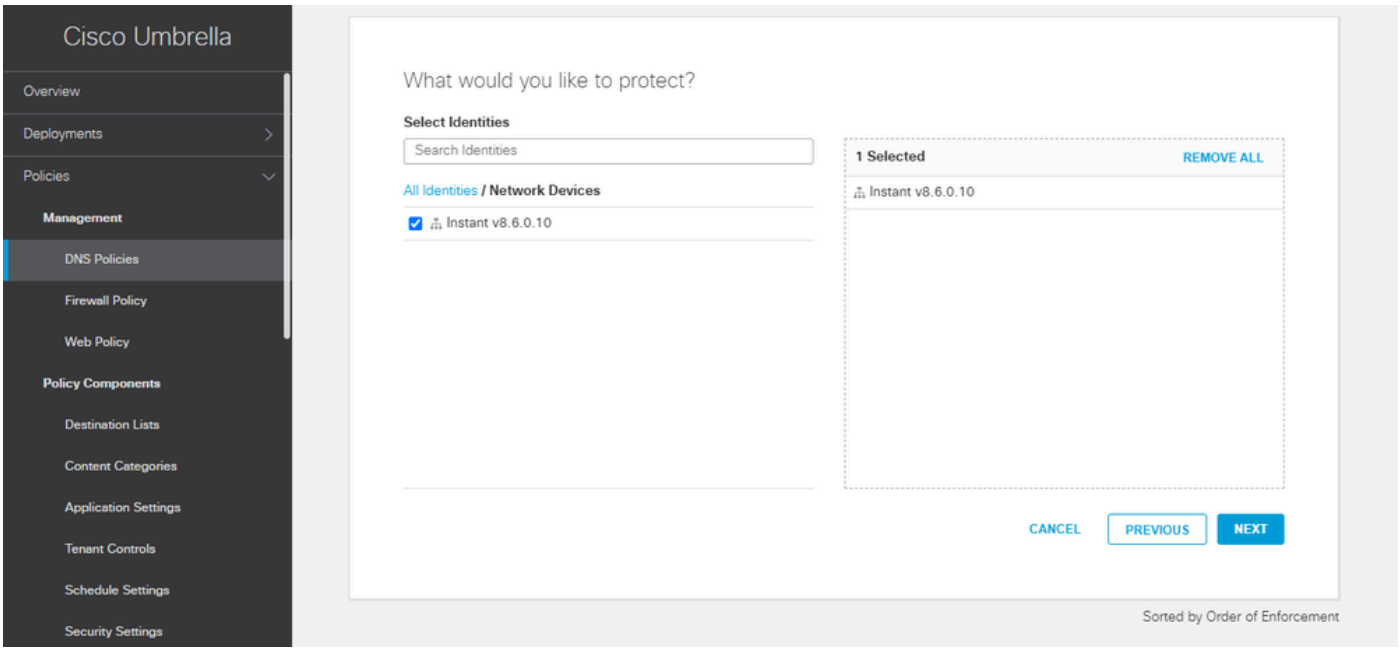


4404011756308

Applica criterio DNS

In Umbrella, il "Criterio predefinito" include automaticamente tutte le identità (come i dispositivi di rete) aggiunte a un dashboard. Non è necessario creare criteri DNS aggiuntivi se tutti i cluster AP nella distribuzione possono essere soggetti allo stesso criterio. In questo caso, passare alla sezione successiva.

In alternativa, se si desidera applicare un criterio personalizzato a un dispositivo di rete specifico, è necessario aggiungere un nuovo criterio nel dashboard Umbrella in Criteri > Tutti i criteri (criteri DNS) e selezionare il dispositivo di rete nel criterio.



4404011773588

Quando nella pagina Criteri DNS (tutti i criteri) sono presenti più criteri, questi vengono valutati

dall'alto in basso in base alla prima corrispondenza. Per ulteriori informazioni, vedere la documentazione sulla precedenza dei criteri e le procedure consigliate per la definizione della documentazione dei criteri.

DNS interno

In un ambiente in cui sono presenti server DNS interni e si desidera inoltrare le query DNS per determinati domini (interni) ai server DNS interni, è possibile utilizzare la funzionalità Domini enterprise in Instant.

Le query DNS possono continuare a essere intercettate dal cluster AP dopo l'abilitazione della funzionalità, ad eccezione del fatto che le query per i domini specificati non possono più essere inoltrate a Umbrella. Possono invece essere inoltrati agli indirizzi IP del server DNS originariamente configurati sulle schede NIC dei client wireless (ad esempio tramite DHCP). Questa funzionalità è simile alla funzionalità Domini interni disponibile nei metodi di implementazione Umbrella standard (con appliance virtuali), in cui non viene utilizzata l'integrazione Aruba Instant.

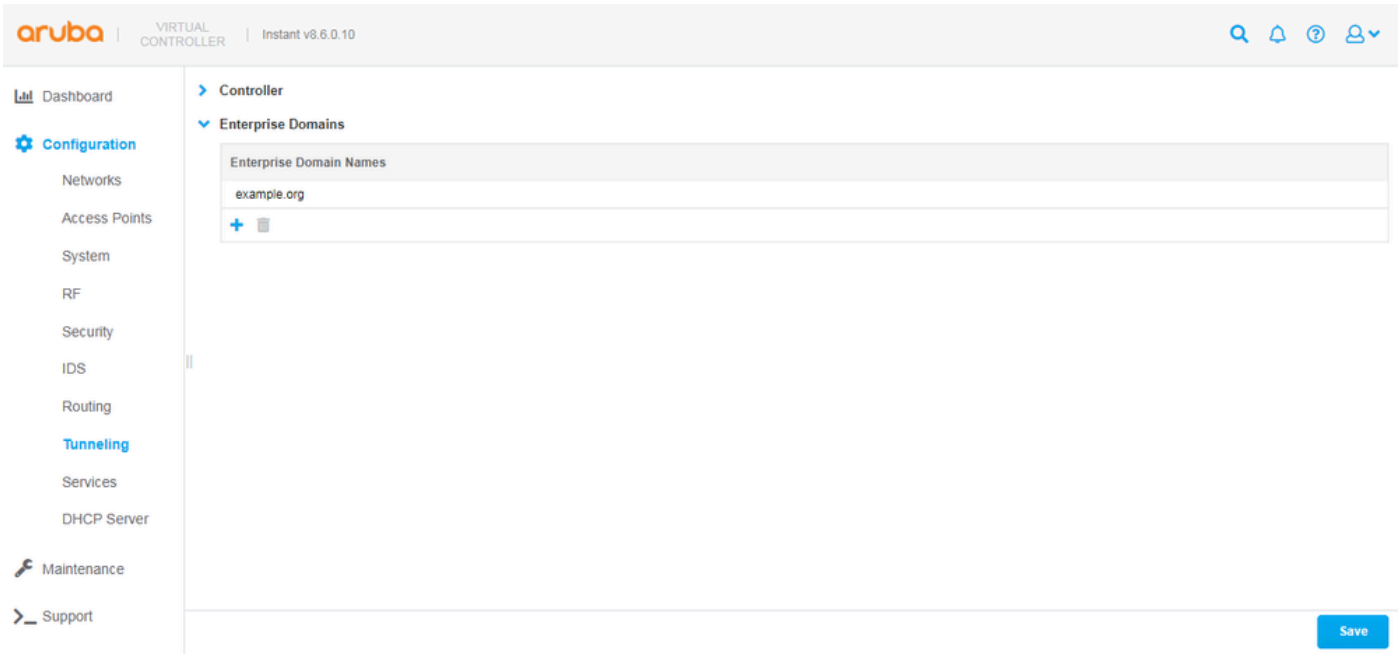
Per configurare la funzionalità su un controller virtuale immediato:

1. Passare a Configurazione > Tunneling > Domini enterprise.

2. Aggiungere o rimuovere domini dalla lista Nomi di dominio enterprise.

3. Selezionare Salva.

Esiste un carattere jolly implicito per ogni dominio aggiunto all'elenco, quindi example.org implica *.example.org.



4404238114452

Verifica

Sia che Umbrella sia stato distribuito sulla WLAN utilizzando i metodi standard a cui si fa riferimento nella sezione "Panoramica della distribuzione" di questa guida, sia che l'integrazione sia descritta nella sezione "Aruba Instant Integration", è possibile verificare che i client wireless stiano utilizzando Umbrella DNS selezionando https://welcome.umbrella.com/ da uno dei client. In seguito viene visualizzato un segno di spunta verde simile allo screenshot mostrato nella documentazione di Umbrella.

4404011960212

In alternativa, è possibile verificare questa condizione eseguendo il comando al prompt dei comandi di un client wireless.

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

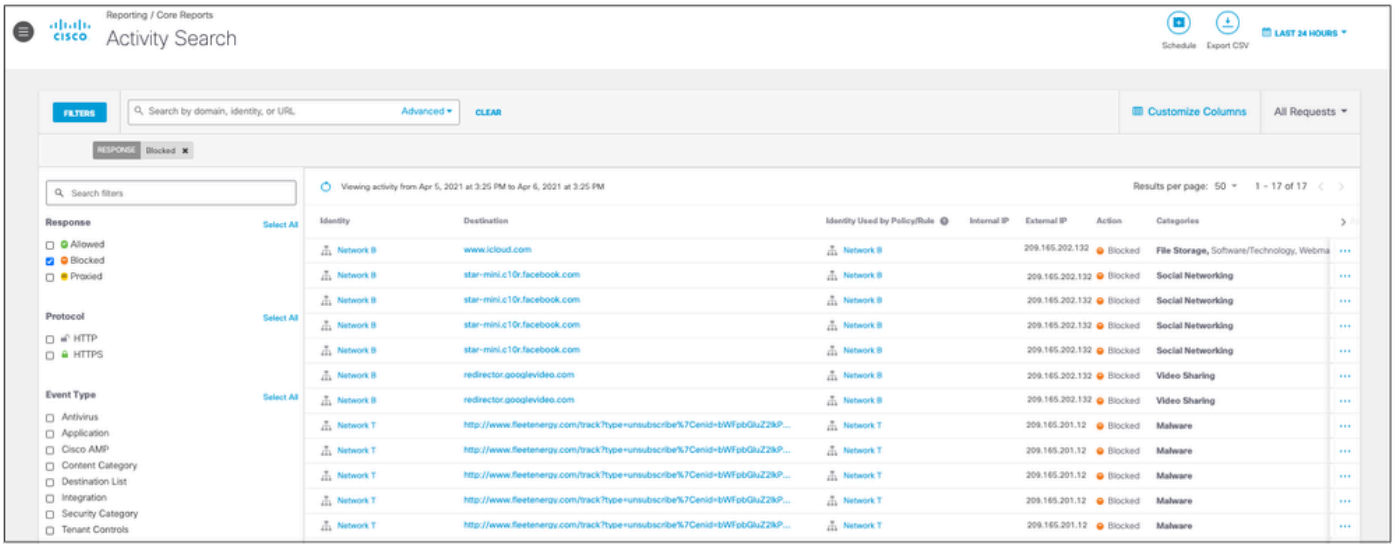
È possibile visualizzare un output con un numero di righe di testo, simile a questo screenshot:

```
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
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

Dall'output del comando, è possibile visualizzare l'ID org del dashboard Umbrella nella riga "orgid" o "id organizzazione" e, se si utilizza l'integrazione istantanea, è possibile visualizzare la riga "device" aggiuntiva che contiene un ID dispositivo.

Per esaminare le query DNS nel dashboard Umbrella, passare a Report > Ricerca attività. Notare che la visualizzazione delle query nell'interfaccia utente del dashboard può richiedere del tempo (circa 15 minuti). Le istruzioni su come utilizzare Ricerca attività sono disponibili all'indirizzo nella documentazione di Umbrella.



4404019393044

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).