Implementazioni sicure di Cisco Umbrella per appliance virtuali e connettori AD

Sommario

Introduzione

In questo documento vengono descritte le best practice e vengono forniti consigli relativi alle installazioni di Cisco Umbrella Virtual Appliance (VA) e Active Directory Connector per ridurre il rischio di attacchi interni derivanti dall'utilizzo di questi componenti.

Il VA esegue una versione avanzata di Ubuntu Linux 20.04. I clienti dispongono di accesso limitato solo per scopi di configurazione e risoluzione dei problemi. I clienti non possono distribuire software o script aggiuntivi sull'appliance VA.

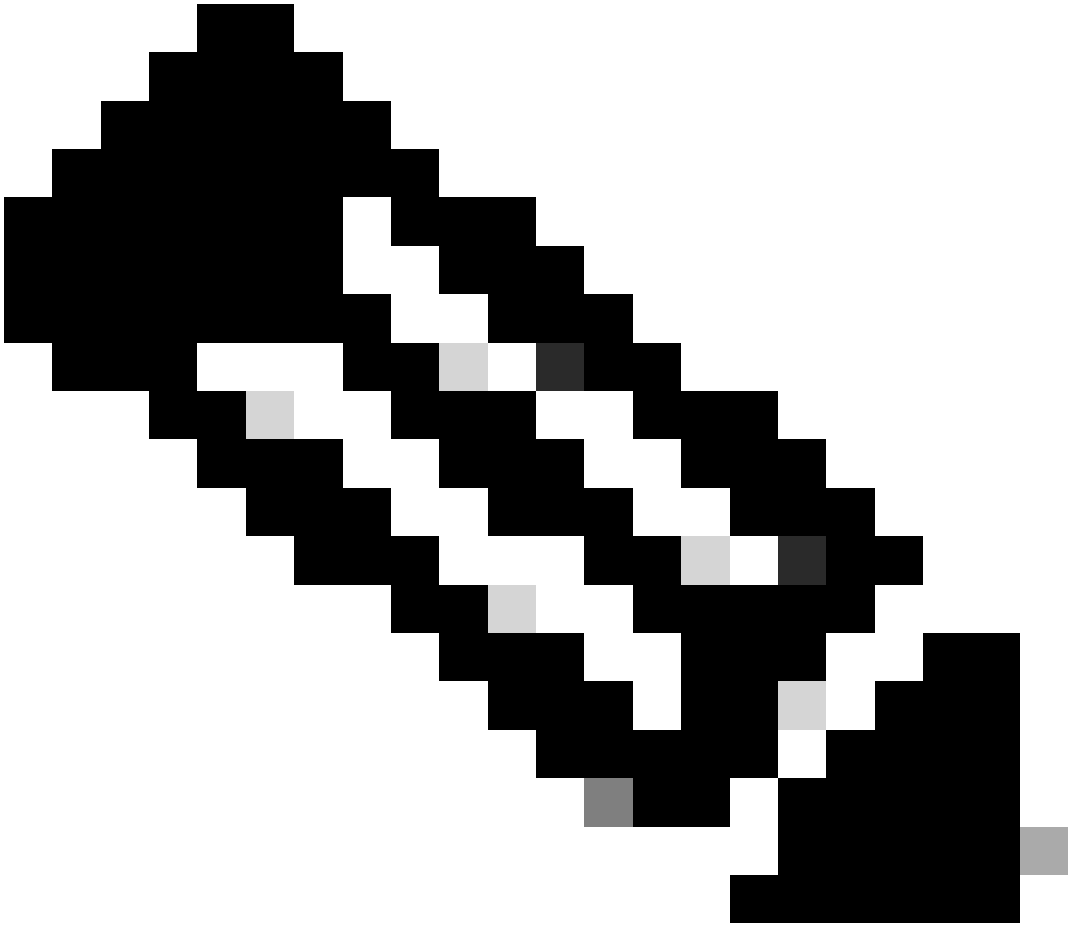
Cisco Umbrella Virtual Appliance

Gestione del file .tar:

- Il software Cisco Umbrella Virtual Appliance (VA) viene scaricato da Umbrella Dashboard come file .tar contenente l'immagine VA effettiva e una firma per tale immagine.
- Cisco consiglia di convalidare la firma per verificare l'integrità dell'immagine VA.

Configurazione delle porte:

- per impostazione predefinita, in fase di distribuzione solo le porte 53 e 443 sono aperte per il traffico in entrata.
- Se si esegue VA in Azure, KVM, Nutanix, AWS o GCP, per impostazione predefinita viene abilitata anche la porta 22 per consentire le connessioni SSH per la configurazione di VA.
- Per i VA in esecuzione su VMware e Hyper-V, la porta 22 viene aperta solo se il comando per abilitare SSH è in esecuzione sul VA.
- Il VA esegue query in uscita su porte/protocolli specifici verso le destinazioni indicate nella documentazione di Umbrella.
- Cisco Umbrella consiglia di impostare delle regole sul firewall per bloccare qualsiasi traffico dai VA verso tutte le altre destinazioni.



Nota: Tutte le comunicazioni HTTPS da/per VA avvengono solo su TLS 1.2. Non vengono utilizzati protocolli meno recenti.

Gestione delle password:

- L'accesso iniziale alla VA richiede una modifica della password.
- Cisco consiglia di ruotare periodicamente la password sulla VA dopo la modifica iniziale della password.

Attenuazione degli attacchi DNS:

- Per ridurre il rischio di un attacco Denial of Service interno al servizio DNS in esecuzione sulla VA, è possibile configurare i limiti di velocità per IP per il DNS sulla VA.
- Questa opzione non è attivata per impostazione predefinita e deve essere configurata in modo esplicito utilizzando le istruzioni documentate nella documentazione di Umbrella.

Monitoraggio dei VLAN su SNMP:

- Se si stanno monitorando i VLAN su SNMP, Cisco Umbrella consiglia di utilizzare SNMPv3 con l'autenticazione e la crittografia.
- Istruzioni per la stessa operazione sono riportate nella documentazione di Umbrella.
- Dopo aver abilitato il monitoraggio SNMP, la porta 161 sul VLAN viene aperta per il traffico in entrata.
- È possibile monitorare vari attributi come la CPU, il carico e la memoria su VA su SNMP.

Utilizzo dell'integrazione AD Cisco con i VA:

- Se si utilizzano i VA con l'integrazione Cisco Umbrella Active Directory, è consigliabile regolare (o regolare) la durata della cache utente sui VA in base al tempo di lease DHCP.
- Per ulteriori informazioni, fare riferimento alle istruzioni contenute nell'accessorio virtuale: Sintonizzazione della documentazione relativa alle impostazioni del case utente. In questo modo si riduce il rischio di attribuzioni errate degli utenti.

Configurazione della registrazione di controllo:

- VA gestisce un registro di controllo di tutte le modifiche di configurazione eseguite su VA.
- È possibile configurare la registrazione remota di questo registro di controllo su un server syslog seguendo le istruzioni riportate nella documentazione di Umbrella.

Configurazione dei VA:

- È necessario configurare almeno due VA per ogni sito Umbrella e l'indirizzo IP di questi due VA può essere distribuito come server DNS agli endpoint.
- Per una maggiore ridondanza, è possibile configurare l'indirizzamento Anycast sulla VA. Ciò consente a più VA di condividere un singolo indirizzo Anycast.
- In questo modo è possibile distribuire più VA e contemporaneamente distribuire solo due IP di server DNS a ciascun endpoint. In caso di guasto a uno dei VA, Anycast assicura che le query DNS vengano instradate all'altro VA che condivide lo stesso IP Anycast.
- Ulteriori informazioni sulla configurazione di Anycast sulla VA.

Configurazione di Cisco Umbrella Active Directory Connector

Creazione di un nome account personalizzato:

- Una delle procedure consigliate per Cisco Umbrella AD Connector è utilizzare un nome account personalizzato anziché il valore predefinito OpenDNS_Connector.
- È possibile creare questo account prima della distribuzione del connettore e concedere le autorizzazioni necessarie.
- È necessario specificare il nome dell'account come parte dell'installazione del connettore.

Configurazione di LDAPS con il connettore AD:

- Umbrella AD Connector tenta di recuperare le informazioni sui gruppi di utenti su LDAPS (dati trasmessi su un canale protetto), altrimenti passa a LDAP su Kerberos (crittografia a livello di pacchetto) o a LDAP su NTLM (solo autenticazione, nessuna crittografia) in questo ordine.

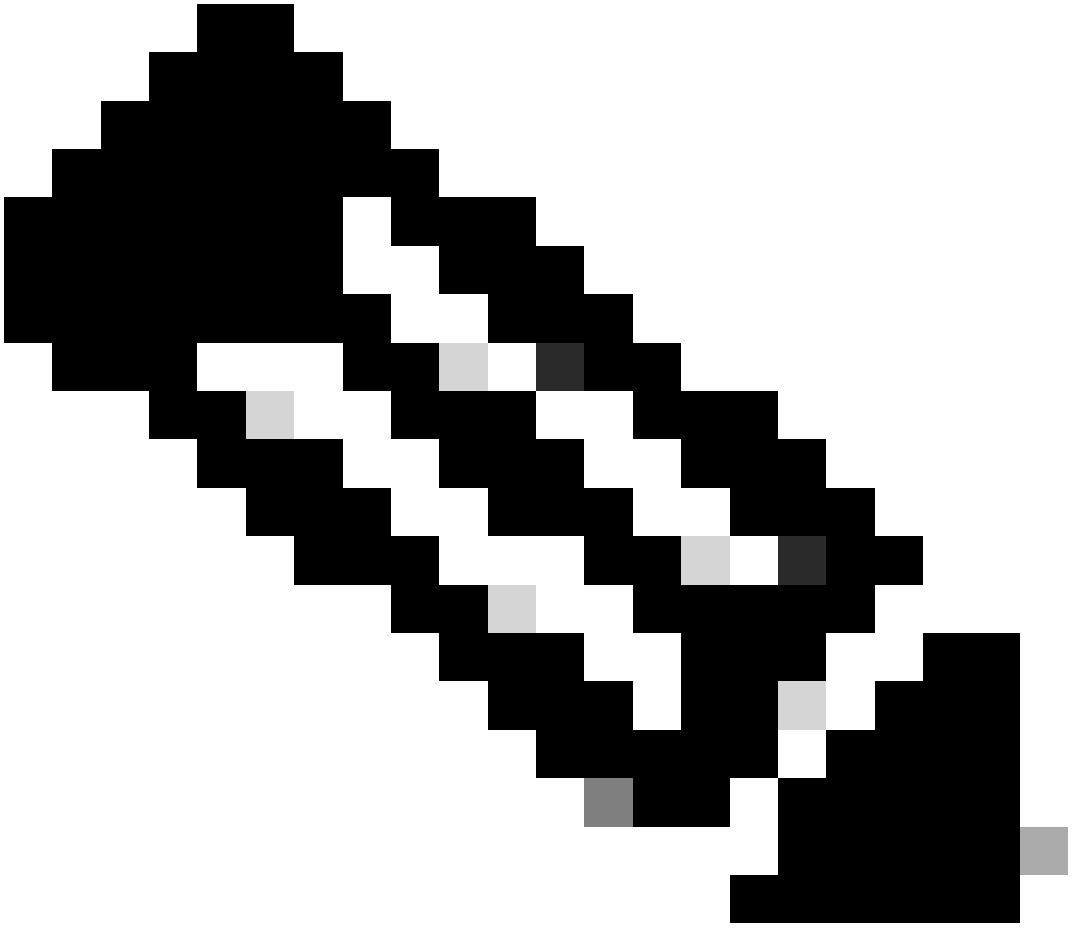
- Cisco Umbrella consiglia di configurare LDAPS sui controller di dominio in modo che il connettore possa recuperare queste informazioni su un canale crittografato.

Gestione del file con estensione ldif:

- Per impostazione predefinita, il connettore memorizza i dettagli degli utenti e dei gruppi recuperati dai controller di dominio in un file .ldif localmente.
- Poiché possono trattarsi di informazioni riservate memorizzate in testo normale, è possibile limitare l'accesso al server che esegue il connettore.
- In alternativa, al momento dell'installazione è possibile scegliere di non memorizzare i file .ldif localmente.

Configurazione delle porte:

- Poiché il connettore è un servizio Windows, non attiva/disattiva alcuna porta sul computer host. Cisco Umbrella consiglia di eseguire il servizio Cisco Umbrella AD Connector su un server Windows dedicato.
- Analogamente al VA, il connettore esegue query in uscita su porte/protocolli specifici verso le destinazioni menzionate nella documentazione di Umbrella. Cisco Umbrella consiglia di impostare regole sul firewall per bloccare qualsiasi traffico dai connettori verso tutte le altre destinazioni.



Nota: Tutte le comunicazioni HTTPS da/verso il connettore avvengono solo su TLS 1.2. Non vengono utilizzati protocolli meno recenti.

Gestione password connettore:

- Cisco consiglia di ruotare periodicamente la password del connettore.
- A tale scopo, è possibile modificare la password dell'account del connettore in Active Directory e quindi aggiornare la password utilizzando lo strumento "PasswordManager" nella cartella del connettore.

Ricezione dei mapping utente-IP:

- Per impostazione predefinita, il connettore comunica l'IP privato.
- AD invia i mapping degli utenti a VA su testo normale.
- È possibile scegliere di configurare VA e il connettore per la comunicazione su un canale crittografato in base alle istruzioni documentate in questo articolo della Knowledge Base.

Gestione certificati:

- La gestione e la revoca dei certificati non rientrano nell'ambito del VA e l'utente è responsabile della presenza della catena di certificati/certificati più recente sul VA e sul connettore, a seconda dei casi.
- L'impostazione di un canale crittografato per questa comunicazione influisce sulle prestazioni del VA e del connettore.

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).