Active Directory Integration



Contents

Active Directory Integration	1
About Active Directory	1
Requirements	. 2
Configure the Domain Controller	. 3
Configure the Sensor	10

Active Directory Integration

The integration of Active Directory technology, developed by Microsoft for Windows operating systems, enhances VMware NSX Network Detection and Response by providing additional information extracted from the Domain Controllers. This information details the Windows users that are logged in on hosts in the network. The system is thus able to associate events that occur in the monitored network with the Windows users logged in on the host. You can then immediately identify the users that have been exposed to a detected threat and take appropriate measures.

About Active Directory

Active Directory (AD) is a directory service developed by Microsoft. It uses their Distributed Component Object Model (DCOM) technology to allow communication between software components distributed across networked computers. An Active Directory environment contains one or more Domain Controller (DC) servers that implement the authentication controls. Security Event logs are some of the event logs on a Windows system. These logs are related to security events, for example, a login attempt or a request for a privileged operation. Windows Management Instrumentation (WMI) is an interface implemented in Windows operating systems through which instrumented components provide information and notifications about the system and its hardware.

Architecture

When using the Active Directory integration, the Sensor connects to one or more Domain Controller (DC) servers, extracts the log information from the Security Event logs and uses these data to correlate IP addresses and timestamps to the Active Directory users who were active on those hosts at the given time. The Sensor will then periodically upload this mapping to its Manager (for On-Premises installations) or to the VMware backend (for hosted installations).

The communication between the Sensor and a Domain Controller relies on the Distributed Component Object Model (DCOM) and Windows Management Instrumentation (WMI) technologies integrated into the operating system.

The following figure summarizes this infrastructure:



In this figure, the network of the company is represented by two Domain Controller servers (DC 1 and DC 2) and three workstations (IP1, IP2, and IP3). Some users are logged in on these workstations:

• User A is on workstation IP1, which used the Domain Controller DC 1 to validate the authentication.

- User B is on workstation IP2, which used the Domain Controller DC1 to validate the authentication.
- User C and User D are on workstation IP3, which used the Domain Controller DC 2 to validate the authentication.

The Sensor has been configured to query both DC1 and DC2. It is therefore aware of the users logged in on any of the three workstations.

Note: You can configure the request polling interval used by the Sensor.

On the right of the Manager, two events are represented. Each event contains a timestamp (TS) and the IP address of the host that generated the event. With the Active Directory integration, the events will also include the list of users that were logged in on the system at this time.

Requirements

The following are required for integration:

- At least one Sensor deployed in either a Hosted or On-Premises environment.
- An infrastructure built on Domain Controllers running Windows Server 2016, 2012, or 2008.

A Domain Controller running Windows Server 2000 or 2003 is not compatible with the Active Directory integration. Contact *VMware Support* (https://my.vmware.com/group/vmware/get-help) if your network contains Domain Controllers with these versions.

The configuration of a Domain Controller requires an account with the administrator privileges.

- The Sensor and the Domain Controller can be in two different networks, however if any equipment is filtering the network streams between the two networks, the underlying protocols Windows uses to execute remote WMI queries require the following communications to be enabled:
 - # TCP Sensor:* to Domain Controller:135

TCP Sensor: [>=1024] to Domain Controller: [>=1024]

These port ranges come from the internal port mapping mechanism Windows uses to execute the RPC calls that support the WMI queries. The client (the Sensor) first connects to the Port Mapper service (port 135) on the server (the Domain Controller) and then requests the port number of the specific service it wants to query. The server replies with the port number (a port greater or equal to 1024) and the client opens a new connection to this port. Because this port number can vary, communication to any port greater or equal to 1024 must be allowed.

Note: The range of dynamic ports for RPC services can be configured and restricted in Windows.

Configure the Domain Controller

Configuration Steps

The Sensor needs to have access to an account with the appropriate rights on the Domain Controller to be able to retrieve the security event log. While an account with full administrator rights could technically be used, it is strongly recommended that you instead create a dedicated account with the least required privileges.

The following steps show the procedure to create such account. The screenshots were taken on a Windows Server 2008 installation. The process is very similar on Windows Server 2012 and 2016.

Procedure

Step 1: Create a new account

Create a new Domain Controller user account using the Active Directory Users and Computers component. In the following example, add a new user logaccess to the domain LASTLINE2008:

Active Directory Users and Computers						
File Action View Help	File Action View Help					
🗢 🔿 🙍 🖬 📋 📓 🙆 🗟	- 🚺 🖬 🚷	💐 🛅 🍸 🗾	έβ.			
Active Directory Users and Comput Saved Queries Saved Queries Bullan Dullan Computers Computers ForeignSecurityPrincipals Managed Service Accounts Users	Name Administrator Administrator Cert Publishers Densel ROD Drs.UpdatePr Donal QudatePr Donal Qudate Donal Com Donan Guests Donan Guests Enterprise R Group Policy Suest Lastinewmi RAS and IAS Read-only D Schema Admins	Type User Security Group Security Group	Description Built-in account for a few Object - User Create in: First name: Last name: Full name: User logon name: [logaccess User logon name (pre [LASTLINE 2008\	admini lastline2008.com/Users logAccess logAccess Qlastline2008.com Windows 2000): logaccess <	×	

Step 2: Add the user account to the Event Log Readers group

- Open Active Directory Users and Computers and then select Users from the left sidebar.
- Right-click the user account from the list and open the Properties.

- From the Member Of tab, click the Add button.
- Select the Event Log Readers group.

Active Directory Users and Comp	outers					- 🗆 X
	LLAD Integration Prop	erties		? ×		
Active Directory Users and Com Saved Queries Playground.tse Builtin Computers Similar Computers Managed Service Accour Users	Remote control General Address Member Of Name Domain Users Event Log Readers Event Log Readers Add F Primary group: Do Set Primary Group	Remote Desktop Si Account Profile Dial-in Env Active Directory Domain Playground tse/Users Playground tse/Users Playground tse/Builtin Remove amain Users There is no need to you have Macintosh applications.	change Primary clients or POSID	COM+ Organization Sessions	1 р с р т р т р т р т ет ет ет ет ет ет р р р р р р р	

Step 3: Grant read access on Security Event logs

The new user, logaccess, must be granted with permission to read the Security Event logs:

- Start the Group Policy Management console by running gpmc.msc.
- Expand the tree, then right-click on Default Domain Controllers Policy (you can select another group policy, depending on the structure of your domain) and select Edit, as in the following example:

		🧮 Group Policy Management	
		Kile Action View Window Help	_ B ×
		V V 2 10 12 1 🗛 🖸 11 🖬	
		Group Policy Management	Default Domain Controllers Policy
		A Forest: lastline2008.com Demains	Scope Details Settings Delegation
		Imains In the string 2008 com	Links
		Default Domain Policy	Dienlau linke in this location:
		🗉 🧾 Domain Controllers	Jastine2008.com
		🖃 📑 Group Policy Objects	The following sites, domains, and OUs are linked to this GPO:
		📕 Default Domain Controllers Po	liev Enforced Link Enabled Pat
		Default Domain Policy WMI Eilbers	GPO Status Introllers No Yes last
		E Starter GPOs	
		Image: A second	Back Up
		👸 Group Policy Modeling	Restore from Backup
		🔀 Group Policy Results	Import Settings Ing
			bave Report his GPO can only apply to the following groups, users, and computers:
			View
			New Window from Here ted Users
			Сору
			Delete
			Rename Remove Properties
D			Refresh
7 RUN			Help
	T		miscronsmiked to the following WMI filter:
	resource and \		<none></none>
	resource, una i		
Open:	gpmc.msc	Open the GPO editor	
	This task is	ill be created with administrative privilence	
	🐨 THIS CASK VU	in be created with aurninistrative privileges.	
		UK Lancel <u>B</u> rowse	

The Group Policy Management Editor starts. Configure the permissions in this window:

- Expand the tree, then select User Rights Assignment in the left panel.
- Select Manage audit and security log in the right panel. This opens the Manage audit and security log properties pop-up.
- Click the Add Users button. The Add User or Group pop-up appears.
- Enter the name of the user (as in this example, LASTLINE2008\logaccess) or click the Browse button to search for it.



• Click the OK button to dismiss the pop-up. Close all the other windows by applying changes if prompted.

Step 4: Provide DCOM permissions

The new user, logaccess, must be granted permission to access DCOM objects:

- Start the Component service program by running dcomcnfg.
- Expand the tree, then right click on My Computer and select Properties, as in the following example:

	Component Services	Hele		
			Antine	
	Console Root Services	COM+ Applications	Actions My Computer	
	Computers	DCOM Config	My computer	
	Invictorigues Invict	b all components best vacation Coordinator	Hore Acudis	
		1		
Run				
Type t resour	the name (rce, and W			
pen: dcom	Opens the properties dialog box for th	e current selection.		
😌 TI	his task will be created with administrative priv	vse		

The My Computer Properties editor starts. Configure the permissions in this window:

- Select the COM Security tab.
- In the Launch and Activation Permissions section, click Edit Limits.
- In the Security Limits section of the pop-up, click Add... to add the new user.
- In the Permissions for Log Access section of the pop-up, select the Allow toggle for Local Launch, Remote Launch, Local Activation, and Remote Activation, as in the following example:

		🛞 Component Services					_ 🗆 🗙	
		💁 File Action View Window H	Help				_ - - - ×	
		🗢 🔿 🙎 📆 🔜 🙆	12 🖬 🗅 🔤 🗃 🏛	<u> </u>				
		Console Root	Name		Actions			
		Component Services	COM+ Applications	1y Computer Properties		? ×	-	
		🖃 🌉 My Computer	Running Processes	General	Options	Default Properties	• •	
		🗄 🧾 COM+ Applications 🗐 🧖 DCOM Config	Distributed Transaction Coordin-	Default Protocols	COM Security	MSDTC		
		🗉 🧮 Running Processes		Access Permissions		aunch and Activation Perr	nission	2 ×
		Distributed Transac Event Viewer (Local)		You may edit who is allow also set limits on applicat	wed default access L tions that determine	Security Limits	Inston	
		🖭 👾 Services (Local)		Caution: Modify	ing access permissi	Group or user names:		
				securely.	to start, connect, ru	& Administrators (LASTLI	NE2008\Administr	▲ (stote
					Edit Limite	Performance Log User & Distributed COM Users	(LASTLINE2008)	Performance Log Distributed COM L
					E dir Ellino	Log Access (logacces	s@lastline2008.co	ป
				Launch and Activation Per	missions	•		
				You may edit who is allow activate objects. You ma determine their own perm	wed by default to la ay also set limits on - nissions.	<u>,</u>	Add	Remove
				Caution: Maditu	ing launch and acti	Permissions for Log Access	Allo	w Deny
				affect the ability	of applications to s	Local Launch		<u>i</u> 🗆 🗌
				and/or fun seco	areiy.	Remote Launch	2	
					Edit Limits	Remote Activation	2	i 🗄 📙
🗁 Run								
	Type the name (resource, and W							
				Learn more about setting the	se properties.	Learn about access control	and permissions	
<u>O</u> pen:	dcomcnfg _						01	Cancel
	😚 🛛 This task wil	I be created with administrative privile	ges.			Cancel Apply		
	C	K Cancel <u>B</u> rows	e					

• Click the OK button to dismiss the pop-up. Close all the other windows by applying changes if prompted.

Step 5: Provide WMI permissions

The new user, logaccess, must be granted permission to access some of the objects available through the WMI interface:

- Start the WMI Management console by running wmimgmt.msc.
- Right click on WMI Control (Local) and select Properties from the menu, as in the following example:

		🚟 wmimgmt <u>- [</u> Co	onsole Root\WMI Control <u>(Local)</u>			
		🚡 File Action '	View Favorites Window Help			_8×
		🔄 🔿 🚺 📅				
		Console Root			Actions	
		WMI Control	Connect to another computer	Management Instrumentation (WMI)	WMI Control (Local)	-
			View New Window from Here	trols the Windows Management Instrumentation (WMI)	More Actions	•
			New Taskpad View			
			Properties			
			Help			
Pup.						
	Type the name of a resource, and Wind					
<u>O</u> pen:	wmimgmt.msc	Opens the properties	dialog box for the current selection.			
	😚 This task will be	e created with admin	istrative privileges.			
	OK	Correct	- Prouro			
	OK					

The Local WMI Control Properties editor starts. Configure the permissions in this window:

- Select the Security tab.
- Expand the tree and Select CIMV2. Click the Security button.
- In the Security for ROOT\CIMV2 pop-up, select the user in the Group or user name section then click Add... to add the new user. Then in the Permissions for Log Access section, select the Allow toggle for Enable Account and Remote Enable, as in the following example:

😽 wmimgmt - [0	onsole Root\WMI Control (Local)] View Favorites Window Help			_ 🗆 ×
Conset Foot ∰ WMI Control # WMI Control	X(Loca) X(Loca	ment Instrumentation (WMI) Local) Properties kup/Restore Security Advanced navigation allows you to set namespace specific se aspet CIMV2 may adopt power Security TerminaServices Ci DEFAULT directop Microsoft Microso	Actions Will Control (Local) More Actions 2 3 3 Security for ROD curly. Group or usen	TVCIMV2 X ames: FVCE FVCE Image: Control (Control (Contro) (Control (Control (Control (Contro) (Contro) (Contro) (Co
Type the name of a resource, and Wind				
Open: wmimgmt.msc	nistrative privileges.			

• Click the OK button to dismiss the pop-up. Close all the other windows by applying changes if prompted.

Configure the Sensor

Configuration Steps

Once your Windows network has been set up properly, the Sensor can be configured to pull information from Active Directory.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the Manager Web UI.

Step 2: Navigate to the Active directory tab

From the Main navigation menu, click [Admin]. On the Admin page, select [Data sources] from left sidebar menu. The Active directory tab is the default view on the Data sources page.

Step 3: Select an appliance

Enter a valid Sensor UUID in the Appliance UUID textbox or click [≡] and select a compatible appliance from the pop-up.

Step 4: Add a Domain Controller

Click the **[ADD DOMAIN CONTROLLER]** button to configure a Domain Controller. If you want to add another Domain Controller to an already existing configuration, click the **[+]** icon.

On the ADD DOMAIN CONTROLLER page, fill in the following:

- Enter a Source Name. This is the name of the domain controller, another way of manually identifying a configured Domain Controller. It can be useful in the event of configuring multiple Domain Controller servers.
- In the Hostname field, enter the hostname or IP address of the domain controller.
- Set a Polling interval. The default is 60 seconds.
- Enter a Username in the format USERNAME. This is the *account used to authenticate* on page 3 with the Domain Controller.
- Enter a Password. The password used to validate the username to the Domain Controller. Enter it a second time in the Confirm password field.

Step 5: Save the configuration

When you are done, click ADD.

Configuration Result

Once the configuration is complete and the system has had time to gather data, you can view user login events from the configured Domain Controller servers on the Network \rightarrow Events page by clicking the User tab.

VMware, Inc. 3401 Hillview Ave. Palo Alto, CA 94304 www.vmware.com

Copyright © 2024 VMware, Inc. All rights reserved. Copyright and trademark information.