

ISEでのユーザごとのダイナミックアクセスコントロールリストの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ISEでの新しいカスタムユーザ属性の設定](#)

[dACLの設定](#)

[カスタム属性を使用した内部ユーザアカウントの設定](#)

[ADユーザアカウントの設定](#)

[ADからISEへの属性のインポート](#)

[内部および外部ユーザの許可プロファイルの設定](#)

[許可ポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、IDストアのタイプに存在するユーザのユーザごとのダイナミックアクセスコントロールリスト(dACL)の設定について説明します。

前提条件

要件

Identity Services Engine(ISE)のポリシー設定に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

ユーザごとのダイナミックアクセスコントロールリスト(DACL)の設定は、ISE内部IDストアまたは外部IDストアに存在するユーザ用です。

設定

ユーザ単位のdACLは、カスタムユーザ属性を使用する内部ストア内の任意のユーザに対して設定できます。Active Directory(AD)内のユーザの場合、文字列型の任意の属性を使用して同じ属性を実現できます。このセクションでは、ISEとADの両方で属性を設定するために必要な情報と、この機能を動作させるためにISEで必要な設定について説明します。

ISEでの新しいカスタムユーザ属性の設定

Administration > Identity Management > Settings > User Custom Attributesの順に移動します。新しい属性を追加して変更を保存するには、図に示すように+ボタンをクリックします。この例では、カスタム属性の名前はACLです。

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and status indicators for 'Evaluation Mode 27 Days' and 'License Warning'. The main menu on the left lists 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Settings' section is expanded to show 'User Custom Attributes'. A table lists existing attributes with columns for 'Mandatory', 'Attribute Name', and 'Data Type'. A new attribute 'ACL' is being added, with a description 'Attribute for ACL per us', data type 'String', and parameters 'String Max length'. The 'Default Value Mandatory' column shows a plus sign and a plus button. At the bottom right, there are 'Save' and 'Reset' buttons.

Mandatory	Attribute Name	Data Type
	AllowPasswordChangeAfterLogin	String
	Description	String
	EmailAddress	String
	EnableFlag	String
	EnablePassword	String
	Firstname	String
	Lastname	String
✓	Name	String
	Password (Credential:Password)	String

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
ACL	Attribute for ACL per us	String	String Max length	+	<input type="checkbox"/>

dACLの設定

ダウンロード可能ACLを設定するには、Policy > Policy Elements > Results > Authorization > Downloadable ACLsの順に移動します。[Add] をクリックします。名前とdACLの内容を指定し、変更を保存します。図に示すように、dACLの名前はNotMuchAccessです。

Dictionaryes Conditions **Results**

Downloadable ACL List > New Downloadable ACL

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Downloadable ACL

* Name NotMuchAccess

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0414243	
AAAAA	

Check DACL Syntax ⓘ

Submit

カスタム属性を使用した内部ユーザアカウントの設定

Administration > Identity Management > Identities > Users > Addの順に移動します。ユーザを作成し、認可されたときにユーザが取得する必要があるdACLの名前を使用してカスタム属性値を設定します。この例では、dACLの名前はNotMuchAccessです。

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Name testuserinternal

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password ●●●●●● ●●●●●● Generate Password ⓘ

Enable Password Generate Password ⓘ

> User Information

> Account Options

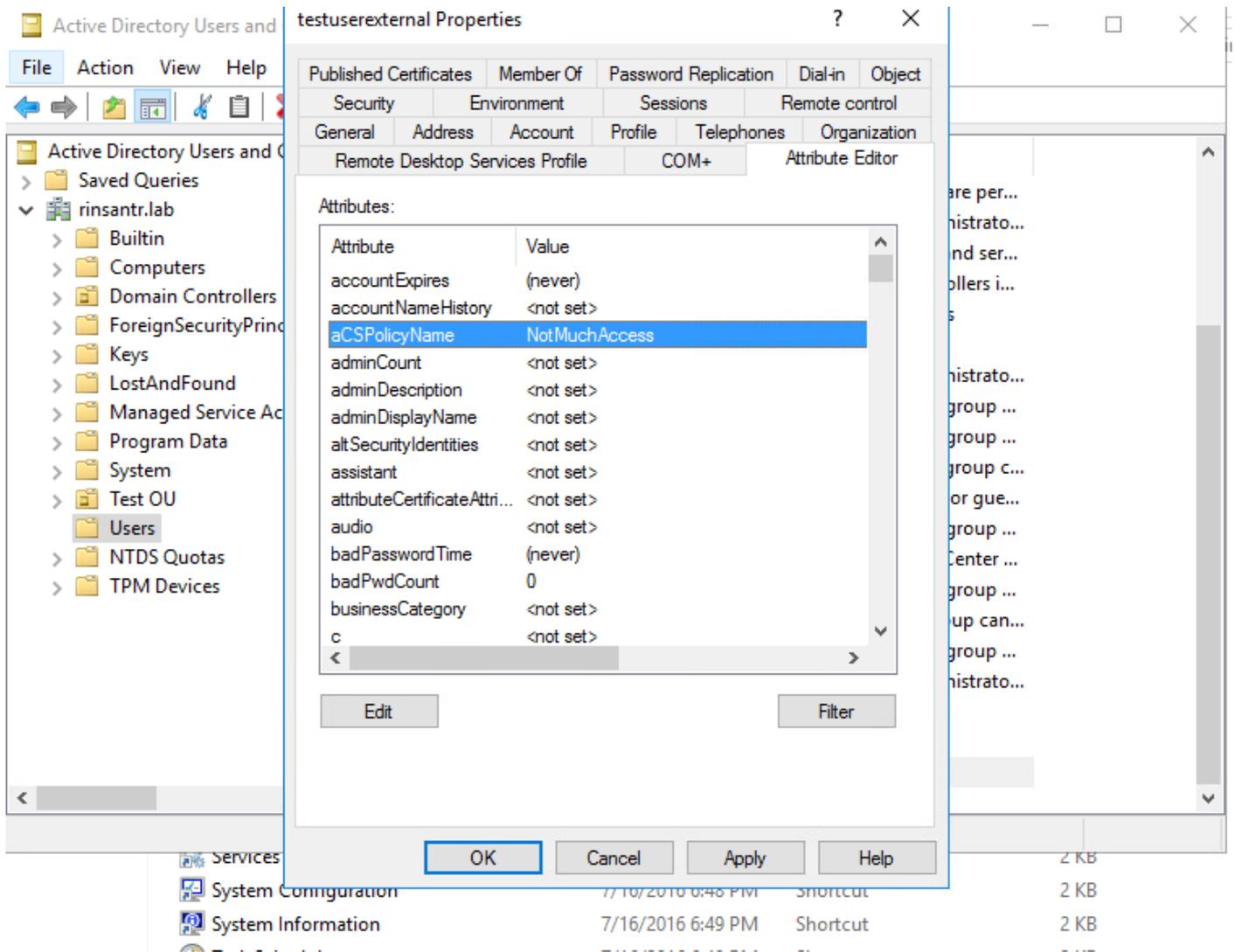
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

ADユーザアカウントの設定

Active Directoryで、ユーザアカウントのプロパティに移動し、次にAttribute Editorタブに移動します。図に示すように、aCSPolicyNameはdACL名を指定するために使用される属性です。ただし、前述のように、文字列値を受け入れることができる属性も使用できます。



ADからISEへの属性のインポート

ADで設定された属性を使用するには、ISEでインポートする必要があります。属性をインポートするには、Administration > Identity Management > External Identity Sources > Active Directory > [Join point configured] > Attributes タブに移動します。Addをクリックし、次にSelect Attributes From Directoryをクリックします。ADでユーザアカウント名を入力し、Retrieve Attributesをクリックします。dACLに設定されている属性を選択し、OKをクリックしてから、Saveをクリックします。図に示すように、aCSPolicyNameは属性です。

Directory Attributes

Only attributes selected below will be available for use as policy conditions in policy rules.

* Sample User or Machine

Account

testuserexternal



Retrieve Attributes...

<input type="checkbox"/>	Name	Type	Example Value
<input checked="" type="checkbox"/>	aCSPolicyName	STRING	NotMuchAccess
<input type="checkbox"/>	accountExpires	STRING	9223372036854775807
<input type="checkbox"/>	badPasswordTime	STRING	0
<input type="checkbox"/>	badPwdCount	STRING	0
<input type="checkbox"/>	cn	STRING	testuserexternal
<input type="checkbox"/>	codePage	STRING	0
<input type="checkbox"/>	countryCode	STRING	0
<input type="checkbox"/>	dSCorePropagationData	STRING	16010101000000.0Z
<input type="checkbox"/>	displayName	STRING	testuserexternal
<input type="checkbox"/>	distinguishedName	STRING	CN=testuserexternal,CN=Users,DC=rinsantr,DC=lab

Cancel OK

Cisco ISE Administration - Identity Management

External Identity Sources

External Identity Sources: Certificate Authentication F, Active Directory, RiniAD, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Social Login

Attributes

Name	Type	Default	Internal Name
<input type="checkbox"/> aCSPolicyName	STRING		aCSPolicyName

Save Reset

内部および外部ユーザの許可プロファイルの設定

認可プロファイルを設定するには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動します。[Add] をクリックします。内部ユーザの名前を指定し、dACL名にInternalUser:<作成されるカスタム属性の名前> を選択します。図に示すように、内部

ユーザのプロファイルInternalUserAttributeTestは、InternalUser:ACLとして設定されたdACLを使用して設定されます。

Cisco ISE Policy • Policy Elements

Dictionaryes Conditions **Results**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  Cisco

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

Common Tasks

DACL Name

外部ユーザの場合は、dACL名として<Join point name>:<attribute configured on AD> を使用します。この例では、プロファイルExternalUserAttributeTestに、RiniAD:aCSPolicyNameとして設定されたdACLが設定されています。ここで、RiniADは参加ポイント名です。

Dictionaryes Conditions **Results**

Authentication >

Authorization ▾

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type ▾

Network Device Profile  Cisco ▾ ⊕

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

▾ Common Tasks

DACL Name ▾

許可ポリシーの設定

認可ポリシーは、ADに存在する外部ユーザのグループに基づいて、またISE内部IDストア内のユーザ名に基づいて、Policy > Policy Setsで設定できます。この例では、testuserexternalはグループrinsantr.lab/Users/Test Groupに存在するユーザで、testuserinternalはISE内部IDストアに存在するユーザです。

Status	Rule Name	Conditions	Results	
			Profiles	Security Groups
+	Search			
✓	Basic Authenticated Access Internal User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed Radius-User-Name EQUALS testuserinternal	InternalUserAttributeTe... x	Select from list
✓	Basic Authenticated Access External User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed RiniAD-ExternalGroups EQUALS rinsantr.lab/Users/Test Group	ExternalUserAttributeT... x	Select from list
✓	Default		DenyAccess x	Select from list

確認

このセクションを使用して、設定が機能するかどうかを確認します。

RADIUSライブログをチェックして、ユーザ認証を確認します。

内部ユーザ :

Jan 18, 2021 03:27:11.5...	✓	🔍	#ACSACL#-IP-...				
Jan 18, 2021 03:27:11.5...	✓	🔍	testuserinternal	B4:96:91:26:E0:2B	Intel-Device	New Polic...	InternalUs...

外部ユーザ :

Jan 18, 2021 03:39:33.3...	✓	🔍	#ACSACL#-IP-...				
Jan 18, 2021 03:39:33.3...	✓	🔍	testuserexternal	B4:96:91:26:E0:2B	Intel-Device	New Polic...	ExternalUs...

成功したユーザ認証の虫眼鏡アイコンをクリックして、詳細ライブログの「概要」セクションで要求が正しいポリシーに一致するかどうかを確認します。

内部ユーザ :

Overview

Event	5200 Authentication succeeded
Username	testuserinternal
Endpoint Id	B4:96:91:26:E0:2B ⓘ
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Authorization Policy	New Policy Set 1 >> Basic Authenticated Access Internal User
Authorization Result	InternalUserAttributeTest

外部ユーザ :

Overview

Event	5200 Authentication succeeded
Username	testuserexternal
Endpoint Id	B4:96:91:26:E0:2B ⓘ
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Authorization Policy	New Policy Set 1 >> Basic Authenticated Access External User
Authorization Result	ExternalUserAttributeTest

詳細なライブログのOther Attributesセクションをチェックして、ユーザ属性が取得されているかどうかを確認します。

内部ユーザ :

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

外部ユーザ :

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

詳細なライブログの結果セクションをチェックして、dACL属性がAccess-Acceptの一部として送信されているかどうかを確認します。

cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-NotMuchAccess-60049cbb
---------------	--

また、RADIUSライブログをチェックして、ユーザ認証の後にdACLがダウンロードされているかどうかを確認します。

Jan 18, 2021 03:39:33.3...



#ACSACL#-IP-NotMuchAccess-60049cbb

dACLのダウンロードに成功したログで虫眼鏡のアイコンをクリックし、「概要」セクションを確認してdACLのダウンロードを確認します。

Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-NotMuchAccess-60049cbb
Endpoint Id	
Endpoint Profile	
Authorization Result	

dACLの内容を確認するには、この詳細レポートの「結果」セクションを確認します。

cisco-av-pair

ip:inacl#1=permit ip any any

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。