Authentication Policies and Authentication Policy Silos

learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn486813(v=ws.11)

- Article
- 08/31/2016

In this article

Applies To: Windows 8.1, Windows Server 2012 R2

This topic for the IT professional describes authentication policy silos and the policies that can restrict accounts to those silos. It also explains how authentication policies can be used to restrict the scope of accounts.

Authentication policy silos and the accompanying policies provide a way to contain high-privilege credentials to systems that are only pertinent to selected users, computers, or services. Silos can be defined and managed in Active Directory Domain Services (AD DS) by using the Active Directory Administrative Center and the Active Directory Windows PowerShell cmdlets.

Authentication policy silos are containers to which administrators can assign user accounts, computer accounts, and service accounts. Sets of accounts can then be managed by the authentication policies that have been applied to that container. This reduces the need for the administrator to track access to resources for individual accounts, and helps prevent malicious users from accessing other resources through credential theft.

Capabilities introduced in Windows Server 2012 R2, allow you to create authentication policy silos, which host a set of high-privilege users. You can then assign authentication policies for this container to limit where privileged accounts can be used in the domain. When accounts are in the Protected Users security group, additional controls are applied, such as the exclusive use of the Kerberos protocol.

With these capabilities, you can limit high-value account usage to high-value hosts. For example, you could create a new Forest Administrators silo that contains enterprise, schema, and domain administrators. Then you could configure the silo with an authentication policy so that password and smartcard-based authentication from systems other than domain controllers and domain administrator consoles would fail.

For information about configuring authentication policy silos and authentication policies, see How to Configure Protected Accounts.

About authentication policy silos

An authentication policy silo controls which accounts can be restricted by the silo and defines the authentication policies to apply to the members. You can create the silo based on the requirements of your organization. The silos are Active Directory objects for users, computers, and services as defined by the schema in the following table.

Active Directory schema for authentication policy silos

Display Name	Description
Authentication Policy Silo	An instance of this class defines authentication policies and related behaviors for assigned users, computers, and services.
Authentication Policy Silos	A container of this class can contain authentication policy silo objects.
Authentication Policy Silo Enforced	Specifies whether the authentication policy silo is enforced. When not enforced, the policy by default is in audit mode. Events that indicate potential successes and failures are generated, but protections are not applied to the system.
Assigned Authentication Policy Silo Backlink	This attribute is the back link for msDS-AssignedAuthNPolicySilo.
Authentication Policy Silo Members	Specifies which principals are assigned to the AuthNPolicySilo.
Authentication Policy Silo Members Backlink	This attribute is the back link for msDS-AuthNPolicySiloMembers.

Authentication policy silos can be configured by using the Active Directory Administrative Console or Windows PowerShell. For more information, see How to Configure Protected Accounts.

About authentication policies

An authentication policy defines the Kerberos protocol ticket-granting ticket (TGT) lifetime properties and authentication access control conditions for an account type. The policy is built on and controls the AD DS container known as the authentication policy silo.

Authentication policies control the following:

- The TGT lifetime for the account, which is set to be non-renewable.
- The criteria that device accounts need to meet to sign in with a password or a certificate.
- The criteria that users and devices need to meet to authenticate to services running as part of the account.

The Active Directory account type determines the caller's role as one of the following:

- **User**

  Users should always be members of the Protected Users security group, which by default rejects attempts to authentication using NTLM.

  Policies can be configured to set the TGT lifetime of a user account to a shorter value or restrict the devices to which a user account can sign in. Rich expressions can be configured in the authentication policy to control the criteria that the users and their devices need to meet to authenticate to the service.

  For more information see Protected Users Security Group.

- **Service**

  Standalone managed service accounts, group managed service accounts, or a custom account object that is derived from these two types of service accounts are used. Policies can set a device's access control conditions, which are used to restrict managed service account credentials to specific devices with an Active Directory identity. Services should never be members of the Protected Users security group because all incoming authentication will fail.

- **Computer**

  The computer account object or the custom account object that is derived from the computer account object is used. Policies can set the access control conditions that are required to allow authentication to the account based on user and device properties. Computers should never be members of the Protected Users security group because all incoming authentication will fail. By default, attempts to use NTLM authentication are rejected. A TGT lifetime should not be configured for computer accounts.

Note

It is possible to set an authentication policy on a set of accounts without associating the policy to an authentication policy silo. You can use this strategy when you have a single account to protect.

Active Directory schema for authentication policies

The policies for the Active Directory objects for users, computers, and services are defined by the schema in the following table.

Type	Display Name	Description
Policy	Authentication Policy	An instance of this class defines authentication policy behaviors for assigned principals.
Policy	Authentication Policies	A container of this class can contain authentication policy objects.
Policy	Authentication Policy Enforced	Specifies whether the authentication policy is enforced. When not enforced, the policy by default is in audit mode, and events that indicate potential successes and failures are generated, but protections are not applied to the system.
Policy	Assigned Authentication Policy Backlink	This attribute is the back link for msDS-AssignedAuthNPolicy.
Policy	Assigned Authentication Policy	Specifies which AuthNPolicy should be applied to this principal.
User	User Authentication Policy	Specifies which AuthNPolicy should be applied to users who are assigned to this silo object.
User	User Authentication Policy Backlink	This attribute is the back link for msDS-UserAuthNPolicy.
User	ms-DS-User-Allowed-To-Authenticate-To	This attribute is used to determine the set of principals allowed to authenticate to a service running under the user account.
User	ms-DS-User-Allowed-To-Authenticate-From	This attribute is used to determine the set of devices to which a user account has permission to sign in.

Type	Display Name	Description
User	User TGT Lifetime	Specifies the maximum age of a Kerberos TGT that is issued to a user (expressed in seconds). Resultant TGTs are non-renewable.
Computer	Computer Authentication Policy	Specifies which AuthNPolicy should be applied to computers that are assigned to this silo object.
Computer	Computer Authentication Policy Backlink	This attribute is the back link for msDS-ComputerAuthNPolicy.
Computer	ms-DS-Computer-Allowed-To-Authenticate-To	This attribute is used to determine the set of principals that are allowed to authenticate to a service running under the computer account.
Computer	Computer TGT Lifetime	Specifies the maximum age of a Kerberos TGT that is issued to a computer (expressed in seconds). It is not recommended to change this setting.
Service	Service Authentication Policy	Specifies which AuthNPolicy should be applied to services that are assigned to this silo object.
Service	Service Authentication Policy Backlink	This attribute is the back link for msDS-ServiceAuthNPolicy.
Service	ms-DS-Service-Allowed-To-Authenticate-To	This attribute is used to determine the set of principals that are allowed to authenticate to a service running under the service account.
Service	ms-DS-Service-Allowed-To-Authenticate-From	This attribute is used to determine the set of devices to which a service account has permission to sign in.

Type	Display Name	Description
Service	Service TGT Lifetime	Specifies the maximum age of a Kerberos TGT that is issued to a service (expressed in seconds).

Authentication policies can be configured for each silo by using the Active Directory Administrative Console or Windows PowerShell. For more information, see How to Configure Protected Accounts.

How it works

This section describes how authentication policy silos and authentication policies work in conjunction with the Protected Users security group and implementation of the Kerberos protocol in Windows.

- How the Kerberos protocol is used with authentication policy silos and policies
- How restricting a user sign-in works
- How restricting service ticket issuance works

Protected accounts

The Protected Users security group triggers non-configurable protection on devices and host computers running Windows Server 2012 R2 and Windows 8.1, and on domain controllers in domains with a primary domain controller running Windows Server 2012 R2. Depending on the domain functional level of the account, members of the Protected Users security group are further protected because of changes in the authentication methods that are supported in Windows.

- The member of the Protected Users security group cannot authenticate by using NTLM, Digest Authentication, or CredSSP default credential delegation. On a device running Windows 8.1 that uses any one of these Security Support Providers (SSPs), authentication to a domain will fail when the account is a member of the Protected Users security group.
- The Kerberos protocol will not use the weaker DES or RC4 encryption types in the preauthentication process. This means that the domain must be configured to support at least the AES encryption type.
- The user’s account cannot be delegated with Kerberos constrained or unconstrained delegation. This means that former connections to other systems may fail if the user is a member of the Protected Users security group.

- The default Kerberos TGTs lifetime setting of four hours is configurable by using authentication policies and silos, which can be accessed through the Active Directory Administrative Center. This means that when four hours has passed, the user must authenticate again.

For more information about this security group, see How the Protected Users group works.

Silos and authentication policies

Authentication policy silos and authentication policies leverage the existing Windows authentication infrastructure. The use of the NTLM protocol is rejected, and the Kerberos protocol with newer encryption types is used. Authentication policies complement the Protected Users security group by providing a way to apply configurable restrictions to accounts, in addition to providing restrictions for accounts for services and computers. Authentication policies are enforced during the Kerberos protocol authentication service (AS) or ticket-granting service (TGS) exchange. For more information about how Windows uses the Kerberos protocol, and what changes have been made to support authentication policy silos and authentication policies, see:

- How the Kerberos Version 5 Authentication Protocol Works
- What's New in Kerberos Authentication (Windows Server 2012)
- Changes in Kerberos Authentication (Windows Server 2008 R2 and Windows 7)

How the Kerberos protocol is used with authentication policy silos and policies

When a domain account is linked to an authentication policy silo, and the user signs in, the Security Accounts Manager adds the claim type of Authentication Policy Silo that includes the silo as the value. This claim on the account provides the access to the targeted silo.

When an authentication policy is enforced and the authentication service request for a domain account is received on the domain controller, the domain controller returns a non-renewable TGT with the configured lifetime (unless the domain TGT lifetime is shorter).

Note

The domain account must have a configured TGT lifetime and must be either directly linked to the policy or indirectly linked through the silo membership.

When an authentication policy is in audit mode and the authentication service request for a domain account is received on the domain controller, the domain controller checks if authentication is allowed for the device so that it can log a warning if there is a failure. An audited authentication policy does not alter the process, so authentication requests will not fail if they do not meet the requirements of the policy.

Note

The domain account must be either directly linked to the policy or indirectly linked through the silo membership.

When an authentication policy is enforced and the authentication service is armored, the authentication service request for a domain account is received on the domain controller, the domain controller checks if authentication is allowed for the device. If it fails, the domain controller returns an error message and logs an event. For information about Kerberos armoring, see Support for claims, compound authentication, and Kerberos armoring.

Note

The domain account must be either directly linked to the policy or indirectly linked through the silo membership.

When an authentication policy is in audit mode and a ticket-granting service request is received by the domain controller for a domain account, the domain controller checks if authentication is allowed based on the request's ticket Privilege Attribute Certificate (PAC) data, and it logs a warning message if it fails. The PAC contains various types of authorization data, including groups that the user is a member of, rights the user has, and what policies apply to the user. This information is used to generate the user's access token. If it is an enforced authentication policy which allows authentication to a user, device, or service, the domain controller checks if authentication is allowed based on the request's ticket PAC data. If it fails, the domain controller returns an error message and logs an event.

Note

The domain account must be either directly linked or linked through silo membership to an audited authentication policy which allows authentication to a user, device or service,

You can use a single authentication policy for all members of a silo, or you can use separate policies for users, computers, and managed service accounts.

Authentication policies can be configured for each silo by using the Active Directory Administrative Console or Windows PowerShell. For more information, see How to Configure Protected Accounts.

How restricting a user sign-in works

Because these authentication policies are applied to an account, it also applies to accounts that are used by services. If you want to limit the usage of a password for a service to specific hosts, this setting is useful. For example, group managed service accounts are configured where the hosts are allowed to retrieve the password from Active Directory Domain Services. However, that password can be used from any host for initial authentication. By applying an access control condition, an additional layer of protection can be achieved by limiting the password to only the set of hosts that can retrieve the password.

When services that run as system, network service, or other local service identity connect to network services, they use the host's computer account. Computer accounts cannot be restricted. So even if the service is using a computer account that is not for a Windows host, it cannot be restricted.

Restricting user sign-in to specific hosts requires the domain controller to validate the host's identity. When using Kerberos authentication with Kerberos armoring (which is part of Dynamic Access Control), the Key Distribution Center is provided with the TGT of the host from which the user is authenticating. The content of this armored TGT is used to complete an access check to determine if the host is allowed.

When a user signs in to Windows or enters their domain credentials in a credential prompt for an application, by default, Windows sends an unarmored AS-REQ to the domain controller. If the user is sending the request from a computer that does not support armoring, such as computers running Windows 7 or Windows Vista, the request fails.

The following list describes the process:

- The domain controller in a domain running Windows Server 2012 R2 queries for the user account and determines if it is configured with an authentication policy that restricts initial authentication that requires armored requests.
- The domain controller will fail the request.
- Because armoring is required, the user can attempt to sign in by using a computer running Windows 8.1 or Windows 8, which is enabled to support Kerberos armoring to retry the sign-in process.
- Windows detects that the domain supports Kerberos armoring and sends an armored AS-REQ to retry the sign-in request.
- The domain controller performs an access check by using the configured access control conditions and the client operating system's identity information in the TGT that was used to armor the request.
- If the access check fails, the domain controller rejects the request.

Even when operating systems support Kerberos armoring, access control requirements can be applied and must be met before access is granted. Users sign in to Windows or enter their domain credentials in a credential prompt for an application. By default, Windows sends an unarmored AS-REQ to the domain controller. If the user is sending the request from a computer that supports armoring, such as Windows 8.1 or Windows 8, authentication policies are evaluated as follows:

1. The domain controller in a domain running Windows Server 2012 R2 queries for the user account and determines if it is configured with an authentication policy that restricts initial authentication that requires armored requests.
2. The domain controller performs an access check by using the configured access control conditions and the system's identity information in the TGT that is used to armor the request. The access check succeeds.

   Note

   If legacy workgroup restrictions are configured, those also need to be met.
3. The domain controller replies with an armored reply (AS-REP), and the authentication continues.

How restricting service ticket issuance works

When an account is not allowed and a user who has a TGT attempts to connect to the service (such as by opening an application that requires authentication to a service that is identified by the service's service principal name (SPN), the following sequence occurs:

1. In an attempt to connect to SPN1 from SPN, Windows sends a TGS-REQ to the domain controller that is requesting a service ticket to SPN1.
2. The domain controller in a domain running Windows Server 2012 R2 looks up SPN1 to find the Active Directory Domain Services account for the service and determines that the account is configured with an authentication policy that restricts service ticket issuance.
3. The domain controller performs an access check by using the configured access control conditions and the user's identity information in the TGT. The access check fails.
4. The domain controller rejects the request.

When an account is allowed because the account meets the access control conditions that are set by the authentication policy, and a user who has a TGT attempts to connect to the service (such as by opening an application that requires authentication to a service that is identified by the service's SPN), the following sequence occurs:

1. In an attempt to connect to SPN1, Windows sends a TGS-REQ to the domain controller that is requesting a service ticket to SPN1.
2. The domain controller in a domain running Windows Server 2012 R2 looks up SPN1 to find the Active Directory Domain Services account for the service and determines that the account is configured with an authentication policy that restricts service ticket issuance.

3. The domain controller performs an access check by using the configured access control conditions and the user's identity information in the TGT. The access check succeeds.

4. The domain controller replies to the request with a ticket-granting service reply (TGS-REP).

Associated error and informational event messages

The following table describes the events that are associated with Protected Users security group and the authentication policies that are applied to authentication policy silos.

The events are recorded in the Applications and Services Logs at **Microsoft\Windows\Authentication**.

For troubleshooting steps that use these events, see Troubleshoot Authentication Policies and Troubleshoot events related to Protected Users.

Event ID and Log	Description
101 **AuthenticationPolicyFailures-DomainController**	Reason: An NTLM sign-in failure occurs because the authentication policy is configured. An event is logged in the domain controller to indicate that NTLM authentication failed because access control restrictions are required, and those restrictions cannot be applied to NTLM. Displays the account, device, policy, and silo names.
105 **AuthenticationPolicyFailures-DomainController**	Reason: A Kerberos restriction failure occurs because the authentication from a particular device was not permitted. An event is logged in the domain controller to indicate that a Kerberos TGT was denied because the device did not meet the enforced access control restrictions. Displays the account, device, policy, silo names, and TGT lifetime.

Event ID and Log	Description
305 **AuthenticationPolicyFailures-DomainController**	Reason: A potential Kerberos restriction failure might occur because the authentication from a particular device was not permitted. In audit mode, an informational event is logged in the domain controller to determine if a Kerberos TGT will be denied because the device did not meet the access control restrictions. Displays the account, device, policy, silo names, and TGT lifetime.
106 **AuthenticationPolicyFailures-DomainController**	Reason: A Kerberos restriction failure occurs because the user or device was not allowed to authenticate to the server. An event is logged in the domain controller to indicate that a Kerberos service ticket was denied because the user, device, or both do not meet the enforced access control restrictions. Displays the device, policy, and silo names.
306 **AuthenticationPolicyFailures-DomainController**	Reason: A Kerberos restriction failure might occur because the user or device was not allowed to authenticate to the server. In audit mode, an informational event is logged on the domain controller to indicate that a Kerberos service ticket will be denied because the user, device, or both do not meet the access control restrictions. Displays the device, policy, and silo names.

See also

How to Configure Protected Accounts

Credentials Protection and Management

Protected Users Security Group