Sicherer Dateizugriff über Dynamic Access Control (DAC)

ONTAP 9

NetApp
April 24, 2024

Inhalt

Sicherer Dateizugriff über Dynamic Access Control (DAC)

Sicherer Dateizugriff über Dynamic Access Control (DAC) mit Übersicht

Der Zugriff lässt sich mithilfe der dynamischen Zugriffssteuerung und der Erstellung zentraler Zugriffsrichtlinien in Active Directory sichern. Darüber hinaus werden sie über Applicate Group Policy Objects (GPOs) auf Dateien und Ordner auf SVMs angewendet. Sie können die Prüfung so konfigurieren, dass zentrale Zugriffs-Policy-Staging-Ereignisse verwendet werden, um die Auswirkungen von Änderungen auf zentrale Zugriffsrichtlinien zu sehen, bevor Sie sie anwenden.

Erweiterung zu CIFS-Anmeldeinformationen

Vor der Dynamic Access Control wurde eine CIFS-Berechtigung mit der Identität eines Sicherheitprinzipals (des Benutzers) und der Mitgliedschaft in einer Windows-Gruppe ausgestattet. Mit der Dynamic Access Control werden drei weitere Arten von Informationen zu den Anmeldeinformationsinformationen, Geräteansprüchen und Benutzeransprüchen hinzugefügt:

- Geräteidentität

  Analog zu den Identitätsinformationen des Benutzers, außer es handelt sich um die Identität und die Gruppenmitgliedschaft des Geräts, von dem sich der Benutzer anmeldet.

- Geräteforderungen

  Behauptungen über einen Sicherheitprinzipal des Geräts. Ein Geräteanspruch kann beispielsweise sein, dass er Mitglied einer bestimmten Organisationseinheit ist.

- Benutzerforderungen

  Behauptungen zu einem Sicherheitprinzipal des Benutzers. Beispielsweise kann eine Benutzerforderung sein, dass ihr AD Konto Mitglied einer bestimmten Organisationseinheit ist.

Zentrale Zugriffsrichtlinien

Zentrale Zugriffsrichtlinien für Dateien ermöglichen Unternehmen die zentrale Bereitstellung und Verwaltung von Autorisierungsrichtlinien, die bedingte Ausdrücke mit Benutzergruppen, Benutzerforderungen, Geräteforderungen und Ressourceneigenschaften beinhalten.

Zum Beispiel muss ein Benutzer zum Zugriff auf Daten mit großen geschäftlichen Auswirkungen ein Vollzeit-Mitarbeiter sein und nur über ein gemanagtes Gerät auf die Daten zugreifen können. Zentrale Zugriffsrichtlinien werden in Active Directory definiert und über den GPO-Mechanismus auf Dateiserver verteilt.

Zentrale Zugriffsrichtlinien-Staging mit erweitertem Auditing

Zentrale Zugriffsrichtlinien können „`steed`“ sein, in diesem Fall werden sie während der Dateizugriffskontrollen auf „`Was-wäre-wenn`“ geprüft. Die Ergebnisse dessen, was passiert wäre, wenn die Richtlinie wirksam wäre

und wie sich diese von den derzeit konfigurierten unterscheidet, werden als Audit-Ereignis protokolliert. Auf diese Weise können Administratoren mithilfe von Audit-Ereignisprotokollen die Auswirkungen einer Änderung der Zugriffsrichtlinie untersuchen, bevor diese tatsächlich eingesetzt wird. Nachdem Sie die Auswirkungen einer Änderung der Zugriffsrichtlinien evaluiert haben, kann die Richtlinie über Gruppenrichtlinienobjekte zu den gewünschten SVMs implementiert werden.

Verwandte Informationen

Unterstützte Gruppenrichtlinienobjekte

Werden Gruppenrichtlinienobjekte auf CIFS-Server angewendet

Aktivieren oder Deaktivieren der GPO-Unterstützung auf einem CIFS-Server

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Anzeigen von Informationen zur Dynamic Access Control-Sicherheit

"SMB- und NFS-Auditing und Sicherheits-Tracing"

Unterstützte Dynamic Access Control-Funktionen

Wenn Sie Dynamic Access Control (DAC) auf Ihrem CIFS-Server verwenden möchten, müssen Sie verstehen, wie ONTAP die Dynamic Access Control-Funktionalität in Active Directory-Umgebungen unterstützt.

Wird für Dynamic Access Control unterstützt

ONTAP unterstützt die folgenden Funktionen, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Forderungen an das Filesystem	Forderungen sind einfache Name- und Wertpaare, die die Wahrheit über einen Benutzer angeben. Benutzerkennung enthält Informationen zu Ansprüchen, und Sicherheitsbeschreibungen in Dateien können Zugriffsprüfungen durchführen, die Schadenprüfungen umfassen. So erhalten Administratoren mehr Kontrolle darüber, wer auf Dateien zugreifen kann.
Bedingte Ausdrücke zu Dateizugriffsprüfungen	Beim Ändern der Sicherheitsparameter einer Datei können Benutzer willkürlich komplexe bedingte Ausdrücke zum Sicherheitsdeskriptor der Datei hinzufügen. Der bedingte Ausdruck kann Prüfungen für Forderungen enthalten.

Funktionalität	Kommentare
Zentrale Steuerung des Dateizugriffs über zentrale Zugriffsrichtlinien	Zentrale Zugriffsrichtlinien sind eine Art ACL, die in Active Directory gespeichert ist und mit einer Datei gekennzeichnet werden kann. Der Zugriff auf die Datei wird nur gewährt, wenn die Zugriffskontrollen sowohl des Sicherheitsdeskriptors auf der Festplatte als auch der getaggten zentralen Zugriffsrichtlinie den Zugriff ermöglichen.auf diese Weise können Administratoren den Zugriff auf Dateien von einem zentralen Speicherort (AD) aus steuern, ohne den Sicherheitsdeskriptor auf der Festplatte ändern zu müssen.
Zentrale Zugriffsrichtlinien-Staging	Fügt die Möglichkeit hinzu, Sicherheitsänderungen auszuprobieren, ohne den tatsächlichen Dateizugriff zu beeinträchtigen, indem Sie „`staging`“ eine Änderung der zentralen Zugriffsrichtlinien vornehmen und die Auswirkung der Änderung in einem Audit-Bericht sehen.
Unterstützung zum Anzeigen von Informationen zur Sicherheit zentraler Zugriffsrichtlinien über die ONTAP-CLI	Erweitert die `vserver security file-directory show` Befehl zum Anzeigen von Informationen über angewandte zentrale Zugriffsrichtlinien.
Verfolgung der Sicherheit, einschließlich zentraler Zugriffsrichtlinien	Erweitert die `vserver security trace` Befehlsfamilie, um Ergebnisse anzuzeigen, die Informationen zu angewandten zentralen Zugriffsrichtlinien enthalten.

Nicht unterstützt für Dynamic Access Control

ONTAP unterstützt die folgenden Funktionen nicht, wenn die dynamische Zugriffssteuerung auf dem CIFS-Server aktiviert ist:

Funktionalität	Kommentare
Automatische Klassifizierung von NTFS-Dateisystemobjekten	Dies ist eine Erweiterung der Windows File Classification Infrastructure, die in ONTAP nicht unterstützt wird.
Erweiterte Audits außer der zentralen Zugriffsrichtlinien-Staging	Für erweiterte Audits wird nur das Staging von zentralen Zugriffsrichtlinien unterstützt.

Überlegungen bei der Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien mit CIFS-Servern

Bei der Verwendung von Dynamic Access Control (DAC) und zentralen Zugriffsrichtlinien

zum Sichern von Dateien und Ordnern auf CIFS-Servern müssen Sie bestimmte Überlegungen beachten.

Der NFS-Zugriff kann auf Root verweigert werden, wenn eine Richtlinienregel auf Domain\Administrator-Benutzer angewendet wird

Unter bestimmten Umständen wird der NFS-Zugriff auf Root verweigert, wenn auf die Daten angewendet wird, auf die der Root-Benutzer zugreifen möchte. Das Problem tritt auf, wenn die zentrale Zugriffsrichtlinie eine Regel enthält, die auf die Domäne\Administrator angewendet wird und das Root-Konto dem Domain\Administrator-Konto zugeordnet ist.

Statt eine Regel auf den Domänenadministrator\anzuwenden, sollten Sie die Regel auf eine Gruppe mit Administratorrechten anwenden, z. B. die Gruppe Domain\Administratoren. Auf diese Weise können Sie Root dem Domain\Administrator-Konto zuordnen, ohne dass Root von diesem Problem betroffen ist.

Die BUILTIN\Administrators-Gruppe des CIFS-Servers hat Zugriff auf Ressourcen, wenn die angewandte zentrale Zugriffsrichtlinie nicht in Active Directory gefunden wird

Es ist möglich, dass Ressourcen innerhalb des CIFS-Servers zentrale Zugriffsrichtlinien auf sie angewendet werden, aber wenn der CIFS-Server die SID der zentralen Zugriffsrichtlinie verwendet, um zu versuchen, Informationen aus Active Directory abzurufen, stimmt die SID keiner vorhandenen zentralen Zugriffsrichtlinien-SIDs in Active Directory überein. Unter diesen Umständen wendet der CIFS-Server die lokale Standard-Recovery-Richtlinie für diese Ressource an.

Die lokale Standard-Wiederherstellungsrichtlinie ermöglicht den Zugriff der BUILTIN\-Administratorgruppe des CIFS-Servers auf diese Ressource.

Aktiviert oder deaktiviert die Übersicht über die dynamische Zugriffskontrolle

Die Option, mit der Sie Dynamic Access Control (DAC) zum Sichern von Objekten auf Ihrem CIFS-Server verwenden können, ist standardmäßig deaktiviert. Sie müssen die Option aktivieren, wenn Sie die dynamische Zugriffssteuerung auf Ihrem CIFS-Server verwenden möchten. Wenn Sie später entscheiden, dass Sie Dynamic Access Control nicht zum Sichern von auf dem CIFS-Server gespeicherten Objekten verwenden möchten, können Sie die Option deaktivieren.

Über diese Aufgabe

Ist die Dynamic Access Control aktiviert, kann das Dateisystem ACLs mit Einträgen im Zusammenhang mit Dynamic Access Control enthalten. Wenn die dynamische Zugriffskontrolle deaktiviert ist, werden die aktuellen Einträge für die dynamische Zugriffskontrolle ignoriert und neue Einträge werden nicht zugelassen.

Diese Option ist nur auf der erweiterten Berechtigungsebene verfügbar.

Schritt

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie die dynamische Zugriffskontrolle benötigen,	Geben Sie den Befehl ein…
Aktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Deaktiviert	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

Verwandte Informationen

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Managen Sie ACLs, die dynamische Zugriffssteuerung enthalten, wenn die dynamische Zugriffskontrolle deaktiviert ist

Wenn Sie Ressourcen haben, bei denen ACLs mit Dynamic Access Control Aces angewendet werden, und Sie Dynamic Access Control auf der Storage Virtual Machine (SVM) deaktivieren, müssen Sie die Dynamic Access Control Aces entfernen, bevor Sie die nicht-dynamischen Zugriffssteuerungsmaßnahmen dieser Ressource verwalten können.

Über diese Aufgabe

Nachdem die Dynamic Access Control deaktiviert ist, können Sie vorhandene nicht-dynamische Access Control Aces nicht entfernen oder neue nicht-dynamische Access Control Aces hinzufügen, bis Sie die vorhandenen Dynamic Access Control Aces entfernt haben.

Sie können das jeweils verwendete Tool zum Verwalten von ACLs verwenden, um diese Schritte durchzuführen.

Schritte

1. Legen Sie fest, welche Dynamic Access Control Aces auf die Ressource angewendet werden.
2. Entfernen Sie die Dynamic Access Control Aces aus der Ressource.
3. Hinzufügen oder Entfernen von nicht-dynamischen Zugriffssteuerungsaces wie gewünscht aus der Ressource.

Konfiguration von zentralen Zugriffsrichtlinien zur Sicherung von Daten auf CIFS-Servern

Sie müssen verschiedene Schritte Unternehmen, um den Zugriff auf Daten auf dem CIFS-Server mithilfe von zentralen Zugriffsrichtlinien zu sichern. Hierzu zählen die Aktivierung von Dynamic Access Control (DAC) auf dem CIFS-Server, die Konfiguration zentraler Zugriffsrichtlinien in Active Directory, die Anwendung der zentralen Zugriffsrichtlinien auf Active Directory-Container mit GPOs, Und Aktivieren der

Gruppenrichtlinienobjekte auf dem CIFS-Server.

Bevor Sie beginnen

- Active Directory muss so konfiguriert sein, dass zentrale Zugriffsrichtlinien verwendet werden.
- Sie müssen über ausreichende Zugriffsmöglichkeiten auf den Active Directory-Domänencontrollern verfügen, um zentrale Zugriffsrichtlinien zu erstellen und Gruppenrichtlinienobjekte zu erstellen und auf die Container anzuwenden, die die CIFS-Server enthalten.
- Sie müssen über ausreichenden administrativen Zugriff auf der Storage Virtual Machine (SVM) verfügen, um die erforderlichen Befehle auszuführen.

Über diese Aufgabe

Zentrale Zugriffsrichtlinien werden definiert und auf Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, GPOs) in Active Directory angewendet. Anweisungen zur Konfiguration zentraler Zugriffsrichtlinien und Gruppenrichtlinienobjekte finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet-Bibliothek"

Schritte

1. Aktivieren Sie Dynamic Access Control auf der SVM, wenn sie nicht bereits über die aktiviert ist `vserver cifs options modify` Befehl.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Gruppenrichtlinienobjekte (Gruppenrichtlinienobjekte, Gruppenrichtlinienobjekte) auf dem CIFS-Server aktivieren, wenn sie nicht bereits mit dem aktiviert sind `vserver cifs group-policy modify` Befehl.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Zentrale Zugriffsregeln und zentrale Zugriffsrichtlinien für Active Directory erstellen
4. Erstellen eines Gruppenrichtlinienobjekts (GPO), um die zentralen Zugriffsrichtlinien in Active Directory zu implementieren.
5. Wenden Sie das GPO auf den Container an, in dem sich das CIFS-Servercomputer-Konto befindet.
6. Aktualisieren Sie manuell die Gruppenrichtlinienobjekte, die auf den CIFS-Server angewendet wurden, indem Sie auf das verwenden `vserver cifs group-policy update` Befehl.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Überprüfen Sie, ob die GPO Central Access Policy auf die Ressourcen auf dem CIFS-Server angewendet wird. Verwenden Sie dazu die `vserver cifs group-policy show-applied` Befehl.

   Das folgende Beispiel zeigt, dass die Standard-Domänenrichtlinie zwei zentrale Zugriffsrichtlinien hat, die auf den CIFS-Server angewendet werden:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
   ```

```
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
```

```
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication Mode for BranchCache: per-share
        Hash Version Support for BranchCache: all-versions
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
  2 entries were displayed.
```

Verwandte Informationen

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Aktivieren oder Deaktivieren der Dynamic Access Control

Zeigt Informationen zur Dynamic Access Control-Sicherheit an

Sie können Informationen zur Dynamic Access Control (DAC)-Sicherheit auf NTFS-Volumes und zu Daten mit NTFS-effektiver Sicherheit für gemischte Security-Volumes anzeigen. Dazu gehören Informationen über bedingte Asse, Ressourcen-Asse und zentrale Zugangspolitik Aces. Sie können die Ergebnisse verwenden, um Ihre Sicherheitskonfiguration zu überprüfen oder Probleme mit dem Dateizugriff zu beheben.

Über diese Aufgabe

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Daten angeben, deren Sicherheitsinformationen für Datei oder Ordner angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

Schritt

1. Anzeige der Dateisicherheitseinstellungen und des Verzeichnisses mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Mit mehr Details	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Wobei Ausgabe mit Gruppen- und Benutzer-SIDs angezeigt wird	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Über die Datei- und Verzeichnissicherheit für Dateien und Verzeichnisse, in denen die hexadezimale Bitmaske in das Textformat übersetzt wird	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Beispiele

Im folgenden Beispiel werden die Sicherheitsinformationen zu Dynamic Access Control über den Pfad angezeigt `/vol1` In SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Verwandte Informationen

Anzeigen von Informationen zu GPO-Konfigurationen

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien

Anzeigen von Informationen zu zentralen Zugriffsrichtlinien-Regeln

Überlegungen zur Dynamic Access Control zurücksetzen

Sie sollten sich dessen bewusst sein, was beim Zurücksetzen auf eine Version von ONTAP passiert, die die dynamische Zugriffssteuerung (Dynamic Access Control, DAC)

nicht unterstützt, und was Sie vor und nach dem Zurücksetzen tun müssen.

Wenn Sie das Cluster auf eine Version von ONTAP zurücksetzen möchten, die keine dynamische Zugriffssteuerung unterstützt, und die dynamische Zugriffssteuerung ist auf einer oder mehreren Storage Virtual Machines (SVMs) aktiviert, müssen Sie vor dem Zurücksetzen die folgenden Schritte ausführen:

- Sie müssen Dynamic Access Control auf allen SVMs deaktivieren, auf denen sie auf dem Cluster aktiviert ist.
- Sie müssen alle Überwachungskonfigurationen auf dem Cluster ändern, die den enthalten `cap-staging` Ereignistyp, um nur das zu verwenden `file-op` Ereignistyp.

Sie müssen einige wichtige Überlegungen zum Zurücksetzen von Dateien und Ordnern mit Dynamic Access Control Aces verstehen und ausführen:

- Wenn der Cluster zurückgesetzt wird, werden vorhandene Dynamic Access Control Aces nicht entfernt. Diese werden jedoch bei der Überprüfung des Dateizugriffs ignoriert.
- Da Dynamic Access Control Aces nach der Reversion ignoriert werden, wird der Zugriff auf Dateien mit Dynamic Access Control Aces geändert.

  Dadurch konnten die Benutzer auf Dateien zugreifen, die zuvor nicht oder gar nicht auf Dateien zugreifen konnten.

- Sie sollten nicht-dynamische Zugriffssteuerung Aces auf die betroffenen Dateien anwenden, um ihre vorherige Sicherheitsstufe wiederherzustellen.

  Dies kann entweder vor dem Zurücksetzen oder unmittelbar nach Abschluss der Umversion erfolgen.

> Da Dynamic Access Control Aces nach der Reversion ignoriert werden, ist es nicht erforderlich, dass Sie sie entfernen, wenn Sie nicht-dynamische Access Control Aces auf die betroffenen Dateien anwenden. Sie können sie jedoch bei Bedarf manuell entfernen.

Hier finden Sie weitere Informationen zur Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien

Weitere Ressourcen unterstützen Sie bei der Konfiguration und Verwendung von Dynamic Access Control und zentralen Zugriffsrichtlinien.

Informationen zum Konfigurieren von Dynamic Access Control und zentralen Zugriffsrichtlinien in Active Directory finden Sie in der Microsoft TechNet-Bibliothek.

"Microsoft TechNet: Dynamic Access Control Scenario Overview"

"Microsoft TechNet: Zentrales Zugriffspolitik-Szenario"

Mithilfe der folgenden Referenzen können Sie den SMB-Server für die Verwendung und Unterstützung von Dynamic Access Control und zentralen Zugriffsrichtlinien konfigurieren:

- **Verwendung von GPOs auf dem SMB-Server**

  Werden Gruppenrichtlinienobjekte auf SMB-Server angewendet

- **Konfiguration der NAS-Prüfung auf dem SMB-Server**

  "SMB- und NFS-Auditing und Sicherheits-Tracing"