# Hilfsmittel zur Nutzung des Bausteins B 5.16 Active Directory

## Kerberos-Richtlinieneinstellungen für Domänen

Seitens des Herstellers wird empfohlen, keine Änderungen an den Standard-Werten der Gruppenrichtlinie bezüglich der Kerberos-Nutzung vorzunehmen. Jedoch kann in Einzelfällen eine Anpassung erforderlich sein. Die aufgeführte Tabelle beinhaltet die Einstellmöglichkeiten der Richtlinie, welche über "Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kerberos-Richtlinie\" aufgerufen werden kann:

| Richtlinie | Standardwert | Empfohlene Einstellung | Kommentare |
|---|---|---|---|
| Benutzeranmeldeeinschränkung erzwingen | Aktiviert | (Keine Änderung) | Ein Benutzer muss über das Recht verfügen, sich lokal anzumelden (für Dienste auf demselben Computer) oder über das Netzwerk auf den Dienst zuzugreifen. |
| Max. Gültigkeitsdauer des Diensttickets | 600 Minuten | (Keine Änderung) | |
| Max. Gültigkeitsdauer des Benutzertickets | 10 Stunden | (Keine Änderung) | |
| Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann | 7 Tage | (Keine Änderung) | |
| Max. Toleranz für die Synchronisation des Computertakts | 5 Minuten | (Keine Änderung) | Diese Richtlinie bezieht sich auf die maximal zulässige Abweichung zwischen den Client- und Server-Uhren. |

**Benutzeranmeldeeinschränkungen erzwingen**

Diese Sicherheitseinstellung bestimmt, ob das Kerberos V5-Schlüsselverteilungscenter (Key Distribution Center, KDC) jede Anforderung für ein Sitzungsticket anhand der Richtlinie für Benutzerrechte des Benutzerkontos überprüft. Die Überprüfung ist optional, da dieser zusätzliche Schritt Zeit in Anspruch nimmt und zu einer Verlangsamung des Netzwerkzugriffs auf Dienste führen kann.

**Max. Gültigkeitsdauer des Diensttickets**

Diese Sicherheitseinstellung bestimmt die Zugriffsdauer eines erteilten Sitzungsticket auf einen bestimmten Dienst. Der Wert muss 10 Minuten überschreiten und kleiner oder gleich der Einstellung für *Max. Gültigkeitsdauer des Benutzertickets* sein.

Legt ein Client ein abgelaufenes Sitzungsticket bei der Verbindungsaufforderung zu einem Server vor, gibt der Server eine Fehlermeldung zurück. Der Client muss daraufhin ein neues Sitzungsticket vom KDC anfordern. Da Sitzungstickets lediglich für die Authentifizierung neuer Verbindungen zu einem Server verwendet werden, werden laufende Operationen nicht unterbrochen, falls das für die Authentifizierung der Verbindung verwendete Sitzungsticket während der Verbindungsdauer abläuft.

**Max. Gültigkeitsdauer des Benutzertickets**

Diese Sicherheitseinstellung bestimmt, wie lange ein dem Benutzer zugeordneten Ticket-Granting Ticket (TGT) verwendet werden kann. Läuft das TGT ab, muss ein neues angefordert oder das vorhandene Ticket erneuert werden.

**Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann**

Dies bestimmt den Zeitraum, in dem ein TGT eines Benutzers erneuert werden kann.

**Max. Toleranz für die Synchronisierung des Computertakts**

Diese Sicherheitseinstellung bestimmt die maximale Zeitdifferenz zwischen der Systemuhrzeit des Clients und der Zeit auf dem Domänen-Controller, welcher die Kerberos-Authentifizierung bereitstellt, die von Kerberos toleriert wird.

Zur Vermeidung von Angriffen durch Wiedereinspielung abgefangener Nachrichten verwendet Kerberos Zeitstempel als Teil seiner Protokolldefinition. Aus diesem Grund sollten die Client und Domänen-Controller Uhren nach Möglichkeit synchron gehalten werden. Des Weiteren ist zu beachten, dass es sich bei dieser Sicherheitseinstellung um keine dauerhafte Einstellung handelt und diese nach einem Neustart des Clients auf den Standardwert zurückgesetzt wird.

### Berechtigungen auf AdminSDHolder-Objekt

Folgende Berechtigungen sollten für das AdminSDHolder-Objekt zugelassen werden:

| **Name** | **Berechtigung** |
|---|---|
| Jeder | Kennwort ändern |
| Administratoren | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Alle Eigenschaften schreiben<br>Löschen<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen |
| Authentifizierte Benutzer | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Berechtigungen lesen |
| Domänen-Admins | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Alle Eigenschaften schreiben<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen |
| Organisations-Admins | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Alle Eigenschaften schreiben<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen |
| Prä-Windows-2000-kompatibler Zugriff | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Berechtigungen lesen |
| SYSTEM | Vollzugriff |

## Virenprüfung durch Einführung von Skriptsignaturen

Durch das Ausschließen des Ordners SYSVOL aus der Virenprüfung erhöht sich zugleich das Virenrisiko für den Domänen-Controller, da Anmeldeskripte und Startskripte infiziert werden können. Um gleichzeitig aber unnötige Datenreplikationen durch den Dateireplizierungsdienst zu vermeiden, weil beispielsweise das Virenschutzprogramm die Metadaten (Sicherheitsinformationen oder Zeitstempel) einer Datei bei der Prüfung verändern könnte, empfiehlt sich der Gebrauch von Skriptsignaturen.

Durch die Verwendung von Skriptsignaturen kann die Integrität von Skripten vor deren Ausführung gewährleistet werden. Eine Richtlinie sollte des Weiteren im Unternehmen vorschreiben, dass alle Skripte im Ordner SYSVOL zu signieren sind und nur signierte Skripte ausgeführt werden dürfen. Signierte Skripte sollten zumindest auf Domänencontrollern und Administratorarbeitsstationen vorgeschrieben werden. Empfohlen wird jedoch, Skriptsignaturen auf allen Computern im Netzwerk vorzuschreiben. Eine entsprechende Unterstützung ist auf den Betriebssystemen Windows 2000, Windows XP sowie der Windows-Server-2003-Familie gegeben.

Zum Beispiel wird mit den im .NET Framework Software Development Kit 2.0 (SDK) enthaltenen WinTrust-Tools die Signierung und Überprüfung von Skripten (unter Verwendung von signtool.exe, signcode.exe bzw. chktrust.exe) ermöglicht. Das .NET Framework SDK 2.0 ist im Microsoft Downloadbereich (http://www.microsoft.com/downloads) verfügbar.

Um festzulegen, dass auf einem Computer nur signierte Skripte ausgeführt werden ist im Registrierungsschlüssel *HKEY_Local_Machine\Software\Microsoft\Windows Script Host* folgender Eintrag zu ergänzen:

Eintragsname: TrustPolicyData

Typ: REG_DWord

Wert: 2

Weitere Informationen zur Implementierung signierter Skripte sind in den Dokumenten *Digital Code Signing Step-by-Step Guide* (http://msdn2.microsoft.com/en-us/library/aa140234(office.10).aspx) und *Windows Script Host: New Code-Signing Features Protect Against Malicious Scripts* (http://go.microsoft.com/fwlink/?LinkId=18550) zu finden.

## Prüfung der migrierten Verzeichnisdienst-Datenbank

Folgende Komponenten sind hinsichtlich der korrekt umgesetzten Konfiguration und Funktion zu prüfen:

| **Konfiguration** | **Verwendetes Tool** | **Testziel** |
|---|---|---|
| Active Directory Service | Dcdiag.exe | Erfolgreiche Bestätigung der Active Directory Konnektivität und dessen Funktionalität |
| | Netdiag.exe | Erfolgreiche Überprüfung der Netzwerk-Konnektivität |
| Active Directory Replikation | Repadmin.exe /replsum | Erfolgreiche Replizierung zwischen der Forest Root Domäne und den übrigen Domänen-Controllern |
| Replizierungsstatus des BDCs | Nltest.exe /bdc_query:<Domänenname> | Erfolgreiche Verbindungsstatus der Backup Domänen-Controller |

| **Funktion** | **Test** | **Prüfung** |
|---|---|---|
| Erstellung eines neuen Benutzerkontos | Auf dem Windows-Server basierten Domänen-Controller ist ein neues Benutzerkonto zu erstellen. | Auf dem Domänen-Controller sollte das neu erstellte Benutzerkonto nun angezeigt werden. |
| Replikation des neuen Benutzerkontos | Nach einer erfolgten Replizierung mit dem BDC ist zu prüfen ob das neue Benutzerkonto auf dem BDC repliziert wurde. | 1. Mittels des Befehls "net user" auf dem Windows NT 4.0-basierten Domänen-Controller ist sicherzustellen, dass das neu erstellte Benutzerkonto vorhanden ist.<br>2. Ein bestehendes Benutzerkonto ist in seinen Eigenschaften abzuändern. Im Anschluss ist zu kontrollieren, ob diese Änderungen repliziert wurden. |
| Erfolgreiche Anmeldung | Benutzer sollen sich erfolgreich anmelden können. | 1. Der Windows-Server basierte Domänen-Controller ist vom Netz zu trennen, um sicherstellen zu können, dass der Windows NT 4.0-basierte Domänen-Controller die Anmeldeversuche seitens der Benutzer übernimmt.<br>2. Es ist zu überprüfen, ob die neuen Benutzerkonto-Rechte von jedem Client-Rechner für eine Anmeldung genutzt werden können. |

| | | |
|---|---|---|
| | | 3. Alle Client-Betriebssysteme können sich in der hochgestuften Domäne und der ihr vertrauenden Domänen anmelden.<br>4. Schritt zwei wird wiederholt unter der Berücksichtigung, dass die Anmeldung an einem Server stattfindet, welcher über einen gesicherten Kanal in einer Vertrauensstellung mit den Windows NT 4.0 und Windows-Server Domänen-Controllern steht. |
| Erfolgreicher Zugriff auf Ressourcen | Benutzer sollen auf wichtige Ressourcen zugreifen können. | 1. Zugriff auf Email<br>2. Zugriff auf netzbasierte Profile<br>3. Zugriff auf Netz-Drucker<br>4. Ressourcenzugriff auf Basis der Benutzer- und Gruppenrechte |

## Zugriffsschutz-Anpassung für die Domänen-Gruppe "Sicherungs-Operatoren"

Die Mitglieder der in Active Directory vordefinierten Gruppe *Sicherungs-Operatoren* verfügen über den Dienstadministratorstatus und somit über das Recht, Dateien (einschließlich der Systemdateien) wiederherzustellen. Die Mitglieder dieser Gruppe sind auf diejenigen Personen zu beschränken, welche Domänen-Controller sichern und wiederherstellen.

Standardmäßig enthält die Gruppe *Sicherungs-Operatoren* keine Mitglieder und kann nur von Mitgliedern der Gruppen *Administratoren, Domänen-Admins* und *Organisations-Admins* geändert werden. Da die Gruppe der *Sicherungs-Operatoren* nicht durch spezielle Standardeinstellungen der Sicherheitsbeschreibung im AdminSDHolder-Objekt geschützt ist, ist der Zugriffsschutz entsprechend der Berechtigungen der anderen Dienstadministratorkonten anzupassen. Die nachfolgende Tabelle gewährt einen Überblick der anzupassenden Berechtigungsstruktur zum Schutz der Gruppe *Sicherungs-Operatoren*:

| **Typ** | **Name** | **Berechtigung** | **Anwenden auf** |
|---|---|---|---|
| Zulassen | Administratoren | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Alle Eigenschaften schreiben<br>Löschen<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen | Nur dieses Objekt |
| Zulassen | Authentifizierte Benutzer | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Berechtigungen lesen | Nur dieses Objekt |
| Zulassen | Domänen-Admins | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Alle Eigenschaften schreiben<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen | Nur dieses Objekt |
| Zulassen | Organisations-Admins | Inhalt auflisten<br>Alle Eigenschaften lesen | Nur dieses Objekt |

| | | | |
|---|---|---|---|
| | | Alle Eigenschaften schreiben<br>Berechtigungen lesen<br>Berechtigungen ändern<br>Besitzer ändern<br>Alle bestätigten Schreibvorgänge<br>Alle erweiterten Rechte<br>Alle untergeordneten Objekte erstellen<br>Alle untergeordneten Objekte löschen | |
| Zulassen | Jeder | Kennwort ändern | Nur dieses Objekt |
| Zulassen | prä-Windows 2000 kompatibler Zugriff | Inhalt auflisten<br>Alle Eigenschaften lesen<br>Berechtigungen lesen | Sondereinstellungen |
| Zulassen | SYSTEM | Vollzugriff | Nur dieses Objekt |

## Sicherheitseinstellungen für Gruppenrichtlinien

Im Folgenden werden Vorgaben für die Sicherheitseinstellungen aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen können. Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen (z. B. Group Policy Objects für Server, Group Policy Objects für Arbeitsplatzrechner). Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

| **Kennwortrichtlinie** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Kennwortchronik erzwingen | 6 Gespeicherte Kennwörter |
| Kennwörter müssen den Komplexitätsanforderungen entsprechen. | Aktiviert |
| Kennwörtern für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern | Deaktiviert |
| Maximales Kennwortalter | 90 Tage |
| Minimale Kennwortlänge | 6 Zeichen |
| Minimales Kennwortalter | 1 Tag |

| **Kontosperrungsrichtlinien** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Kontensperrungsschwelle | 3 Ungültige Anmeldeversuche |
| Kontosperrdauer | 0 (Hinweis: Konto ist gesperrt, bis Administrator Sperrung aufhebt) |
| Kontosperrungszähler zurücksetzen nach | 30 Minuten |

| **Kerberos-Richtlinie** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Benutzeranmeldeeinschränkungen erzwingen | Aktiviert |
| Max. Gültigkeitsdauer des Benutzertickets | 8 Stunden |
| Max. Gültigkeitsdauer des Diensttickets | 60 Minuten |
| Max. Toleranz für die Synchronisation des Computertakts | 5 Minuten |
| Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann | 1 Tag |

| **Überwachungsrichtlinie** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Active Directory-Zugriff überwachen | Erfolgreich, Fehlgeschlagen |
| Anmeldeereignisse überwachen | Erfolgreich, Fehlgeschlagen |
| Anmeldeversuche überwachen | Erfolgreich, Fehlgeschlagen |

| | |
|---|---|
| Kontenverwaltung überwachen | Erfolgreich, Fehlgeschlagen |
| Objektzugriffsversuche überwachen | Fehlgeschlagen |
| Prozessverfolgung überwachen | Keine Überwachung |
| Rechteverwendung überwachen | Fehlgeschlagen |
| Richtlinienänderungen überwachen | Erfolgreich, Fehlgeschlagen |
| Systemereignisse überwachen | Erfolgreich, Fehlgeschlagen |

| **Zuweisen von Benutzerrechten** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Als Dienst anmelden | Definiert, aber leer |
| Ändern der Systemzeit | Administratoren |
| Anheben der Zeitplanungspriorität | Administratoren |
| Anheben von Quoten | Administratoren |
| Anmelden als Stapelverarbeitungsauftrag | Definiert, aber leer |
| Anmeldung als Batchauftrag verweigern | Nicht definiert |
| Anmeldung als Dienst verweigern | Nicht definiert |
| Auf diesen Computer vom Netzwerk aus zugreifen | Jeder,<br>Administratoren,<br>Authentisierte Benutzer,<br>Sicherungs-Operatoren |
| Auslassen der durchsuchenden Überprüfung | Jeder |
| Debuggen von Programmen | Nicht definiert |
| Einsetzen als Teil des Betriebssystems | Definiert, aber leer |
| Entfernen des Computers von der Dockingstation | Administratoren |
| Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird | Administratoren |
| Ersetzen eines Tokens auf Prozessebene | Definiert, aber leer |
| Erstellen einer Auslagerungsdatei | Administratoren |
| Erstellen eines Profils der Systemleistung | Administratoren |
| Erstellen eines Profils für einen Einzelprozess | Administratoren |
| Erstellen eines Tokenobjekts | Definiert, aber leer |
| Erstellen von dauerhaft freigegebenen Objekten | Definiert, aber leer |
| Erzwingen des Herunterfahrens von einem Remote-system aus | Administratoren |
| Generieren von Sicherheitsüberwachungen | Definiert, aber leer |
| Herunterfahren des Systems | Administratoren |
| Hinzufügen von Arbeitsstationen zur Domäne | Definiert, aber leer |
| Laden und Entfernen von Gerätetreibern | Administratoren |
| Lokal anmelden | Administratoren,<br>Sicherungs-Operatoren |
| Lokale Anmeldung verweigern | Nicht definiert |
| Sichern von Dateien und Verzeichnissen | Sicherungs-Operatoren |
| Sperren von Seiten im Speicher | Definiert aber leer |
| Synchronisieren von Verzeichnisdienstdaten | Definiert, aber leer<br>Hinweis: Gemäß der Dokumentation zum Ressorce- |

| | |
|---|---|
| | Kit findet diese Einstellung in der gegenwärtigen Version von Windows 2000 keine Anwendung. |
| Übernehmen des Besitzes von Dateien und Objekten | Administratoren |
| Verändern der Firmwareumgebungsvariablen | Administratoren |
| Verwalten von Überwachungs- und Sicherheits-protokollen | Administratoren |
| Wiederherstellen von Dateien und Verzeichnissen | Administratoren |
| Zugriff vom Netzwerk auf diesen Computer verwei-gern | Nicht definiert |

| **Sicherheitsoptionen** | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Administrator umbenennen | Nicht definiert |
| Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern | 7 Tage |
| Anwendern das Installieren von Druckertreibern nicht erlauben | Aktiviert |
| Anzahl zwischenzuspeichernder vorheriger Anmel-dungen (für den Fall, dass der Domänencontroller nicht verfügbar ist) | 0 Anmeldungen |
| Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen | Aktiviert |
| Auswerfen von NTFS-Wechselmedien zulassen | Administratoren |
| Benutzer automatisch abmelden, wenn die Anmelde-zeit überschritten wird (lokal) | Aktiviert |
| Benutzer nach Ablauf der Anmeldezeit automatisch abmelden | Aktiviert |
| Clientkommunikation digital signieren (immer) | Deaktiviert |
| Clientkommunikation digital signieren (wenn möglich) | Aktiviert |
| Die Verwendung des Sicherungs- und Wieder-herstellungsrechts überprüfen | Deaktiviert |
| Gastkonto umbenennen | Nicht definiert |
| Herunterfahren des Systems ohne Anmeldung zulassen | Deaktiviert |
| LAN Manager-Authentisierungsebene | Nur NTLMv2-Antworten senden\LM verweigern |
| Leerlaufzeitspanne bis zur Trennung der Sitzung | 15 Minuten |
| Letzten Benutzernamen nicht im Anmeldedialog anzeigen | Aktiviert |
| Nachricht für Benutzer, die sich anmelden wollen | Nicht definiert |
| Nachrichtentitel für Benutzer, die sich anmelden wollen | Nicht definiert |
| Serverkommunikation digital signieren (immer) | Deaktiviert |

| Sicherheitsoptionen (Fortsetzung) | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Serverkommunikation digital signieren (wenn möglich) | Aktiviert |
| Serveroperatoren das Einrichten von geplanten Tasks erlauben (Nur für Domänencontroller) | Nicht definiert |
| Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich) | Aktiviert |
| Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich) | Aktiviert |
| Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer) | Deaktiviert |
| Sicherer Kanal: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher) | Deaktiviert (Hinweis: In reinen Windows 2000 Umgebungen aktivieren) |
| Standardberechtigungen globaler Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken | Aktiviert |
| STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren | Deaktiviert (Hinweis: D. h. STRG+ALT+ENTF ist erforderlich) |
| System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können | Deaktiviert |
| Systemwartung des Computerkontokennworts nicht gestatten | Deaktiviert |
| Unverschlüsseltes Kennwort senden, um Verbindung mit SMB-Servern von Drittanbietern herzustellen | Deaktiviert |
| Verhalten bei der Installation von nichtsignierten Dateien (außer Treibern) | Warnen, aber Installation zulassen |
| Verhalten bei der Installation von nichtsignierten Treibern | Warnen, aber Installation zulassen |
| Verhalten beim Entfernen von Smartcards | Computer sperren |
| Weitere Einschränkungen für anonyme Verbindungen | Kein Zugriff ohne explizite anonyme Berechtigung |
| Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen | Deaktiviert |
| Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen | Deaktiviert |
| Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken | Aktiviert |
| Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken | Aktiviert |
| Zugriff auf globale Systemobjekte prüfen | Deaktiviert |

| Ereignisprotokoll | |
|---|---|
| **Richtlinie** | **Computereinstellung** |
| Anwendungsprotokoll aufbewahren für | Nicht definiert |
| Aufbewahrungsmethode des Anwendungsprotokolls | Ereignisse bei Bedarf überschreiben |
| Aufbewahrungsmethode des Sicherheitsprotokolls | Ereignisse bei Bedarf überschreiben Hinweis: Im Hochsicherheitsbereich ist folgende Einstellung zu |

| | |
|---|---|
| | wählen: Ereignisse nicht überschreiben (Protokoll manuell aufräumen) |
| Aufbewahrungsmethode des Systemprotokolls | Ereignisse bei Bedarf überschreiben |
| Gastkontozugriff auf Anwendungsprotokoll einschränken | Aktiviert |
| Gastkontozugriff auf Sicherheitsprotokoll einschränken | Aktiviert |
| Gastkontozugriff auf Systemprotokoll einschränken | Aktiviert |
| Maximale Größe des Anwendungsprotokolls | 30080 Kilobytes |
| Maximale Größe des Sicherheitsprotokolls | 100992 Kilobytes |
| Maximale Größe des Systemprotokolls | 30080 Kilobytes |
| Sicherheitsprotokoll aufbewahren für | Nicht definiert |
| System bei Erreichen der max. Sicherheitsprotokoll-größe herunterfahren | Deaktiviert (Hinweis: Für Hochsicherheitssysteme aktivieren) |
| Systemprotokoll aufbewahren für | Nicht definiert |